

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

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

**Руководство администратора
RU.29144487.506900.001 98**

На 460 листах

Москва
2024

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ	14
1.1 Назначение	14
1.2 Структура ПО «Mailion»	14
1.3 Уровень подготовки пользователя и администратора	15
1.4 Системные требования	17
1.4.1 Базовый продукт (дистрибутив) «Mailion», серверная часть	17
1.4.1.1 Аппаратные требования	17
1.4.1.1.1 Описание групп сервера	17
1.4.1.1.2 Стандартные расчеты аппаратной части	19
1.4.1.1.3 Расчет требований для 10 000 пользователей	23
1.4.1.1.4 Требования к дисковой подсистеме	27
1.4.1.1.5 Требования к сетевой подсистеме	27
1.4.1.2 Программные требования	28
1.4.2 Базовый продукт (дистрибутив) «Mailion», веб-интерфейс	30
1.4.3 Базовый продукт (дистрибутив) «МойОфис Почта», настольный клиент	33
1.5 Требования по работе с DNS	35
1.5.1 Организация работы сервисов разрешения имен	35
1.5.2 Разрешение имен на машине оператора	35
1.5.3 Формирование внешних доменных имен инсталляций	36
1.5.4 Необходимые DNS-записи	37
1.5.4.1 Внешние DNS-записи	37
1.5.4.2 Внутренние DNS-записи	39
1.6 Рекомендации	39
1.6.1 Рекомендации по разметке дисков	39
1.7 Ограничения	40
1.7.1 Ограничения при выполнении кластерной установки	40
1.7.2 Ограничение по работе с файлом inventory	41
1.7.3 Ограничение по работе с Ansible	42
1.7.4 Ограничение по работе с системами виртуализации	42
1.7.5 Ограничение по работе с хостами MX	42
1.7.6 Ограничение при заполнении файлов переменных	42
1.7.7 Ограничение при использовании данных внешнего каталога	42
1.7.8 Поддерживаемые языки интерфейса	43
1.7.9 Поддерживаемые веб-браузеры	43
2 ПЕРВИЧНАЯ УСТАНОВКА	44
2.1 Состав дистрибутива	44

2.2 Подготовка к установке	44
2.2.1 Описание ролей Ansible для преднастройки серверов перед установкой	44
2.2.2 Подготовка инфраструктуры установки	50
2.2.2.1 Установка хранилища образов Docker (docker_registry)	50
2.2.2.2 Установка конфигурационных файлов Ansible для развертывания ПО «Mailion»	51
2.2.2.3 Установка ПО «Mailion» с машины оператора	52
2.2.2.4 Размещение SSL-сертификатов для шифрования	55
2.2.3 Настройка основных параметров установки	56
2.2.3.1 Минимальные параметры установки	56
2.2.3.1.1 Настройка параметров установки ansible_user	58
2.2.3.1.2 Настройка параметров установки ArangoDB	58
2.2.3.1.3 Настройка параметров codec_secret_key	59
2.2.3.1.4 Настройка параметров dispersed_object_store	59
2.2.3.1.5 Настройка параметра Docker	60
2.2.3.1.6 Настройка параметров grafana	60
2.2.3.1.7 Настройка house	60
2.2.3.1.8 Настройка hydra	61
2.2.3.1.9 Настройка параметров jwt_key	61
2.2.3.1.10 Настройка параметров keepalived	62
2.2.3.1.11 Настройка параметров mailion	63
2.2.3.1.12 Настройка параметров MongoDB	65
2.2.3.1.13 Настройка дополнительных параметров postfix	66
2.2.3.1.14 Настройка параметров NATS	66
2.2.3.1.15 Настройка параметров redis	67
2.2.3.1.16 Настройка параметров rsrampd	68
2.2.3.1.17 Настройка параметров servus	69
2.2.3.1.18 Настройка параметров unbound	69
2.2.3.1.19 Настройка параметров resolv	70
2.2.3.1.20 Настройка параметров sophokles	70
2.2.3.1.21 Настройка параметров theseus	70
2.2.3.1.22 Настройка параметров CA	71
2.2.3.1.23 Настройка параметров viper	71
2.2.3.1.24 Настройка параметров ntp	71
2.2.3.1.25 Настройка параметров chrony	72
2.2.4 Настройка дополнительных параметров установки	72

2.2.5	Настройка межсетевого экранирования	72
2.2.5.1	Настройки правил внешнего межсетевого экрана	75
2.3	Запуск установки	75
2.4	Проверка корректности установки	76
2.4.1	Добавление дополнительных доменов для обслуживания инсталляцией	76
2.5	Установка клиента «МойОфис Почта»	77
2.5.1	Установка программы на ОС Windows	77
2.5.1.1	Установка с помощью MSI-пакета	77
2.5.2	Установка приложения на ОС Linux	80
2.5.2.1	Установка дистрибутива sh	80
2.5.2.2	Установка дистрибутива rpm	83
2.5.2.2.1	Установка rpm с помощью терминала	83
2.5.2.2.2	Установка rpm с помощью приложения установки	83
2.6	Установка в составе других продуктов ПО «МойОфис»	84
3	ОБНОВЛЕНИЕ С ПРЕДЫДУЩИХ ВЕРСИЙ	85
4	ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ И РЕКОМЕНДАЦИИ ПО УСТАНОВКЕ	86
4.1	Доступ к веб-интерфейсам вспомогательных систем для управления ПО «Mailion»	86
4.1.1	ArangoDB	86
4.1.2	Rspamd	87
4.1.3	Kunkka	87
4.1.4	Prometheus	88
4.1.5	Alertmanager	89
4.1.6	Grafana	90
4.2	Настройка взаимодействия со службой каталогов	91
4.3	Настройка антивирусного программного обеспечения	93
4.4	Настройка сервиса Vault	94
4.4.1	Установка сервиса Vault	95
4.4.1.1	Этапы установки	95
4.4.1.2	Настройка Vault AppRole и доступа к кластеру для приложений	97
4.4.1.3	Инициализация секретов	98
4.4.1.4	Настройка .ansible.cfg для доступа к развернутому Vault-серверу	99
4.4.1.5	Подготовка inventory файла	99
4.4.2	Установка на другие хосты	99
4.4.3	Создание доменных имен	100
4.4.4	Генерация CA сертификата	101

4.4.5	Создание сертификатов для каждого инстанса	101
4.4.6	Настройка конфигурационного файла Vault для каждого инстанса	102
4.4.7	Рестарт, распечатка первого инстанса Vault	104
4.4.8	Запуск и распечатка остальных инстансов Vault	105
4.4.9	Верификация работы кластера	106
4.4.10	Настройка стенда Mailion	106
4.5	Рекомендации по безопасности	107
4.6	Рекомендации по версии ядра Linux	108
5	ПОДГОТОВКА К РАБОТЕ	109
5.1	Доступ к ПО «Mailion»	109
5.2	Запуск системы	109
5.3	Проверка работоспособности системы	110
6	РАБОТА В ПАНЕЛИ АДМИНИСТРИРОВАНИЯ	113
6.1	Интерфейс приложения Панель администрирования	114
6.2	Управление пользователями	115
6.2.1	Просмотр списка пользователей	115
6.2.2	Просмотр записи о пользователе	116
6.2.3	Создание пользователя	117
6.2.4	Поиск пользователя	119
6.2.5	Блокировка и разблокировка пользователя	120
6.2.6	Удаление пользователя	121
6.2.7	Сброс пароля пользователя	122
6.2.8	Завершение всех сеансов пользователя	123
6.2.9	Изменение членства пользователя в группах рассылки	123
6.2.10	Редактирование данных пользователя	126
6.3	Управление группами рассылки	128
6.3.1	Просмотр списка групп рассылки	128
6.3.2	Просмотр записи о группе	128
6.3.3	Создание группы рассылки	129
6.3.4	Поиск группы рассылки	132
6.3.5	Добавление/исключение членов группы рассылки	133
6.3.6	Удаление групп рассылки	134
6.3.7	Редактирование группы рассылки	134
6.3.8	Настройка динамических групп рассылки	136
6.4	Управление ресурсами	137
6.4.1	Создание ресурса	137
6.4.2	Просмотр данных о пространстве для встречи	139
6.4.3	Поиск ресурса	139
6.4.4	Редактировать запись о пространстве для встречи	139

6.4.5 Фильтрация ресурсов	140
6.4.6 Удаление ресурса	140
6.5 Управление доменами	140
6.5.1 Создание домена	140
6.5.2 Поиск домена	141
6.5.3 Просмотр данных о домене	142
6.5.4 Редактировать запись о домене	142
6.5.5 Фильтрация доменов	142
6.5.6 Удаление домена	143
6.6 Управление единицами организационной структуры	143
6.6.1 Создание организационной единицы	144
6.6.2 Просмотр данных	145
6.6.3 Редактирование записи о сотруднике	145
6.6.4 Поиск единицы организационной структуры	146
6.6.5 Создание дочерней единицы	146
6.6.6 Удаление дочерней единицы	147
6.6.7 Удаление организационной единицы	148
6.7 Управление сотрудниками	148
6.7.1 Добавление нового сотрудника	148
6.7.2 Редактирование организационной единицы	149
6.7.3 Поиск сотрудника	149
6.7.4 Удаление сотрудника	150
6.8 Управление справочниками	150
6.8.1 Создание записи в справочнике	150
6.8.2 Поиск записи в справочнике	151
6.8.3 Редактирование записи в справочнике	151
6.8.4 Удалить запись в справочнике	151
7 РАСШИРЕННОЕ АДМИНИСТРИРОВАНИЕ С ПОМОЩЬЮ	
ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ	152
7.1 Информация для работы с интерфейсом командной строки	152
7.1.1 Установка	152
7.1.2 Просмотр команд	152
7.1.3 Основные роли для администрирования ПО «Mailion» с помощью интерфейса командной строки	153
7.2 Установка общей квоты на тенант администратором инсталляции	153
7.3 Операции над тенантом	155
7.3.1 Создание тенанта	156
7.3.2 Настройка уведомлений об истечении срока жизни пароля	157
7.3.3 Создание группы ALL для тенанта	159
7.3.4 Создание GAL-пользователя в тенанте	160

7.3.5	Создание администратора тенанта	162
7.3.6	Создание пользователя тенанта	165
7.3.7	Добавление роли администратора тенанта пользователю	169
7.3.8	Настройка квот в тенанте	170
7.3.8.1	Создание квот профиля	171
7.3.8.2	Удаление квот профиля	172
7.3.8.3	Обновление квот профиля	174
7.3.8.4	Создание квот профиля пользователя	176
7.3.8.5	Удаление квот профиля пользователя	177
7.3.8.6	Обновление квот профиля пользователя	178
7.3.8.7	Получение квот профиля	180
7.3.8.8	Установка общей квоты тенанта на почту	181
7.3.8.9	Получение общей квоты на тенант и общей квоты тенанта на почту	182
7.3.8.10	Нулевая квота пользователя	183
7.3.9	Удаление тенанта	184
7.3.10	Удаление письма у всех получателей в рамках тенанта	185
7.4	Создание пользовательских GAL-тегов	187
7.5	Настройка двухфакторной аутентификации	189
7.6	Создание домена	192
7.7	Создание первичной организационной структуры	196
7.8	Создание организации	199
7.9	Операции над пользователями, группами и ресурсами	201
7.10	Делегирование управления группами	207
7.11	Создание динамической группы	210
7.12	Массовое создание пользователей в каталоге	214
7.12.1	Подготовка файла импорта	218
7.12.2	Примеры сообщений системы	220
7.12.3	Возможные ошибки при импорте пользователей	222
7.13	Массовое создание групп в каталоге	225
7.13.1	Импорт групп	225
7.13.2	Импорт связей групп	229
7.13.3	Подготовка файла импорта	231
7.13.4	Примеры сообщений системы	232
7.13.5	Возможные ошибки при импорте групп	233
7.13.6	Автоматизация переноса групп и их связей из LDAP-каталогов в каталог ПО «Mailion»	236
7.14	Массовое создание ресурсов в каталоге	238
7.14.1	Подготовка файла импорта	242
7.14.2	Примеры сообщений системы	243

7.14.3	Возможные ошибки при импорте объектов ресурсов	244
7.15	Настройка миграции данных календаря	246
7.15.1	Миграция данных календаря из Microsoft Exchange в ПО «Mailion»	249
7.15.2	Миграция данных календаря из ПО «Mailion» в Microsoft Exchange	253
7.16	Настройка миграции почты	256
7.16.1	Миграция данных почты из Microsoft Exchange в ПО «Mailion»	259
7.16.2	Поддерживаемые правила при миграции данных почты	260
7.16.3	Миграция данных почты из ПО «Mailion» в Microsoft Exchange	261
7.17	Управление делегированием учетных записей	262
7.17.1	Делегирование с уровнем доступа «Не может» (Cannot)	262
7.17.2	Делегирование с уровнем доступа «От имени» (OnBehalf)	264
7.17.3	Делегирование с уровнем доступа «Отправить как» (SendAs)	265
7.17.4	Отзыв доступа к делегированной учетной записи у всех делегатов	267
7.17.5	Отзыв доступа к делегированной учетной записи у определенного делегата	270
7.17.6	Просмотр всех делегатов	273
7.17.7	Просмотр всех делегированных учетных записей	277
7.18	Поиск писем по заданным критериям	279
7.19	Массовое удаление писем	286
7.20	Удаление пользователя, группы и ресурса	288
7.21	Восстановление удаленных писем в почтовом ящике пользователя	289
7.22	Просмотр истории комментариев блокировки пользователей	293
7.23	Работа с корпоративными подписями	296
7.24	Работа с черными и белыми списками отправителей	303
7.24.1	Добавление отправителей в список	304
7.24.2	Обновление списка отправителей	306
7.24.3	Удаление отправителей из списка	307
8	СОПОСТАВЛЕНИЕ LDAP АТТРИБУТОВ КАТАЛОГА	309
8.1	Настройка маппинга через файл	309
8.2	Добавление маппинга через команды	313
8.2.1	Добавление маппинга при создании домена	314
8.2.2	Добавление маппинга при настройке делегации домена	316
8.2.3	Добавление маппинга при обновлении делегации в домене	318
9	НАСТРОЙКА KERBEROS	321

9.1	Поддержка kerberos для домена	321
9.2	Настройка для веб-клиента	324
9.2.1	Настройка браузера для авторизации через Kerberos	324
9.2.2	Проверка конфигурации Kerberos	325
9.2.3	Настройка ОС Windows	325
9.2.4	Настройка браузеров в ОС Windows	327
9.2.4.1	Настройка в Internet Explorer	327
9.2.4.2	Настройка Google Chrome	329
9.2.4.3	Настройка Mozilla Firefox	329
9.2.4.4	Настройка приложений в ОС Windows	330
9.2.4.4.1	Thunderbird	330
9.2.4.4.2	Microsoft Outlook	332
10	УРОВЕНЬ ДОСТУПНОСТИ ПО «MAILION»	333
11	НАСТРОЙКА ОГРАНИЧЕНИЙ ДЛЯ ПОИСКА ПО ВЛОЖЕНИЯМ.....	334
11.1	Ограничение размера вложений для поиска	334
11.2	Отключение поиска по вложениям	334
11.3	Ограничение скорости парсинга	335
12	ИНСТРУКЦИЯ ПО ОБНОВЛЕНИЮ СЕРТИФИКАТОВ НА ФРОНТЕНД-СЕРВЕРАХ	336
13	РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ	337
13.1	Dispersed object store	337
13.1.1	Снятие бэкапа	338
13.1.2	Проверка статуса бэкапа	339
13.1.3	Получение списка бэкапов	347
13.1.4	Восстановление из бэкапа	347
13.1.5	Частичное восстановление из бэкапа для кластера	349
13.2	ArangoDB	351
13.2.1	Резервное копирование	351
13.2.2	Восстановление	352
13.3	Redis	353
13.3.1	Резервное копирование	353
13.3.2	Восстановление	353
13.4	MongoDB	354
13.4.1	Резервное копирование	354
13.4.2	Восстановление	355
13.5	Search	356
13.5.1	Ручная синхронизация данных в dirbek – поиске по пользователям	356
13.5.2	Ручная переиндексация почтовых ящиков или календарных событий в поиске	357

13.6 Настройка роли ApplicationImpersonation (Олицетворение)	357
14 АВТОМАТИЧЕСКОЕ КОНФИГУРИРОВАНИЕ КЛИЕНТА	
«МОЙОФИС ПОЧТА»	360
14.1 Адресные книги CardDAV	360
14.2 Календари CalDAV	361
14.3 Глобальная адресная книга LDAP	361
14.4 Настройки FCM	362
14.5 Другие ответы сервера	363
15 УДАЛЕНИЕ КЛИЕНТА «МОЙОФИС ПОЧТА»	364
15.1 Удаление приложения на ОС Windows	364
15.2 Удаление приложения на ОС Linux	367
16 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	370
16.1 Сбор и анализ логов	370
16.1.1 Syslog-ng tier	370
16.1.2 Syslog-ng collector	370
16.1.3 Доставка журналов до сервера логирования	371
16.1.4 Настройка параметров Syslog-ng	371
16.2 Антиспам	373
16.3 Подключение антивирусного модуля KSE (Kaspersky)	376
16.4 Аудит действий	377
16.4.1 Поиск событий безопасности пользователя	378
16.4.1.1 Вход в систему	378
16.4.1.2 Смена пароля пользователя	380
16.4.2 Поиск событий безопасности администратора	382
16.4.2.1 Операции над пользователем	382
16.4.2.1.1 Создание пользователя	382
16.4.2.1.2 Обновление профиля пользователя	385
16.4.2.1.3 Удаление пользователя	388
16.4.2.2 Операции над доменом	389
16.4.2.2.1 Создание домена	390
16.4.2.2.2 Обновление домена	392
16.4.2.2.3 Удаление домена	394
16.4.2.3 Операции над ресурсом	396
16.4.2.3.1 Создание ресурса	396
16.4.2.3.2 Обновление ресурса	398
16.4.2.4 Операции над группами	400
16.4.2.4.1 Удаление группы	401
16.4.2.4.2 Обновление профиля группы	403

16.5 Перечень регистрируемых методов API	405
16.6 Дополнительные меры защиты ПО «Mailion»	410
17 ВОЗМОЖНЫЕ СИТУАЦИИ И СПОСОБЫ РЕШЕНИЯ	412
18 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА	413
ПРИЛОЖЕНИЕ А. ПРИМЕР НАПИСАНИЯ ВНЕШНИХ DNS-ЗАПИСЕЙ	414
ПРИЛОЖЕНИЕ Б. НАСТРОЙКИ INVENTORY ФАЙЛА ДЛЯ РАБОТЫ С VAULT	416
ПРИЛОЖЕНИЕ В. КОМАНДЫ, ВЫПОЛНЯЕМЫЕ С ПОМОЩЬЮ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ, И ИХ ОПИСАНИЕ	425
ПРИЛОЖЕНИЕ Г. ПРИМЕРЫ JSON-ФАЙЛОВ ДЛЯ КОМАНД, ВЫПОЛНЯЕМЫХ С ПОМОЩЬЮ ИНТЕРФЕЙСА ПРОГРАММНОЙ СТРОКИ	429
Г.1 Файл настроек импорта пользователей	429
Г.2 Схема записи пользователя	430
Г.3 Список глобальных адресных книг	436
Г.4 Файл настроек импорта групп	437
Г.5 Схема записи группы	438
Г.6 Файл настроек для импорта связей групп	439
Г.7 Схема записи связей групп	440
Г.8 Файл настроек импорта ресурсов	441
Г.9 Схема записи ресурса	442
Г.10 Конфигурационный файл для миграции календаря из Microsoft Exchange в ПО «Mailion»	444
Г.11 Конфигурационный файл для миграции календаря из ПО «Mailion» в Microsoft Exchange	449
Г.12 Конфигурационный файл для миграции почты из Microsoft Exchange в ПО «Mailion», из ПО «Mailion» в Microsoft Exchange	455

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

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

Таблица 1 – Перечень сокращений, терминов и определений

Сокращение, термин	Расшифровка и определение
AD	Microsoft Active Directory, служба каталогов, разработанная Microsoft для доменных сетей Windows
API	Application Programming Interface, программный интерфейс приложения
CA	Certification Authority, центр сертификации
DNS	Domain Name System, система доменных имён
Docker	Программное обеспечение для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации, контейнеризатор приложений
DOS	Dispersed Object Store, распределенное объектное хранилище
FCM	Firebase Cloud Messaging, служба, которая упрощает обмен сообщениями между мобильными и серверными приложениями
FQDN	Fully Qualified Domain Name, полное доменное имя, иногда также называемое абсолютным доменным именем. Это доменное имя, которое указывает точное местоположение домена в древовидной иерархии системы доменных имен (DNS). Включает в себя имена всех родительских доменов иерархии DNS
GAL	Global Address List, глобальная адресная книга
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
MX	Mail Exchanger, тип DNS-записи, предназначенный для маршрутизации электронной почты с использованием протокола SMTP
SPN	Service Principal Name, уникальный идентификатор экземпляра сервиса. SPN используется аутентификацией Kerberos для сопоставления экземпляра сервиса с учетной записью сервиса (service logon account)
Standalone	Конфигурация установки ПО «Mailion» без отказоустойчивости

Сокращение, термин	Расшифровка и определение
Бэкап (backup)	Резервное копирование
ДУ	Директория установки
Нода	Виртуальная или физическая машина, на которой разворачиваются и запускаются контейнеры
ООО	Общество с ограниченной ответственностью
ОС	Операционная система
Панель администрирования	Панель администрирования «Mailion»
ПК	Персональный компьютер
ПО	Программное обеспечение
ПО «Mailion»	Программное обеспечение «Корпоративная система электронной почты и планирования совместной работы команд «Mailion»
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

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

В состав продукта входят:

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

1.2 Структура ПО «Mailion»

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

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

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

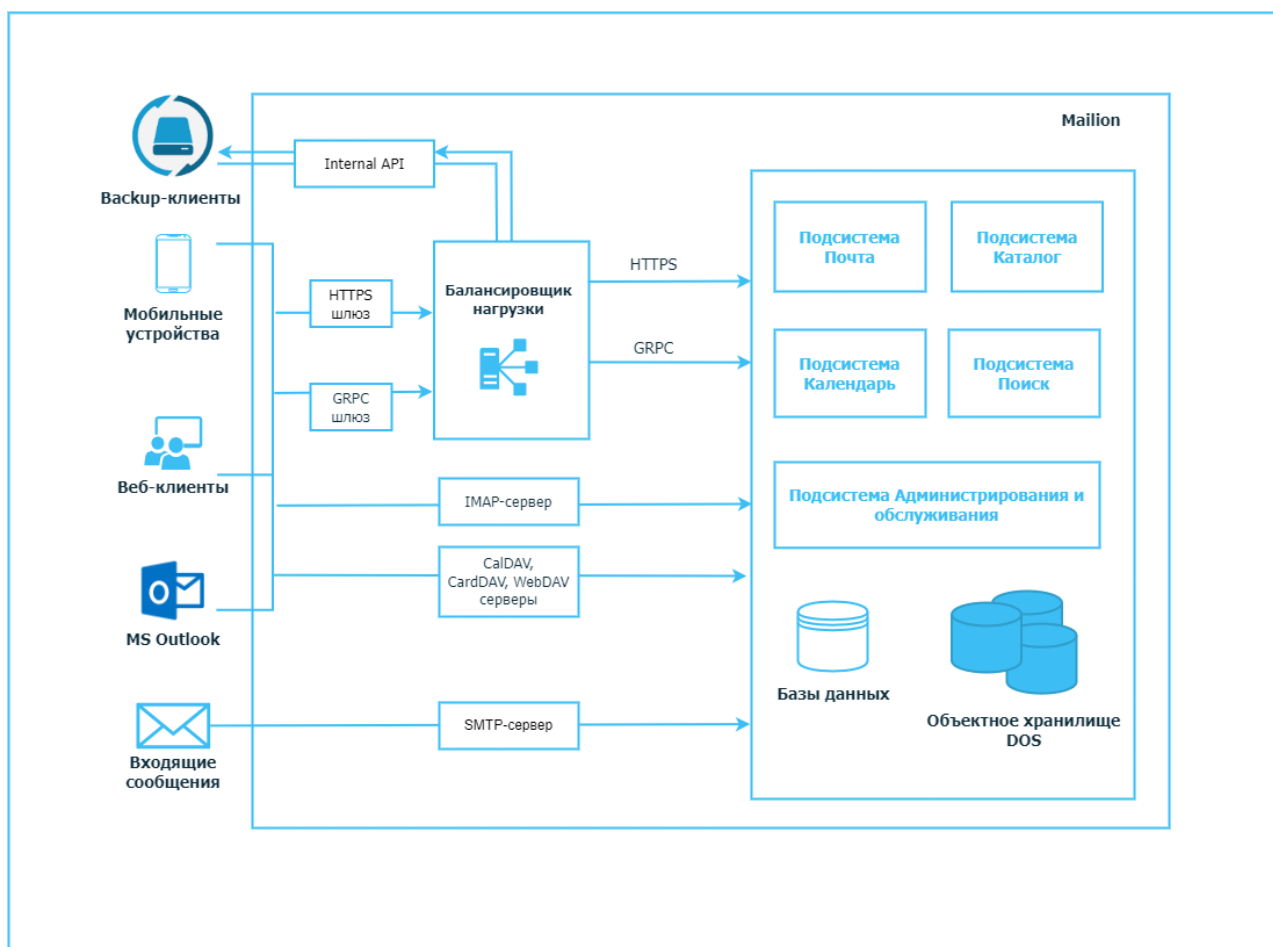


Рисунок 1 – Общая логическая схема ПО «Mailion»

1.3 Уровень подготовки пользователя и администратора

Пользователь Административной панели «Mailion» должен обладать следующими навыками:

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

Администратор ПО «Mailion» должен соответствовать следующим требованиям:

- знание основ сетевого администрирования:
 - сетевая модель OSI и стек протоколов TCP/IP;

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

1.4 Системные требования

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

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

1.4.1.1 Аппаратные требования

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

1.4.1.1.1 Описание групп сервера

В таблице 2 приведено обоснование выделения машин под группы сервера.

Таблица 2 – Описание групп сервера

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

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

1.4.1.1.2 Стандартные расчеты аппаратной части

Минимальные требования для установки ПО «Mailion» без отказоустойчивости (Mailion «Standalone») и для отказоустойчивой (кластерной) установки приведены в таблицах 3, 4.

Важно – Режим и последующая настройка параметров на оборудовании без поддержки отказоустойчивости предоставляется в целях демонстрации функциональности ПО «Mailion». **Данный режим не поддерживается, не рекомендуется его использовать.**

Таблица 3 – Минимальные требования (установка без отказоустойчивости)

Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
Mailion «Standalone»					1	12	16	-	50
ИТОГО:					1	12	16	0	50

Таблица 4 – Минимальные требования (отказоустойчивая установка)

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

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

Рекомендованные требования для установки ПО «Mailion» на отказоустойчивом оборудовании приведены в таблице 5.

Таблица 5 – Рекомендованные требования (отказоустойчивая установка)

Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_frontend	4	4	10		2	8	8	20	
ucs_mail	4	4		10	4	16	16		40
ucs_catalog	8	8	10		2	16	16	20	
ucs_apps	8	8	10		2	16	16	20	
ucs_calendar									
ucs_balancers									
ucs_search	4	8		30	3	12	24		90
ucs_converter	4	8		30	3				
ucs_etcd	8	16		30	3	24	48		90
ucs_arangodb_agency									
ucs_mongodb									
ucs_arangodb									
ucs_mq									
dispersed_object_store	4	4	60	10	4	16	16	240	40
ucs_redis_data	8	8		10	3	24	24		30

Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
	на каждую роль					итого на группу			
ucs_redis_cache									
ucs_infrastructure	4	8	200		1	4	8	200	
ИТОГО:					26	144	184	510	290

Примечания	Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
		на каждую роль					итого на группу			
Блок ВМ поисковой подсистемы	ucs_search	8	32	50	256	3	24	96	150	768
ВМ группы очередей и хранилищ данных о работе региона	ucs_etcd	16	32	50	201	3	48	96	150	603
	ucs_arangodb_agency									
	ucs_mq									
ВМ группы баз данных	ucs_mongodb ucs_arangodb									
ВМ группы хранилищ	dispersed_object_store	4	8	3471	24	4	16	32	13883	95
ВМ группы кэширующих баз данных	ucs_redis_cache	8	8	0	50	3	24	24	0	150
	ucs_redis_data									

Примечания	Имя группы сервера	VCPU	RAM, Gb	HDD, Gb (без учета ОС)	SSD, Gb	Количество виртуальных машин	VCPU	RAM, Gb	HDD, Gb	SSD, Gb
		на каждую роль					итого на группу			
ВМ инфраструктуры. Является хранилищем всех образов инсталляции, сервером мониторинга, логколлектором	ucs_infrastructure	4	8	300	0	1	4	8	300	0
ИТОГО:						18	144	284	14684	1716

Параметры расчета и дополнительные пояснения приведены в таблицах 7, 8.

Таблица 7 – Параметры расчета

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

Параметр	Значения	Заполнить	Комментарий
Избыточность данных DOS (d+p)	3	нет	Итоговая избыточность хранилища
Количество писем, шт	20971520	нет	

Таблица 8 – Дополнительные пояснения

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

1.4.1.1.4 Требования к дисковой подсистеме

Требования к дисковой подсистеме приведены в таблице 9.

Таблица 9 – Характеристики дисков

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

1.4.1.1.5 Требования к сетевой подсистеме

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

1.4.1.2 Программные требования

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

Таблица 10 – Требования к программному обеспечению для места оператора

Требование	Описания	
Поддерживаемые браузеры	Перечень поддерживаемых браузеров приведен в разделе 1.4.2	
Python	v. 3.6+	
Модули Python	jmespath	
	jinja2	не ниже версии v.2.10
	ansible	2.11 или новее, но до 2.12
	python-netaddr	python3-netaddr
	dnspython	
	pymongo	не ниже версии 3.12
Дополнительные пакеты	mongodb-mongosh	

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

Примечание – В таблице описана минимальная настройка.

Требование	Описания
ОС	Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 1.7 – Орёл (базовый);

Требование	Описания
	Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 1.7 – Воронеж (усиленный); Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 1.7 – Смоленск (с ограничениями)
Стандартные репозитории ОС	Подключение всех стандартных репозиторияв ОС либо их зеркал во внутренней сети для установок в закрытом контуре
Доступ	Для каждого сервера, на котором выполняется установка, должен быть обеспечен SSH-доступ: – с sudo привилегиями (ALL=(ALL) NOPASSWD: ALL); – без пароля (доступ по ключу)

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

Требования к аппаратному и программному обеспечению приведены в таблице 12.

Таблица 12 – Требования к аппаратному и программному обеспечению

Базовый продукт	Аппаратные требования		Программные требования
	минимальные	рекомендуемые	Поддерживаемые клиентские ОС и браузеры не ниже указанных версий
Mailion.Web	<ul style="list-style-type: none"> • CPU – x86/x64c тактовой частотой 1,6 ГГц; • RAM – 2 ГБ; • HDD – 3 ГБ для установки; • монитор с разрешением экрана – 1280x720; • клавиатура, мышь; • для работы требуется подключение к Интернету (минимум LTE) 	<ul style="list-style-type: none"> • CPU – x64 с тактовой частотой 3,0 ГГц и выше; • RAM – 8 ГБ; • HDD – 3 ГБ для установки. • монитор с разрешением экрана – 1920x1080 и выше; • клавиатура, мышь; • для работы требуется подключение к Интернету (минимум LTE) 	Ubuntu 20.04, 64 bit: <ul style="list-style-type: none"> • Chrome 108+; • Firefox 100+; Alt Linux 8 СП, 32/64 bit: <ul style="list-style-type: none"> • Chrome 92+; • Firefox 90+; «Альт Рабочая станция» версии 10, 32/64 bit: <ul style="list-style-type: none"> • Chrome 92+; • Firefox 90+; Windows 7, 32 & 64 bit: <ul style="list-style-type: none"> • Yandex 21+; • Chrome 107+; • Firefox 107+; Microsoft EDGE 87+; Windows 8/8.1, 32 & 64 bit: <ul style="list-style-type: none"> • Yandex 21+; • Chrome 107+;

Базовый продукт	Аппаратные требования		Программные требования
	минимальные	рекомендуемые	Поддерживаемые клиентские ОС и браузеры не ниже указанных версий
			<ul style="list-style-type: none"> • Firefox 107+; • Microsoft EDGE 87+; Windows 10, 32 & 64 bit: <ul style="list-style-type: none"> • Yandex 21+; • Chrome 108+; • Firefox 108+; • Microsoft EDGE 87+; MacOS (catalina): <ul style="list-style-type: none"> • Safari 13+; • Firefox 100+; • Chrome 108+; MacOS (ventura): <ul style="list-style-type: none"> • Safari 15.4+; • Firefox 100+; • Chrome 108+; RedOS 7.3: <ul style="list-style-type: none"> • Chrome 100+; • Firefox 108+; RedOS 7.3 SE: <ul style="list-style-type: none"> • Chrome 100+; • Firefox 108+; Операционная система специального назначения «Astra

Базовый продукт	Аппаратные требования		Программные требования
	минимальные	рекомендуемые	Поддерживаемые клиентские ОС и браузеры не ниже указанных версий
			<p>Linux Special Edition» РУСБ.10015-01 1.7 – Орёл:</p> <ul style="list-style-type: none"> • Chrome 108+; • Firefox 100+; • Yandex 21+; <p>Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 1.7 – Воронеж:</p> <ul style="list-style-type: none"> • Chrome 99+; • Firefox 99+; • Yandex 21+; <p>Операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 1.7 – Смоленск:</p> <ul style="list-style-type: none"> • Chrome 99+; • Firefox 99+; • Yandex 21+; <p>iOS 15.4.1; iOS 15.5; Android 10+</p>

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

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

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

Базовый продукт (дистрибутив)	Минимальные требования	Рекомендуемые требования
«МойОфис Почта», настольный клиент	<ul style="list-style-type: none"> – процессор x64 с тактовой частотой 1,0 ГГц; – оперативная память 2 Гб; – пространство для установки на жестком диске 3 Гб; – монитор с разрешением 1024x768; – клавиатура, мышь. 	<ul style="list-style-type: none"> – процессор x64 с тактовой частотой 2,0 ГГц и выше; – оперативная память 4 Гб и выше; – пространство для установки на жестком диске 5 Гб и выше; – монитор с разрешением 1920x1080 и выше; – клавиатура, мышь.

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

Таблица 14 – Поддерживаемые операционные системы для настольных клиентов «МойОфис Почта»

Базовый продукт (дистрибутив)	Платформа	Версии операционных систем
«МойОфис Почта», настольный клиент	Microsoft Windows	<ul style="list-style-type: none"> – Microsoft Windows 10 (64 bit); – Microsoft Windows 11 (64 bit).

Базовый продукт (дистрибутив)	Платформа	Версии операционных систем
	Linux	<ul style="list-style-type: none"> – Альт Рабочая станция 9 (64 bit); – Альт Рабочая станция К 9 (64 bit); – Альт Рабочая станция 10 (64 bit); – Альт Рабочая станция К 10 (64 bit); – Альт Образование 9 (64 bit); – Альт Образование 10 (64 bit); – Astra Linux Common Edition релиз 2.12 (64 bit); – Astra Linux Special Edition релиз 1.6 (64 bit); – Astra Linux Special Edition релиз 1.7 «Орел» (64 bit); – Astra Linux Special Edition релиз 1.7 «Воронеж» (64 bit); – Astra Linux Special Edition релиз 1.7 «Смоленск» (64 bit); – «Альт СП» («Альт 8 СП») 10 Рабочая станция (64 bit); – РЕД ОС 7.3.3, «Рабочая станция» (64 bit); – РОСА ХРОМ 12 Рабочая станция (64 bit); – РОСА КОБАЛЬТ 7.9 Рабочая станция (64 bit).
	Библиотеки и сертификаты	<p>Необходимо наличие:</p> <ul style="list-style-type: none"> – КриптоПро CSP 5.0.12000; – библиотеки Крипто Про PKCS#11; – действительного сертификата.

1.5 Требования по работе с DNS

1.5.1 Организация работы сервисов разрешения имен

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

1.5.2 Разрешение имен на машине оператора

Перед установкой необходимо убедиться, что на машине оператора доступен и подключен DNS-сервер, в котором созданы записи, согласно разделу 1.5.3.1. Должны быть доступны DNS-записи для машин группы **ucs_db**. Если по какой-либо причине это невозможно, то на машине оператора можно отредактировать файл `/etc/hosts` и внести в него соответствующие сопоставления имен и адресов. Пример приведен ниже:

```
192.168.0.1 ucs-db-1.installation.example.net
192.168.0.1 mongodb.ucs-db-1.installation.example.net
...
192.168.0.n ucs-db-n.installation.example.net
192.168.0.n mongodb.ucs-db-n.installation.example.net
```

Проверить разрешение имени машины в адрес можно с помощью команды:

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

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:;, udp: 65494
;; QUESTION SECTION:
;mongodb.ucs-db-1.installation.example.net. IN A
```

```
;; ANSWER SECTION:
mongodb.ucs-db-1.installation.example.net. 900 IN CNAME ucs-db-1.installation.example.net.
ucs-db-1.installation.example.net. 900 IN A 192.168.0.1

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

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

```
mongodb.ucs-db-1.installation.example.net. 900 IN CNAME ucs-db-1.installation.example.net.
ucs-db-1.installation.example.net. 900 IN A 192.168.0.1
```

1.5.3 Формирование внешних доменных имен инсталляций

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

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

Пример работы шаблона приведен в таблице 15.

Таблица 15 – Примеры работы шаблона

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

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

1.5.4 Необходимые DNS-записи

1.5.4.1 Внешние DNS-записи

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

Таблица 16 – Сведения про необходимые для инсталляции внешние DNS-записи

Имя записи	Тип записи	Значение	Комментарии
api	CNAME	@	
auth	CNAME	@	
autoconfig	CNAME	@	
avatars	CNAME	@	
caldav	CNAME	@	
carddav	CNAME	@	
db	CNAME	@	
@	A	<ucs_frontend_vip>	Значение должно быть равно VIP-адресу между серверами с ролью ucs_frontend или адресу самого сервера этой группы, если производится установка без отказоустойчивости
@	TXT	"v=spf1 mx a:relay.<mailion_external_domain> ~all"	Необходимо указать сформированное имя, с учетом значения в словаре mailion_external_domain
@	MX	10 <mx1>	MX-запись указывает на А-запись в которой содержится адрес первого сервера из группы ucs_mail
@	MX	10 <mx2>	MX-запись указывает на А-запись в которой содержится адрес второго сервера из группы ucs_mail (и т.д.)
grpc	CNAME	@	
imap	CNAME	@	

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

Таблица 17 – Сведения про необходимые для инсталляции внешние DNS-записи

Имя записи	Тип	Приоритет	Вес	Порт	Адрес
_autodiscover._tcp	SRV	0	0	443	<mailion_external_domain>.
_caldavs._tcp	SRV	0	0	6787	caldav.<mailion_external_domain>.
_carddavs._tcp	SRV	0	0	6787	carddav.<mailion_external_domain>.
_grpsec._tcp	SRV	0	0	3142	grpс.<mailion_external_domain>.
_imap._tcp	SRV	0	0	143	imap.<mailion_external_domain>.
_imaps._tcp	SRV	10	0	993	imaps.<mailion_external_domain>.
_smtps._tcp	SRV	10	0	465	smtp.<mailion_external_domain>.
_submission._tcp	SRV	0	0	587	smtp.<mailion_external_domain>.
_submissions._tcp	SRV	10	0	465	smtp.<mailion_external_domain>.

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

1.5.4.2 Внутренние DNS-записи

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

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

Пример заполнения таких записей приведен в таблице 18.

Таблица 18 – Пример заполнения

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

Важно – **unbound** не должен быть доступен из внешней сети.

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

1.6 Рекомендации

1.6.1 Рекомендации по разметке дисков

При разметке дисков требуется учитывать следующее:

- все рекомендуемые аппаратные требования приведены в разделе 1.4.1.1, в соответствии с приведенными в разделе таблицами для разных типов установки будут разные требования по выделяемому дисковому пространству;
- для всех серверов рекомендуется оставлять не менее 20 Гб на корневой раздел для штатной работы ОС.
- для роли **ucs_infrastructure** или инсталляции в режиме «Standalone» рекомендуется выделить 50 Гб на корневой раздел, так как во время установки все образы

инсталляции предварительно копируются в локальное хранилище docker (/var/lib/docker/);

- для всех серверов рекомендуется выделять отдельный раздел /srv, в который происходит установка компонентов системы, и переполнение которого не приведет к аварийной работе самой ОС. В этот раздел также могут быть направлены копии журналов работы компонентов, при соответствующей настройке лог-коллектора, что потребует дополнительного дискового пространства;
- для сервера роли **dispersed_object_store** рекомендуется выделять независимые диски HDD для серверной части и диски SSD под метаданные. Например:
 - /srv/docker/dispersed_object_store/data/metadata/ – SSD, индексы документов и сегментов;
 - /srv/docker/dispersed_object_store/data/disk1/{blob,rocksdb} – HDD1, бэкенд1 – блоб и индекс бэкенда;
 - /srv/docker/dispersed_object_store/data/disk2/{blob,rocksdb} – HDD2, бэкенд2 – блоб и индекс бэкенда;
- распределение сегментов (data segments) + (parity segments):
 - сумма data segments + parity segments не должна превышать количества независимых дисков в серверной части хранилища;
 - не менее 2 + 1 независимых дисков в серверной части хранилища;
 - для кластера из трех машин минимально допустимые значения – 2 (data segments) + 1 (parity segments) сегментов.

1.7 Ограничения

1.7.1 Ограничения при выполнении кластерной установки

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

Пример совместимости ролей приведен в таблице 19.

Таблица 19 – Совместимости ролей

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

Важно – Не рекомендуется совмещать серверные роли при установке.

1.7.2 Ограничение по работе с файлом `inventory`

В файл `hosts.yml` вносятся только полные доменные имена (далее – FQDN). Часть логики установщика использует их для формирования доменных имен и адресов сервисов.

1.7.3 Ограничение по работе с Ansible

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

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

1.7.4 Ограничение по работе с системами виртуализации

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

- VMware;
- KVM.

1.7.5 Ограничение по работе с хостами MX

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

1.7.6 Ограничение при заполнении файлов переменных

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

1.7.7 Ограничение при использовании данных внешнего каталога

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

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

Важно – Если этот пользователь еще не был создан в ПО «Mailion» (а при отправке письма на почту из внешнего каталога в ПО «Mailion» создается пользователь, если он еще не был синхронизирован), то чтобы под ним потом авторизоваться, необходимо опять же использовать для входа не **`test@ipa.example.installation.net`**, на который осуществлялась отправка письма, а **`test@installation.net`** – потому что такой Email заведен во внешнем каталоге.

1.7.8 Поддерживаемые языки интерфейса

- Русский;
- Английский.

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

- испанский;
- португальский;
- французский.

1.7.9 Поддерживаемые веб-браузеры

Перечень поддерживаемых веб-браузеров приведен в разделе 1.4.2.

2 ПЕРВИЧНАЯ УСТАНОВКА

2.1 Состав дистрибутива

В состав дистрибутива ПО «Mailion» входят:

- Установщик места оператора (`mailion_ansible_bin_1.6.1.run`).
- Установщик окружения для проведения установки, включающий все необходимые образы и пакеты (`mailion_infra_1.6.1.run`).
- Файлы `tpl` (Third-party license).

Для самостоятельной установки настольного приложения «МойОфис Почта» с поддержкой криптографической защиты данных доступны следующие дистрибутивы (см. Таблица 20):

Таблица 20 – Список дистрибутивов ПО «МойОфис Почта»

ОС	Дистрибутивы
Windows	MyOffice_Mail_PSN_Windows_2.6.1.msi
Linux	MyOffice_Mail_PSN_clean_Linux_x64_2.6.1.sh myofficemail-clean-2.6.1-17.x86_64.rpm

2.2 Подготовка к установке

2.2.1 Описание ролей Ansible для преднастройки серверов перед установкой

Ansible применяется для автоматизации настройки и развёртывания сервисов.

Общие роли Ansible описаны в таблице 21.

Таблица 21 – Описание общих ролей Ansible для преднастройки серверов перед установкой

Наименование роли	Описание
<code>authorized_keys</code>	Добавляет указанные ssh-ключи для выбранных пользователей на серверы группы <code>play_hosts</code>
<code>hostname</code>	Устанавливает <code>hostname</code> для выбранных серверов
<code>SELinux</code>	Проверяет режим работы <code>SELinux</code> и переключает его в режим «enforcing» Примечание – Только для дистрибутивов с пакетным менеджером <code>yum</code> .

Наименование роли	Описание
package manager	Настраивает пакетный менеджер
locale	Устанавливает параметры locale на серверах
timezone	Устанавливает часовой пояс на серверах
sshd	Производит настройку службы удаленного доступа sshd
chrony	Устанавливает и настраивает службу синхронизации времени chronyd Примечание – Только для ОС на базе Red Hat.
timesyncd	Устанавливает и настраивает службу синхронизации времени timesyncd Примечание – Только для ОС Astra Linux.
sysctl	Устанавливает требуемые параметры ядра на серверах
limits	Настраивает параметры ограничений на серверах
kernel_ml	Устанавливает пакет kernel_ml последнего доступного ядра
kernel_ml_deb	Устанавливает пакет kernel_ml последнего доступного ядра для ubuntu
rsyslog	Устанавливает и настраивает сервис сбора журналов
docker	Устанавливает и настраивает Docker , подключает к docker registry
unbound	Устанавливает и настраивает кэширующий DNS-сервер
iptables	Устанавливает и настраивает службы межсетевого экрана с параметрами, требуемыми для конкретной роли
resolv	Производит настройку файла resolv.conf
package_tools	Добавляет требуемые пакеты для работы ПО «Mailion» в целевую ОС

Роли, используемые для подготовки ПО «Mailion», описаны далее в таблице 22.

Таблица 22 – Описание ролей, используемых при подготовке ПО «Mailion»

Наименование роли	Описание
keepalived	Устанавливает и запускает службу, реализующую протокол VRRP
cAdvisor	Устанавливает сервис cAdvisor , осуществляющий сбор метрик работы контейнеров
node_exporter	Устанавливает сервис node_exporter , осуществляющий сбор метрик работы сервера

Наименование роли	Описание
node_cert_exporter	Мониторинг срока действия сертификатов
node_filestat_exporter	Мониторинг появления дампов памяти
blackbox_exporter	Мониторинг доступности веб-интерфейса
syslog_ng	Устанавливает сервис централизованного сбора журналов работы системы
logrotate	Настраивает ротацию хранимых журналов работы системы
ca	Устанавливает и настраивает сервис внутреннего центра сертификации
alertmanager	Устанавливает и настраивает сервис оповещений о событиях мониторинга
devkalion	Устанавливает и настраивает сервис автообнаружения сервисов инсталляции для мониторинга
gesiona	Устанавливает и настраивает сервис, экспортирующий список сервисов инсталляции для сервиса мониторинга
prometheus	Устанавливает и настраивает сервис мониторинга
grafana	Устанавливает и настраивает сервис отображения данных мониторинга инсталляции
kunkka	Устанавливает и настраивает сервис отображения данных о запущенных контейнерах на каждом сервере и их конфигурационных файлов
plugin_certificate	Роль, выписывающая сертификат для сборки клиентских приложений outlook plugin
etcd	Устанавливает базу данных etcd
hydra	Устанавливает и настраивает сервис обнаружения и балансировки нагрузки gRPC
nats	Устанавливает и настраивает NATS
nats_exporter	Сбор метрик мониторинга с NATS
mongodb	Устанавливает и настраивает документоориентированную СУБД
mongodb.mailion_migration	Устанавливает миграции данных сервисов в базах MongoDB
mongodb_exporter	Сбор метрик мониторинга с MongoDB
dorofej	Роль работы с модулем Ansible , реализующим первичную миграцию СУБД
arangodb	Устанавливает и настраивает гибридную, документноориентированную и графоориентированную базу данных

Наименование роли	Описание
arangodb.migration	Устанавливает миграции данных сервисов в базах ArangoDB
redis	Устанавливает и настраивает кластер хранилищ Redis
theseus	Устанавливает и настраивает сервис работы с учетными данными
perseus	Устанавливает и настраивает сервис хранения контактов
erakles	Устанавливает и настраивает сервис работы с сущностями
odusseus	Устанавливает и настраивает сервис работы с регионами
talaos	Устанавливает и настраивает сервис работы с тенантами
daidal	Устанавливает и настраивает сервис работы с доменами
minos	Устанавливает и настраивает сервис работы с сессиями
ektor	Устанавливает и настраивает сервис работы со связями, сущностями
pasifae	Устанавливает и настраивает сервис подсказок при поиске
dispersed_object_store	Устанавливает и настраивает объектное хранилище, предоставляющее gRPC-интерфейс для хранения бинарных данных и метаданных
achill	Устанавливает и настраивает сервис работы с аватарками
jod	Устанавливает и настраивает сервис для конвертации документов
pregen	Устанавливает и настраивает сервис для конвертации документов
cvm	Устанавливает и настраивает сервис для конвертации документов
cu	Устанавливает и настраивает сервис для конвертации документов
sdd	Устанавливает и настраивает сервис для конвертации документов
meero	Устанавливает и настраивает сервис генерации превью
mailbek	Устанавливает и настраивает сервис проксирования запросов к шардированным данным на экземплярах поисковой системы
dirbek	Сервис поиска по каталогу
helpbek	Устанавливает и настраивает поисковый сервис по имеющейся веб-документации инсталляции
tripoli	Устанавливает и настраивает единый индексно-поисковый сервис
rspamd	Устанавливает и настраивает сервис антиспама
zeus	Устанавливает и настраивает сервис, отвечающий за шаблонизацию и настройку работы с письмами
paranoid	Устанавливает и настраивает сервис, реализующий протоколы Postfix Policy Delegation и Nginx HTTP Auth

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

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

2.2.2 Подготовка инфраструктуры установки

Для подготовки инфраструктуры установки должны быть проведены следующие действия:

1. Установка хранилища образов **Docker (docker_registry)**.
2. Установка подсистемы управления конфигурациями (**Ansible**).

Подробная информация о выполнении данных действий приведена в разделах 2.2.2.1 и 2.2.2.2.

2.2.2.1 Установка хранилища образов Docker (docker_registry)

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

Этапы установки:

1. Скопировать файл `mailion_infra_1.6.1.run` на сервер.
2. Запустить скрипт установки: `bash mailion_infra_1.6.1.run`.
3. Согласиться на продолжение установки, нажать на клавишу "Y".
4. Указать тип контейнерной виртуализации (`docker` или `podman`).

Администратору отобразится:

```

Welcome to Mailion Infrastructure Installer
This script is meant to be used on Infrastructure Server (see manual for default)
choose container_management_tool ('docker' or 'podman'):*
Do you want to continue?                                [y/N] y
  Make sure that the operating system is compatible    [ OK ]
  Ensure that yum-utils is installed                   [ OK ]
  Ensure that docker-ce repository is available        [CHANGE]
  Ensure that docker is installed                      [CHANGE]
  Ensure that jq package is installed                  [CHANGE]
  Install nct-ministerium                              [ OK ]
  Install ucs-colorize                                 [ OK ]
  Ensure that docker dir exists                        [CHANGE]
  Ensure that docker daemon config exists              [CHANGE]
  Check if docker daemon needs to be restarted        [ OK ]
  Ensure that docker is started                       [CHANGE]
  Ensure that docker is enabled                       [CHANGE]
  Check if docker is available                        [ OK ]
  Ensure that registry image is available              [CHANGE]
  Check if container with registry is available        [ OK ]
  Ensure that registry configuration directory exists   [CHANGE]

```

Ensure that docker-registry anv file exists	[CHANGE]
Check if old registry data directory exists	[OK]
Ensure that registry data directory exists	[CHANGE]
Ensure that container with registry is available	[CHANGE]
Wait for docker-registry to start	[OK]
Ensure that docker-registry is running	[OK]
Extracting registry archive...	[OK]
Check if the script is run with superuser privileges	[OK]
Remove dangling and outdated images	[OK]

*в данной строке необходимо полностью ввести название типа контейнеризации.

После этого установка хранилища образов **Docker (docker_registry)** будет завершена.

2.2.2.2 Установка конфигурационных файлов Ansible для развертывания ПО «Mailion»

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

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

Этапы установки:

1. Скопировать файл mailion_ansible_bin_1.6.1.run в домашнюю директорию пользователя.
2. Запустить скрипт установки: bash mailion_ansible_bin_1.6.1.run.
3. Согласиться на продолжение установки, нажать на клавишу "Y".

Администратору отобразится:

Welcome to Mailion Ansible Installer version 2022.01 This script is meant to be used on operator workstation	
Do you want to continue?	[y/N] y

Ensure that python-netaddr is installed	[CHANGE]
Ensure that python2-jmespath is installed	[CHANGE]
Install nct-dorofej	[OK]
Install nct-ministerium	[OK]
Ensure that version directory is present	[CHANGE]
Ensure that version 2022.01 is present	[CHANGE]
Set 2022.01 as latest	[OK]
Create roles symlink	[OK]
Create contrib symlink	[OK]
Create playbooks symlink	[OK]
Create group_vars directory	[OK]
Create group_vars/all symlink	[OK]
Create host_vars directory	[OK]
Create certificates directory	[OK]
Install ucs-storm	[OK]
Create certificates symlink	[OK]

После этого установка конфигурационных файлов Ansible будет завершена.

2.2.2.3 Установка ПО «Mailion» с машины оператора

В инсталляторе представлены предзаполненные файлы конфигураций (установка выполняется в разделе 2.2.2.2), которые призваны помочь в настройке необходимого функционала будущей системы. В директории установки (ДУ) в папке **contrib** находятся 3 варианта возможной установки:

- кластерная конфигурация;
- «Standalone»;
- распределенная конфигурация «Standalone».

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

При установке конфигурации «Standalone» необходимо воспроизвести аналогичные этапы установки, описанные в данном разделе. Отличаться будет название папки, в которой находится конфигурационный файл для данной конфигурации (описано в п. 3 Этапы установки).

Структура папок приведена на рисунке 2.

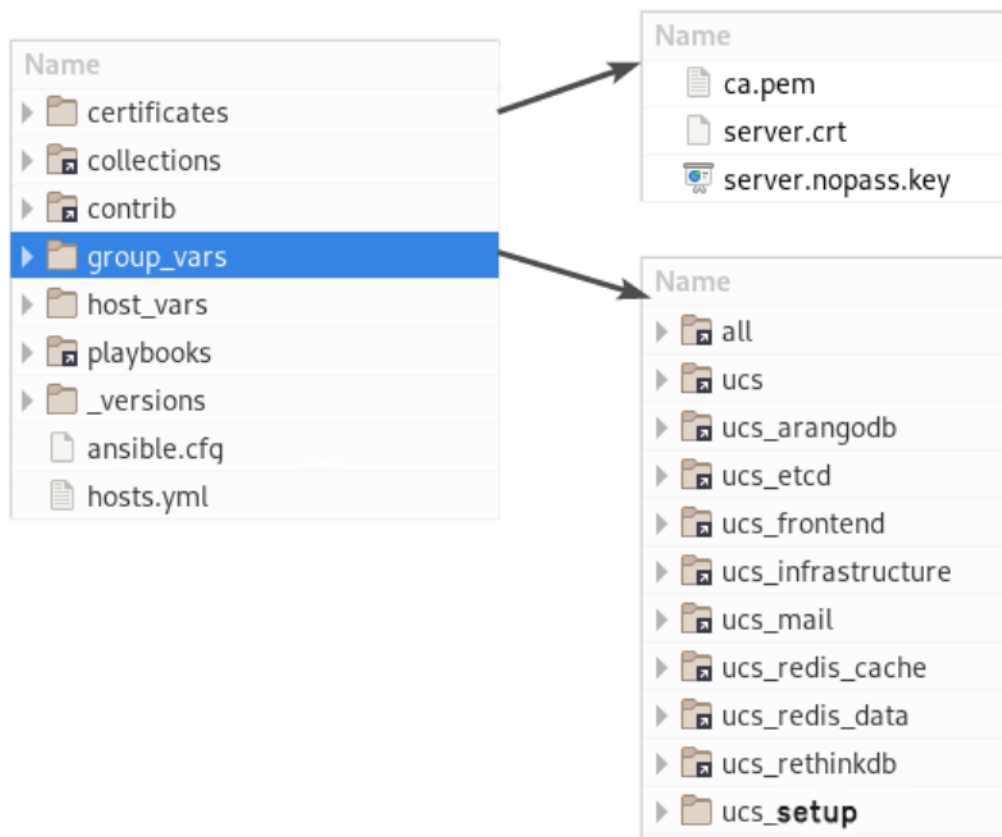


Рисунок 2 – Структура папок

Этапы установки:

1. Перейти в каталог `~/install_mailion/` с помощью команды:

```
[root@ucs-installer ~]# cd ~/install_mailion
```

2. Скопировать файл `contrib/mailion/ansible.cfg` в корневой раздел <ДУ> с помощью команды:

```
[root@ucs-installer ~/install_mailion]# cp contrib/mailion/ansible.cfg.
```

3. Подготовить файл `inventory`. Примеры заполненных файлов можно найти в каталоге `~/contrib/mailion/`. Скопировать необходимый файл следующей командой:

```
[root@ucs-installer ~/install_mailion]# cp contrib/mailion/cluster/hosts.yml hosts.yml
```

Важно – Для установки конфигурации «Standalone» необходимо скопировать конфигурационный файл из папки `contrib/mailion/standalone`.

4. Заполнить файл **inventory**.
5. Заменить имя группы **ucs_setup** на имя текущей инсталляции.
6. Скопировать ssl-ключи для внешнего домена в каталог **certificates**. Подробнее про размещение ключей можно прочитать в разделе 2.2.2.4.
7. Создать в папке групповых переменных (**group_vars**) каталог для серверов с именем группы инсталляции из секции 3 файла **inventory** (по умолчанию – **ucs_setup**).
8. Для кластерной установки скопировать в папку групповых переменных (**group_vars**) каталог с переменными для заполнения:

```
[root@ucs-installer ~/install_mailion]# cp -r contrib/mailion/cluster/group_vars/ucs_setup/*  
group_vars/ucs_setup
```

Для установки конфигурации «Standalone» необходимо скопировать конфигурационный файл из папки **contrib/mailion/standalone**.

9. Открыть файл **main.yml** из каталога размещения.
10. Отредактировать значение параметров по комментариям. Примеры параметров для минимальной настройки можно найти в разделе 2.2.3.1.
11. Открыть файл **ministerium.yml** из каталога размещения.
12. Отредактировать значение параметров по комментариям. Примеры заполнения параметров можно найти в разделе 2.2.3.1.
13. При необходимости хранения паролей в зашифрованном виде следует зашифровать содержимое файла **main.yml** с помощью команды:

```
[root@ucs-installer ~/install_mailion]]# ansible-vault encrypt group_vars/ucs_setup/main.yml --ask-  
vault-pass
```

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

```
[root@ucs-installer ~/install_mailion]]# ansible-vault encrypt group_vars/ucs_setup/main.yml --vault-  
password-file=.filesecret
```

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

```
[root@ucs-installer ~/install_mailion]]# ansible-vault edit group_vars/ucs_setup/main.yml --vault-  
password-file=.filesecret* (или --ask-vault-pass)
```

2.2.2.4 Размещение SSL-сертификатов для шифрования

Имена сертификатов могут быть произвольными, но они потребуются для дальнейшего заполнения параметров групповых переменных, поэтому важно их запомнить. В файле групповых переменных `extra_vars.yml`, который был скопирован на шаге 8 в разделе 2.2.2.3, заполнены имена сертификатов по умолчанию. Если назвать файлы сертификатов соответственно, то менять имена в переменных не нужно. В документации далее используются примеры именно таких имен.

Порядок размещения сертификатов (в примере показан порядок размещения сертификатов с использованием редактора Vim, разместить сертификаты можно без его использования):

1. Разместить сертификат внешнего домена:

```
[root@ucs-installer ~/install_mailion]# vim certificates/server.crt
```

2. Разместить ключ внешнего домена:

```
[root@ucs-installer ~/install_mailion]# vim certificates/server.nopass.key
```

3. Разместить цепочку сертификатов промежуточных центров сертификации (CA) внешнего домена:

```
[root@ucs-installer ~/install_mailion]# vim certificates/ca.pem
```

В конце файла не должно быть пустой строки. Рекомендуется прочитать файл с помощью утилиты CAT. В результате отобразится следующее:

```
[root@ucs-installer ~/install_mailion]# cat certificates/server.crt
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
[root@ucs-installer ~/install_mailion]#
```

4. Скопировать файлы сертификатов (`ca.pem` `server.crt` `server.nopass.key`) в папку: **collections/ansible_collections/nct/certs/roles/tls_certs/files.**

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

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

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

2.2.3 Настройка основных параметров установки

2.2.3.1 Минимальные параметры установки

Минимальные параметры, обязательные для заполнения:

- **ansible_user;**
- **arangodb_bearer_token;**
- **arangodb_users;**
- **codec_secret_key;**
- **dispersed_object_store_management_token;**
- **grafana_admin_password;**
- **house_ldapauth_password_salt;**
- **hydra_get_service_list_token;**
- **jwt_key;**
- **keepalived_vrrp_instances;**
- **mailion_cluster;**
- **mailion_domain_module;**
- **mailion_external_domain;**
- **mailion_installation_admin_password;**
- **mailion_integrations;**
- **mailion_internal_web_auth;**
- **mailion_max_users;**
- **mailion_service_accounts;**
- **mailion_supported_domains;**
- **mailion_tenants;**
- **mongodb_root_password;**
- **mongodb_secured_key;**

- **mongodb_management_users;**
- **nats_authorization_password;**
- **nats_cluster_authorization_password;**
- **redis_cluster_replicas;**
- **redis_dafnis_password;**
- **redis_dowal_password;**
- **redis_ektor_password;**
- **redis_erakles_password;**
- **redis_euripides_password;**
- **redis_hog_password;**
- **redis_homeros_password;**
- **redis_leda_password;**
- **redis_minos_password;**
- **redis_rspamd_password;**
- **redis_sdd_password;**
- **redis_viper_password;**
- **rspamd_kse_endpoints;**
- **rspamd_dkim_hosts;**
- **rspamd_web_password;**
- **servus;**
- **sophokles_access_token;**
- **theseus_cipher_key;**
- **tls_certs_remote_token_key;**
- **unbound_forward_addresses.**

Структура и способы заполнения указанных параметров приведены в разделах ниже.

2.2.3.1.1 Настройка параметров установки `ansible_user`

Настройка параметров приведена в таблице 23.

Таблица 23 – Настройка параметров `ansible_user`

Параметр	Тип данных	Описание
<code>ansible_user:</code>	str	Имя пользователя, под которым установщик будут доступны серверы инсталляции по SSH

Пример корректно настроенного параметра:

```
ansible_user: "root"
```

2.2.3.1.2 Настройка параметров установки ArangoDB

Настройка параметров приведена в таблице 24.

Таблица 24 – Настройка параметров ArangoDB

Параметр	Тип	Описание
<code>arangodb_bearer_token:</code>	str	Токен авторизации по http для сбора метрик сервисом мониторинга
<code>arangodb_users:</code>		Словарь пользователей СУБД
<code>ektor:</code>		Имя пользователя одноименного сервиса (не изменяется)
<code>password:</code>	str	Пароль пользователя одноименного сервиса
<code>root:</code>		Имя суперпользователя СУБД
<code>password:</code>	str	Пароль суперпользователя СУБД

Пример корректно настроенного параметра:

```
arangodb_bearer_token:
"eyJhbGciOiJIUzI1NiIsInR5cGU6IjYiLCJ1eWciOiJ0bm90cmVudCI6dXN1cmVudC9pZCI6ImZvbyJ9.
Vra2xXWl2-XS9leYTYgosSLXiswSfPa8SCLN8C1VVR8"
arangodb_users:
ektor:
  # Generate the password with: pwgen 20 1
  password: "oikahy2dah4aHah3quia"
sophokles:
  # Generate the password with: pwgen 20 1
  password: "quuuphoh6Yoomae2Ieso"
euripides:
  # Generate the password with: pwgen 20 1
  password: "we0quee4vaesiex8liJa"
root:
  # Generate the password with: pwgen 20 1
```

```
password: "jeibash6jaes0Inoo7ka"
```

2.2.3.1.3 Настройка параметров `codec_secret_key`

Настройка параметров приведена в таблице 25.

Таблица 25 – Настройка параметров `codec_secret_key`

Параметр	Тип	Описание
<code>codec_secret_key:</code>		Словарь параметров секретов для формирования зашифрованной ссылки
<code>rcr:</code>	str	Используется для формирования ссылки на проксирование данных внутри системы
<code>secret_link:</code>	str	Используется для формирования ссылки на проксируемые ресурсы
<code>values_codec</code>	str	Значение

Пример корректно настроенного параметра:

```
codec_secret_key:
rcr: "O1Wk7ha80M1qfvq8UtuZg918AZyh+q65s68dKvXwVTQ="
secret_link: "69rUgWgrLbV50CiAEK78AJrLoWBGHGwYCX25phh3yg="
values_codec: "ggxhfxrjshb034fosedfwd3d"
```

2.2.3.1.4 Настройка параметров `dispersed_object_store`

Настройка параметров приведена в таблице 26.

Таблица 26 – Настройка параметров `dispersed_object_store`

Параметр	Тип	Описание
<code>dispersed_object_store_management_token:</code> ""	str	Токен доступа для управления через API сервиса

Пример корректно настроенного параметра:

```
dispersed_object_store_management_token: "Aig2utoavi6iageil tas"
```

2.2.3.1.5 Настройка параметра Docker

Настройка параметров приведена в таблице 27.

Таблица 27 – Настройка параметров **Docker**

Параметр	Тип	Описание
docker_daemon_parameters:		Параметры демона docker
bip:	str	Подсеть и маска для docker
dns:	list	Список строк с адресами DNS-серверов
mtu:	int	Значение MTU для сетевого интерфейса docker

Пример корректно настроенного параметра:

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

2.2.3.1.6 Настройка параметров grafana

Настройка параметров приведена в таблице 28.

Таблица 28 – Настройка параметров **grafana**

Параметр	Тип	Описание
grafana_admin_password:	str	Пароль администратора grafana

Пример корректно настроенного параметра:

```
grafana_admin_password: "Ooj0Inahgh2Ixailoxie"
```

2.2.3.1.7 Настройка house

Настройка параметров приведена в таблице 29.

Таблица 29 – Настройка параметров **house**

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

Пример корректно настроенного параметра:

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

2.2.3.1.8 Настройка hydra

Настройка параметров приведена в таблице 30.

Таблица 30 – Настройка параметров **hydra**

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

Пример корректно настроенного параметра:

```
hydra_get_service_list_token: "maiquauzuwooQu9ooR7x"
```

2.2.3.1.9 Настройка параметров jwt_key

Настройка параметров приведена в таблице 31.

Таблица 31 – Настройка параметров **jwt_key**

Параметр	Тип	Описание
jwt_key:		Параметры jwt_key
priv:	str	Закрытый ключ
pub:	str	Публичный ключ

Пример корректно настроенного параметра:

```
jwt_key:
priv: |
-----BEGIN RSA PRIVATE KEY-----
MIIeowIBAAKCAQEA063xN82Y0tJBq8sfd79bJ+4W9QEdOueQljPziN4JdYntS381
AqxOA4Ud886S4LdwCN2KSpuh7QSHkzjzH9AIDrHCYShOfP AeHLMCBDSzazr2IOc0
Jaw3bHRfrM9Iib+X4qdDE88Mfk+B/8Sa/xG2HJVy0Jjb4XoipwzEB900a+6zpnLT
q/kNt7YtrTBmrgpSzFMr0VD+x0Ftb9zhiFVLyVscVKEl67+TNIWahgzH14YF8xP8
gb89coH114YUNfxN8IKURdY9QFNuZLF+x8xfl4CWwydSbtL7dFFK0HVowMt4tnoJ
okthJ5JZNw+XZAXHS3NyuvbYmP+iqRuL2YAr2wIDAQABAoIBAGyNHs5HGHHRsOuw
VorKDq0DY7Jwx9SVO4hLS/A8LQ2hlZbJvR2JztfvQ9TrclbauxFQysJH3Vn2oK/W
3JbL3rUSY2P/j4Bygn6lLbuNwGiU6/MjnZJUJnfvlcDA67AfeHw62iMmYnmDvB61
a+ax5nnyCdb/DIMsZujTmxONVHykFSF8xQhIRCJQCIXx3fl dJyaG4Qpy9WqIDVRX
5SUYegDVtNQQKO4UgrgTnOFBkPCbN9SmWEqNTnZVzPAMA3sbJkYsNEVbtuHg8G0M
nWzN7hBV6pulP096IDrSJC7qpVmb75UG5f9Oo2F0x1hHyE7bCiXN+ilcDHpFul7g
u6vptYECgYEA+PWFT4+kYRA3cb5Ki6oHLM4uhIrJzxJxWalb2Iky1 Ta3YZ4alsXL
9uac3vqZJBTPjJLwmUaktUmf+xf3CBq5e3O3BcKDDn3svs7ibawjoWK6lG5D+tf
XwzkRMT2IK6hDn16IK/DchFYTw5zy/AbyjJEAjN2y/JaLwhTywGXLdkCgYEA2aqD
zNT+Oxt9LTtnvr8RUAMIGn/g07WQNYWWmlc6HSq+lhxyvN5+PaFcjMLCIOpX7ut
YG9arh8PwDfc4kpZwnB6QWcqTucZOzbIcsVWWsMoWftVjpbCCkxZ9Sg0waKju7Bz
Dzrjzsn+AoC7O/RydhbUALUoEN5Toz8Sv5bZMtMCgYEA1mnGHaaNoNbxmXGVDEIs
mcccdQyOw+TleDCWTJ6PJ9t2ABH/BUJcbuhlViujzGaM7viBdJRgkUc9nsAbo7FGz
```

```
H0G3xc/F5I/MKAa92TZRSv3yjSpDI1XlTrkIo72qzJS1uyAQHbSitEwB7Vx6GGs7
0+cd0PN33eBIEVqvqAg/pskCgYB00NJTR6v5RNN1RwBymIBMRJR3ta8Pb82qCv47
dbd2l83auLA2Y9d+Ca+sjkBJnX905WYy9RARipIFcvWUbJqng33ZQ+is19HuuYPy
NH4Xz80EHaLZF4ejxz4wGBfYI9UDkbruXYiNHIK4PSY/Eu+20KGOj6qlAuyYG+2P
7QE8CQKBgBxUBFeFTRZxvUV+FfCvgrQxoD6C9PA46/wV9qkVfCo8i7UnDc7ovKuQ
Uq3/k9aD8NKVjJnJ7/kQEnLlBjcHcpazMHQJnvpfRaqfBre0G1ok9sPH/rvTgK1U
cIKH2eSXgRhKgLf3Dtf6m2bULj0HN0FIydngH0F1EqK10vnmvqfkN
-----END RSA PRIVATE KEY-----
```

pub: |

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA063xN82YotJBq8sfd79b
J+4W9QEdOueQljPziN4JdYntS381AqxOA4Ud886S4LdwCN2KSpuh7QSHkzjzH9Al
DrHCYShoPfaeHLMCBDSzazr2IOc0Jaw3bHRfrM9Ib+X4qdDE88Mfk+B/8Sa/xG2
HJVy0Jjb4XoipwzEB900a+6zpnLTq/kNt7YtrTBmrgpSzFMr0VD+x0Ftb9zhiFVL
yVscVKEl67+TNIWahgzh14YF8xP8gb89coH114YUNfxN8IKURdY9QFNuZLF+x8xf
L4CWwydSbtL7dFFK0HVowMt4tnoJokthJ5JZNw+XZAXHS3NyuvbYmP+iqRuL2YAr
2wIDAQAB
-----END PUBLIC KEY-----
```

2.2.3.1.10 Настройка параметров `keepalived`

Настройка параметров приведена в таблице 32.

Таблица 32 – Настройка параметров `keepalived`

Параметр	Тип	Описание
<code>keepalived_vrrp_instances</code>		Параметры <code>keepalived</code>
<code>ucs_frontend:</code>		Параметры <code>ucs_frontend</code>
<code>password:</code>	str	Пароль
<code>virtual_ip</code>	str	Виртуальный IP для группы хостов <code>ucs_frontend</code>
<code>ucs_mail:</code>		Параметры <code>ucs_mail</code>
<code>password:</code>	str	Пароль
<code>virtual_ip</code>	str	Виртуальный IP для группы хостов <code>ucs_mail</code>

Пример корректно настроенного параметра:

```
keepalived_vrrp_instances:
ucs_frontend:
password: "UgohSh8i"
virtual_ip: "192.168.10.10"
ucs_mail:
password: "keeB5ooH"
virtual_ip: "192.168.10.10"
```

2.2.3.1.11 Настройка параметров mailion

Настройка параметров приведена в таблице 33.

Таблица 33 – Настройка параметров mailion

Параметр	Тип	Описание
mailion_cluster:	bool	Флаг кластерной или «Standalone» инсталляции
mailion_domain_module	special	Переменная для генерации эндпоинтов инсталляции
mailion_external_domain:	str	Внешний домен инсталляции
mailion_installation_admin_password	Str	Пароль для администратора всей инсталляции (!)
mailion_integrations	dict	Словарь, содержащий настройки интеграций
mailion_integrations.microsoft	bool	Включение и отключение интеграции с решениями Microsoft
mailion_integrations.freeipa	bool	Включение и отключение интеграции с FreeIPA
mailion_integrations.squadus	bool	Включение и отключение интеграции с ПО Squadus
mailion_integrations.co_auth	bool	Включение и отключение интеграции с ПО «МойОфис «Частное Облако»
mailion_integrations.psn	bool	Включение и отключение интеграции с PSN
mailion_integrations.google_oauth	bool	Включение и отключение интеграции с Google OAuth
mailion_internal_web_auth	dict	Словарь, содержащий настройки внутренней веб-аутентификации
mailion_internal_web_auth.enabled	bool	Включение и отключение аутентификации для доступа к веб-интерфейсам инфраструктурных сервисов (мониторинг, grafana и т.д.)
mailion_internal_web_auth.password	str	Пароль для аутентификации для доступа к веб-интерфейсам инфраструктурных сервисов
mailion_max_users:	int	Максимальное количество пользователей в инсталляции
mailion_service_accounts	dict	Словарь, содержащий пароли сервисов (values) и имена сервисов (keys)
mailion_supported_domains	list	Список доменов, которые инсталляция будет поддерживать

Пример корректно настроенного параметра:

```
mailion_cluster: true
mailion_domain_module: "{service}.{domain}"
mailion_external_domain: "installation.example.net"
mailion_installation_admin_password: "oor3Iekichocaiphahr5"
```

```
mailion_integrations:
  aldpro: false
  co_auth: false
  freeipa: false
  google_oauth: false
  microsoft: false
  psn: false
  samba_dc: false
  squadus: false
mailion_internal_web_auth:
  enabled: true
  password: "rfkg7shtasjffa6vnd"
mailion_max_users: 100
mailion_service_accounts:
  ararat: "Jo8be1pheicahmieV2oa"
  ares: "72gyV456uh9ARiYs8jBx"
  ariadne: "Um6heiNie2doeshee2sa"
  atlas: "Gaezohg1Ad3naf5ahpef"
  clotho: "Hyrq5iedwemdLNrV47KT"
  cox: "Ii0eeceen5tilOe6xaeb"
  dfink_plugin: "Gaezohg1Ad312345hpef"
  elysion: "le0eelePhooghoughoopo"
  erakles: "Ui6ohDahLeitozughugh"
  hog: "shee8eimoh4AivigePei"
  homeros: "ooph8EfulEesu2quahl1u"
  house: "ahb9Hai3Quaid4aed7an"
  imap: "feo6aita3El6aiMaeboh"
  kongur: "aa6eizooguPhene9uifu"
  kronos: "iphuTh0eiY2ook4aeph5"
  leda: "72YjiCQrnwUwCR32sVrL"
  lmtp: "aicae3yo7Aukaejee2e"
  marker: "eer1edaeceeJu6naiPom"  minos: "eshegh3iaR0fie0G"
  othrys: "eeth8Avohv8OpheeHieg"
  paranoid: "Yoa4eNgahm0aeChu8uWe"
  perseus: "Oogh9ahroow2eicaeng7"
  razor: "Ohquietikenu2Aeloh6E"
  theseus: "eileixietai0cahQu3ma"
  viper: "Feir8uewie4Ieshu4thi"
  woof: "at6Ohdapohaitahtho2j"
  zeus: "fa4Ohxaithee0yae1eit"
mailion_supported_domains: []
```


2.2.3.1.12 Настройка параметров MongoDB

Настройка параметров приведена в таблице 34.

Таблица 34 – Настройка параметров MongoDB

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

Пример корректно настроенного параметра:

```
## MongoDB secrets
## Generate the password with `pwgen 16 1`
mongodb_root_password: "ohre4Rohngahshah"
## Generate the password with `pwgen 16 1`
mongodb_secured_key: "uGhie5ieweixaе9C"
mongodb_management_users:
  achill:
    password: "cohh0Av2mai2aJae"
  beef:
    password: "idohjie2Ikeice0I"
  clotho:
    password: "wahcoovei0bahRu4"
  daidal:
    password: "cheYichoongoh4gi"
  erakles:
    password: "Uxeu4ieph1uix1ah"
  hog:
    password: "rae0faeng1Seupee"
  homeros:
    password: "хоорunaihuopae4J"
  marker:
    password: "ohvufоosaeTeeCo3"
mongodb_exporter:
```

```

password: "woo2Yua2saeboh1 "
kongur:
password: "ahmeayooH1yahlohreem"
kronos:
password: "peiNguxud8ooThaiCahL"
odusseus:
password: "oY9ja7ietheec6sahthe"
perseus:
password: "xuoboop5Geneemei"
sophokles:
password: "baexuli5oow8ohTh"
talaos:
password: "Ahroozait4pesupohpho"
themis:
password: "feef8euch8gaiwieRoig"
theseus:
password: "ua8mu0uoj6uvieDu2gei"thoth:
password: "BooRah6oaI9Naehai2ph"

```

2.2.3.1.13 Настройка дополнительных параметров postfix

Настройка дополнительных параметров приведена в таблице 35.

Таблица 35 – Настройка дополнительных параметров postfix

Параметр	Тип	Описание
postfix_additional_mynetworks:	list	Список дополнительных сетей, из которых разрешена отправка через МТА инсталляции

Пример корректно настроенного параметра:

```

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

```

2.2.3.1.14 Настройка параметров NATS

Настройка параметров приведена в таблице 36.

Таблица 36 – Настройка параметров NATS

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

Пример корректно настроенных параметров:

```
nats_authorization_password: "Fiohoogh7Raobi4yeiSi"
nats_cluster_authorization_password: "ao1Iey7luRohl ahf9eVe"
```

2.2.3.1.15 Настройка параметров redis

Настройка параметров приведена в таблице 37.

Таблица 37 – Настройка параметров **redis**

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

Пример корректно настроенных параметров:

```
redis_dafnis_password: "eexaiSheQuoivul oo4ak"
redis_dowal_password: "oasu7nieNg0aeshaiphi"
redis_ektor_password: "eisach9eet8thaug9Ieg"
redis_erakles_password: "zae9iaL3ooth3ahphugh"
redis_euripides_password: "xi6Ohy8io5ku7veQuau7"
redis_hog_password: "dighaeX0hoov6aeJee3u"
redis_homeros_password: "chae7quah7Li2zohbe8o"
redis_leda_password: "Aiy6iiyeiZo2caaleofe"
redis_minos_password: "quie2jiG2CeucosShahG"
```

```
redis_rspamd_password: "Iughoo2iuS2Xew1die4p"
redis_sdd_password: "fohphow6eat1aekod5Oh"
redis_viper_password: "Tee9han6ienaYoSievoo"
```

2.2.3.1.16 Настройка параметров rspamd

Настройка параметров приведена в таблице 38.

Таблица 38 – Настройка параметров **rspamd**

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

Пример корректно настроенного параметра:

```
rspamd_dkim_hosts:
installation.example.net:
dkim_key: |
-----BEGIN PRIVATE KEY-----
MIIEvwIBADANBgkqhkiG9w0BAQEFAASCBAkwggSIAgEAAoIBAQC3euVQm/Djy1z1
JhbTC5Cs99HmrgN6DldM5xivTyhopgkGIHXIoWaKft3wK.m/Pzah2/BkcTXtDa3w
E70bmjVXF2xkXG5DAuY9ChnX6+xWYCeBUeRsMSnWdyoNBwFK9rjE2vZ+u3OzLhz
wP6PuIyigV7A3D9Mtok0XA3iH/7G+99ARjxhj8hCkYEqEsR688uU1JNeztTfkte+
mz6n7w8AO2jdpdG8wRqjvj4B4H0MaaP7R4y/UopZ+UP0RABm7KryOjgC15uLou9Y
Yg9ym0VkaIOvc0xQT7Zk13yf8vluVS/6yhO3FcKYB4mx0Szz1RpU2ueyvD2COSj
C+2uZsPFAgMBAAECggEBAK6+xEH2kwFRAPKWWSydGigyS4K11OO7wRWIMNuf4zT
fUsf+GaHoAPGk7eVozHlq+nOhdfXz2rRpqdlGf06BJNbI2+ePIFj9IXz5dMoZcm
KAHYA2a1VUYRpr8oCfu+3dRg/dn4S58miRHtoESfPonS7rx9x2e3fYs5IRtk35EA
Wp5Vy+2U36cKIILVtAOvzRbGi9SLjPAvuc/WKGda2IA7HBlhep/Yrm0RUoH//5Px
fJwLVSy34B31Fx1wZk80aVquXCv644GbR89RIQtziHg9q4g/wyZ5/+ZG/967kim
tKDS8PWhAK5pjUHS9cED/hjs+ITINCi4qKf2zj2XSqECgYEA3X9zmaAw9JLnelZN
3oVM/boqtwfPgnO6Y98inDMsecAICWLCAsEsWYY90IB3FQCXJXVrGTxKnHa3S0fR
MTX5xx3Rta5SWf88jUQCmZEuxHBeIEN9JKebKC97rKIIIJmYJ8PVZ8c6LAvMgmYc
sd+GyjJAmV+N7j5Eo8tXmZCCuK0CgYEA1A9t7P6GjXQQFrIk81+x+0JHmIN+DPKs
eyR6avDfd32HIq2dPCMmjCAI7EFbfOPVNx9rZvLrEWtTkGU8DYBPIZ955EJORi9l
eqYeOKwhWLUMgwHyWIEJZPeY3o31TF1NwNG16Qy98h4zr2SUaTuCccoNWAc0GuI
rA1Gjn7AonkCgYEAuMpgFJS8Aw+cdwARrxffb7+Na23kvZz3X+ME6PP4owqGqe3u
loW7DmVkpNLIhokbkHDJjSAzzx1sBi5AZKH3ZRuHnd91bQf36JNY5+2r6s8keB5W
```

```

BYKfe4NB1uDfwLbjrik/nXklGyIs2I2AWxV1SrNqGYsSyjTA5zX6O2/I33ECgYBS
eO23jgWmXc0kBoR4Ym9F2LEfj4QmZPrPqZAypxtBzYaq7JSKHuGO/bHCAGkkWTdD
COUsVK03SRZnY8HHPm+1MSCmtWLbyPMekByQzeDqLv9+s/MdTQbqTaEWbP9Jg8AJ
jYXB7UKyNyzCucs+YfaK97mbiJWsOSYeQ8t8/67LgQKbgQCk4q/D5Cq5Fqalbk/0
jyEQAmHgrhWEJO2bECGjGIJ13/Hj3bbQ3znfPUDf9MLDtrveGu4YdspL3S4yahLO
EXxXPgwHCDLqamx5vj4QKFPFQEHXv68RK6RKhw7m2IeyI/7nsHPvjZhNZI4ulSTN
CLCjuiw8tvlafY26wKDyIpnvRQ==
-----END PRIVATE KEY-----

```

```
rspamd_web_password: "iePixieTaf4IriequieX"
```

2.2.3.1.17 Настройка параметров **servus**

Настройка параметров приведена в таблице 39.

Таблица 39 – Настройка параметров **servus**

Параметр	Тип	Описание
servus:	str	Параметры servus

Пример корректно настроенного параметра:

```
servus: "Iefae4yoh4rohceepoli"
```

2.2.3.1.18 Настройка параметров **unbound**

Настройка параметров приведена в таблице 40.

Таблица 40 – Настройка параметров **unbound**

Параметр	Тип	Описание
unbound_access_control:	dict	Параметры доступа к управлению unbound
network1	str	Подсеть, из которой разрешен доступ к кэширующему DNS
unbound_enable_automwildcard:	bool	Флаг использования автоматического формирования DNS-записей внутренних адресов на базе серверов в файле inventory и их значений переменной ansible_default_ipv4
unbound_forward_addresses:	list	Список строк внешних DNS-сервисов, на которые будут перенаправляться запросы unbound серверов

Пример корректно настроенного параметра:

```
unbound_enable_automwildcard: false
unbound_access_control:
```

```
network1: "192.168.1.0/24"
unbound_forward_addresses:
- "8.8.8.8"
  - "1.1.1.1"
```

2.2.3.1.19 Настройка параметров **resolv**

Настройка параметров приведена в таблице 41.

Таблица 41 – Настройка параметров **resolv**

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

Пример корректно настроенного параметра:

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

2.2.3.1.20 Настройка параметров **sophokles**

Настройка параметров приведена в таблице 42.

Таблица 42 – Настройка параметров **sophokles**

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

Пример корректно настроенного параметра:

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

2.2.3.1.21 Настройка параметров **theseus**

Настройка параметров приведена в таблице 43.

Таблица 43 – Настройка параметров **theseus**

Параметр	Тип	Описание
theseus_cipher_key:	str	Ключ шифрования theseus

Пример корректно настроенного параметра:

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

2.2.3.1.22 Настройка параметров CA

Настройка параметров приведена в таблице 44.

Таблица 44 – Настройка параметров CA

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

Пример корректно настроенного параметра:

```
tls_certs_remote_token_key: "afba15d0def55ca6e57efb481f8232a5"
```

2.2.3.1.23 Настройка параметров viper

Настройка параметров приведена в таблице 45.

Таблица 45 – Настройка параметров viper

Параметр	Тип	Описание
viper_calendar_settings_sender_white_list:	list	Список отправителей, которые могут присылать календарные письма за участника события (например, сервисные ящики no-reply).
regexp:	str	Выбор отправителей по регулярному выражению
sender_in_reply_to	bool	Добавить отправителя в reply_to

Пример корректно настроенного параметра:

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

2.2.3.1.24 Настройка параметров ntp

Настройка параметров приведена в таблице 46.

Таблица 46 – Настройка параметров ntp

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

2.2.3.1.25 Настройка параметров chrony

Настройка параметров приведена в таблице 47.

Таблица 47 – Настройка параметров **chrony**

Параметр	Тип	Описание
ntp_servers:	list	Список ntp серверов

2.2.4 Настройка дополнительных параметров установки

Настройка дополнительных параметров установки не выполняется для ПО «Mailion».

2.2.5 Настройка межсетевого экранирования

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

Установленные правила межсетевого экрана приведены в таблице 48.

Таблица 48 – Установленные правила межсетевого экрана

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

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

* если используется контейнерная виртуализация **podman**.

2.2.5.1 Настройки правил внешнего межсетевого экрана

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

Во внешний контур должны быть доступны только следующие порты:

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

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

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

- 465/tcp;
- 587/tcp;

– порты на реальные IP серверов **ucs_mail**:

- 25/tcp.

2.3 Запуск установки

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

```
[root@ucs-installer ~/install_mailion]# ansible-playbook playbooks/main.yml --diff
```

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

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

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

После этого запускаются роли, описанные в разделе 2.2.1.

2.4 Проверка корректности установки

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

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

2.4.1 Добавление дополнительных доменов для обслуживания инсталляцией

В ПО «Mailion» добавлена поддержка дополнительных доменов. Чтобы добавить дополнительный домен необходимо добавить его в список `mailion_supported_domain`:

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

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

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

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

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

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

2.5 Установка клиента «МойОфис Почта»

2.5.1 Установка программы на ОС Windows

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

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

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

Подключение необходимо выполнять под учетной записью пользователя с правами администратора.

2.5.1.1 Установка с помощью MSI-пакета

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

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

В таблице ниже представлено подробное описание параметров установки.

Таблица 49 – Параметры установки ПО «МойОфис Почта»

Параметр	Описание
/i или /package	Установить ПО «МойОфис Почта».
<путь к дистрибутиву>	Расположение и имя файла пакета установки.
INSTALL_DIRECTORY_PATH=[path]	Абсолютный путь, указывающий место установки. Если используется параметр INSTALL_DIRECTORY_NAME , то этот параметр игнорируется.

Параметр	Описание
INSTALL_DIRECTORY_NAME=[name]	Название папки для установки, которая будет создана в папке Program Files .
TASKBAR_SHORTCUT={true,false}	Закрепить/не закреплять ярлык на панели задач в ОС Windows 7 или 8. По умолчанию true .
DESKTOP_SHORTCUT={true,false}	Создать/не создавать ярлык на рабочем столе. По умолчанию true .
START_MENU_SHORTCUT={true,false}	Создать/не создавать ярлык в меню «Пуск». По умолчанию true .
INSTALL_MAINTENANCE_SERVICE={true,false}	Включить/отключить установку сервиса поддержки Maintenance Service. По умолчанию true .
REMOVE_DISTRIBUTION_DIR={true,false}	Удалить/не удалять папку с дистрибутивом distribution из существующей установки. По умолчанию true .
PREVENT_REBOOT_REQUIRED={true,false}	Запретить/не запрещать перезагрузку компьютера в процессе установки. Включение данного параметра может привести к неполной установке ПО. По умолчанию false .
OPTIONAL_EXTENSIONS={true,false}	Включить/отключить установку расширений. По умолчанию true .
EXTRACT_DIR=[directory]	Папка для распаковки файлов приложения. Файлы распаковываются в указанную папку, и установка приложения не производится. Все остальные параметры установки игнорируются.
/m	Создать MIF-файл состояния.
/q, /quiet и /passive	Параметры отображения: – /q и /quiet – «тихий» режим, без взаимодействия с пользователем. – /passive – автоматический режим. Только указатель хода выполнения.
/norestart, /forcerestart и /promptrestart	Параметры перезагрузки: – /norestart – останавливает перезагрузку устройства после завершения установки. Используется по умолчанию. – /promptrestart – запрашивает пользователя, если требуется перезагрузка. – /forcerestart – перезапускает устройство после завершения установки.

Параметр	Описание
/L или /log	<p>Генерировать лог-файл (ведение журнала).</p> <p>Параметры:</p> <ul style="list-style-type: none"> – /L – путь к файлу журнала. – i – занесение в журнал сообщений о состоянии. – w – занесение в журнал не критических предупреждений. – e – занесение в журнал сообщений об ошибках. – a – занесение в журнал выполнения действий. – r – занесение в журнал записей со сведениями о действиях. – u – занесение в журнал запросов пользователей. – c – занесение в журнал исходных параметров пользовательского интерфейса. – m – занесение в журнал нехватки памяти. – p – занесение в журнал свойств терминала. – v – занесение в журнал подробных сведений. <p>Для использования параметра v следует задавать /L*v.</p> <ul style="list-style-type: none"> – + – добавление в существующий файл. – ! – сброс в журнал каждой строки. – * – занесение в журнал всех сведений, кроме параметра v. Это подстановочный знак. – Имя_файла_журнала.txt – имя и путь к текстовому файлу журнала.

Пример:

```
msiexec.exe /i "C:\Дистрибутивы\MyOffice_Mail_PSN_Windows_2.6.1.msi"
INSTALL_DIRECTORY_PATH="C:\MyOfficeMail\"
TASKBAR_SHORTCUT=false
DESKTOP_SHORTCUT=false
INSTALL_MAINTENANCE_SERVICE=false
/quiet
```

2.5.2 Установка приложения на ОС Linux

2.5.2.1 Установка дистрибутива sh

Перед началом установки разместите исполняемый файл дистрибутива `MyOffice_Mail_PSN_clean_Linux_x64_2.6.1.sh` в сетевой папке, доступной на рабочем месте пользователя, или в локальной папке на рабочем месте пользователя.

Если установка будет осуществляться локально, откройте терминал.

Если установка будет осуществляться удаленно, выполните следующие действия:

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

Для установки ПО «МойОфис Почта» выполните следующие действия:

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

```
chmod +x ./MyOffice_Mail_PSN_clean_Linux_x64_2.6.1.sh
```

3. Запустите выполнение файла дистрибутива:

```
./MyOffice_Mail_PSN_clean_Linux_x64_2.6.1.sh
```


4. Укажите **1**, чтобы начать процесс установки (см. Рисунок 2).

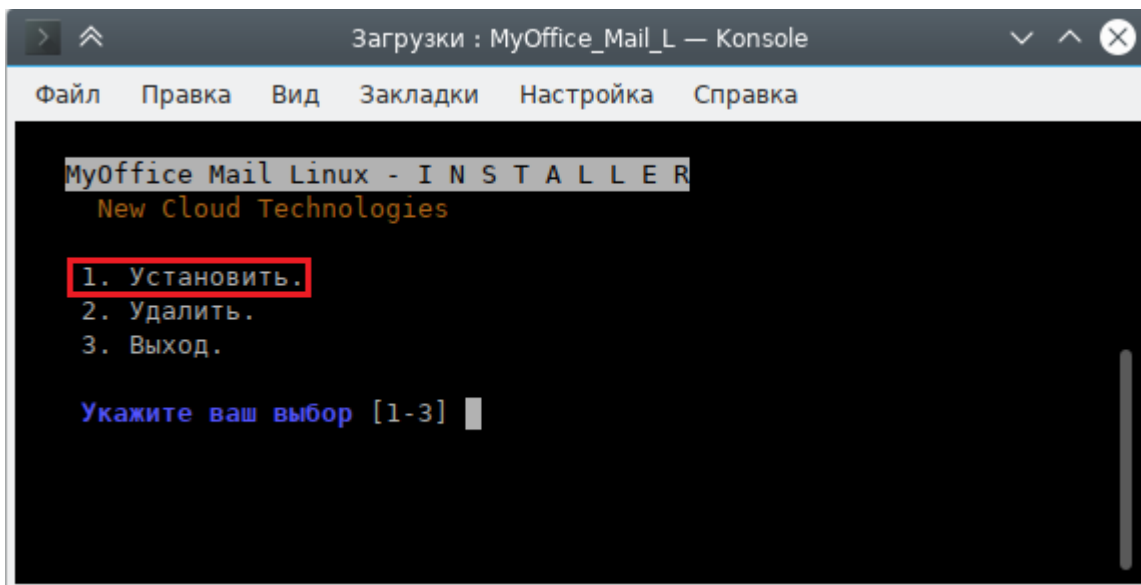


Рисунок 2 – Выбор основного сценария действий

5. Укажите **1**, чтобы прочитать лицензионное соглашение (см. Рисунок 3).

6. Укажите **2**, чтобы принять лицензионное соглашение и установить программу.

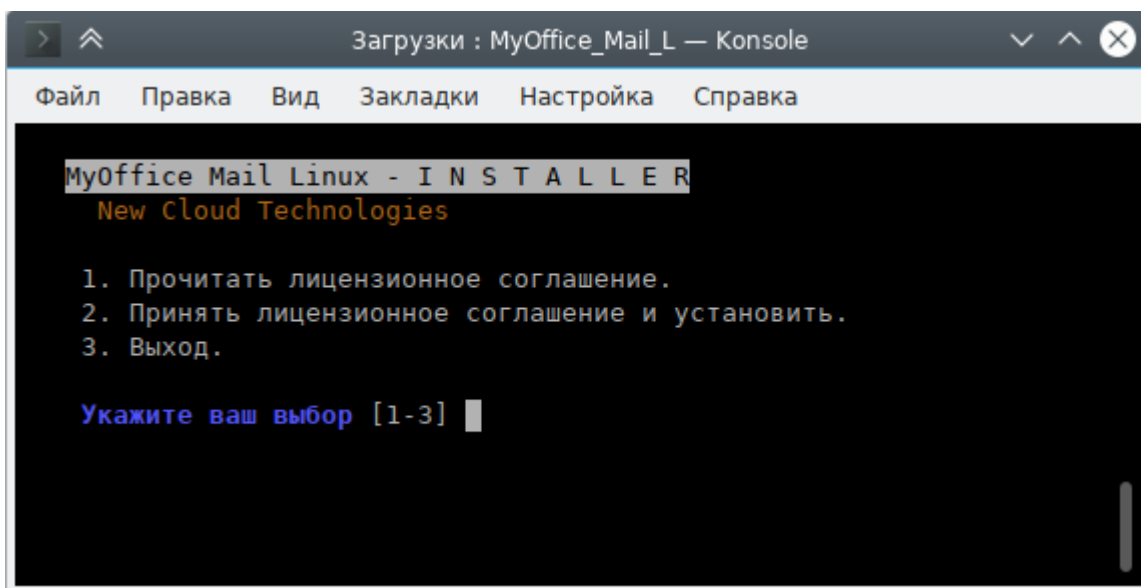


Рисунок 3 – Лицензионное соглашение и начало установки

7. При необходимости укажите папку для установки программы (см. Рисунок 4).

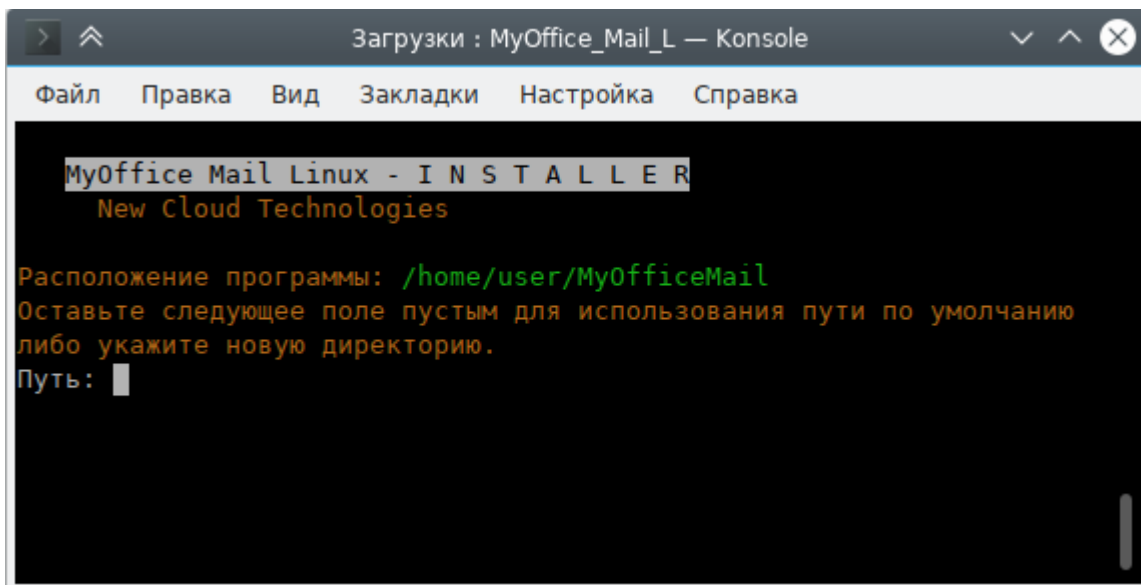


Рисунок 4 – Выбор папки для установки

8. Дождитесь полной установки компонентов программы (см. Рисунок 5).

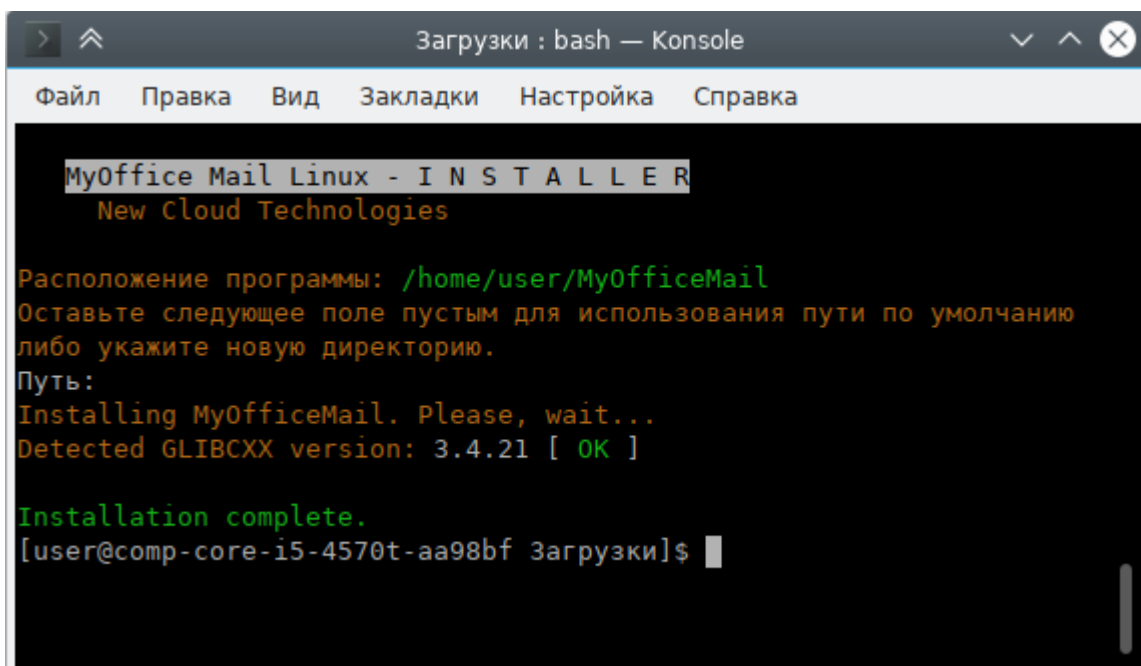


Рисунок 5 – Установка завершена успешно

2.5.2.2 Установка дистрибутива rpm

2.5.2.2.1 Установка rpm с помощью терминала

Установку приложения «МойОфис Почта» на ОС Linux (дистрибутив rpm) можно выполнить с помощью терминала или программы, предназначенной для установки пакетов.

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

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

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

```
sudo rpm -iU myofficemail-clean-2.6.1-17.x86_64.rpm
```

2.5.2.2.2 Установка rpm с помощью приложения установки

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

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

- Щелчком правой кнопки мыши откройте контекстное меню файла дистрибутива приложения «МойОфис Почта» и выберите пункт **Открыть в** [наименование программы] / **Открыть с помощью** [наименование программы] / **Открыть с помощью другого приложения** (см. Рисунок 6).

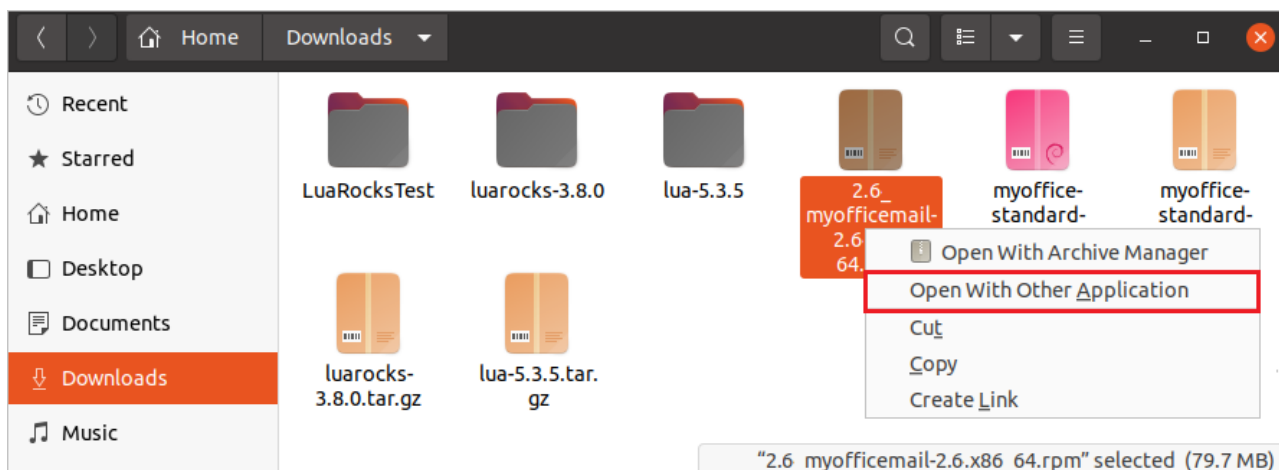


Рисунок 6 – Пример контекстного меню дистрибутива «МойОфис Почта»

Выберите приложение установки (см. Рисунок 7).

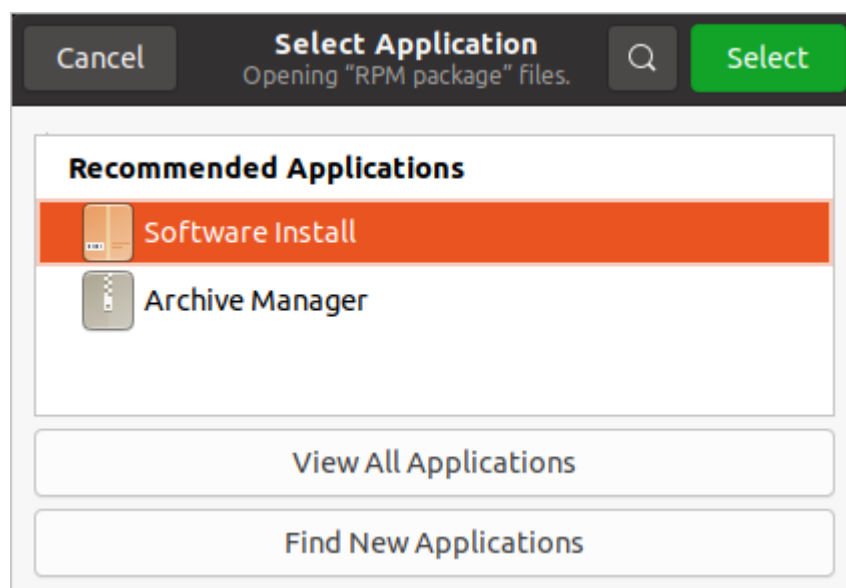


Рисунок 7 – Выбор приложения для открытия пакета **rpm**

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

2.6 Установка в составе других продуктов ПО «МойОфис»

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

3 ОБНОВЛЕНИЕ С ПРЕДЫДУЩИХ ВЕРСИЙ

Данный дистрибутив предназначен для установки с нуля. Обновления возможны с версии 1.3.2 и выше. Состав дистрибутива приведен в разделе 2.1.

Перед обновлением необходимо в файлах **group_vars/ucs_setup/*** проверить наличие новых переменных. Новые переменные находятся в файлах **contrib/mailion/cluster/group_vars/ucs_setup/*** (для «Standalone» инсталляции в **contrib/mailion/standalone/group_vars/ucs_setup/***).

Пример – При обновлении с версии 1.6 в файл **group_vars/ucs_setup/main.yml** необходимо добавить новый параметр в секцию **mongodb_management_users**:

```
ektor:  
# Generate it with: `pwgen 16 1`  
password: "Aiy5laetaixeicho"
```

Пароль необходимо сгенерировать командой **pwgen 16 1**.

В данном файле, в секции **mailion_service_accounts** необходимо проверить наличие переменной с паролем для **adonis**. Если она имеется, то убрать её.

Обновление ПО «Mailion» осуществляется аналогично установке новой версии, подробная информация по установке приведена в разделе 2.

Важно – Перед обновлением необходимо изменить значение переменной **mailion_release_name** на значение, аналогичное номеру актуального релиза.

Команда для запуска установки приведена в разделе 2.3.

4 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ И РЕКОМЕНДАЦИИ ПО УСТАНОВКЕ

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

4.1.1 ArangoDB

ArangoDB – система управления базами данных. Административная панель управления ArangoDB доступна по адресу `https://arangodb.<catalog_inventory_hostname>:8529`, где `<catalog_inventory_hostname>` – FQDN любого хоста из группы `ucs_catalog` (по умолчанию, там располагается сервис `arangodb_coordinator`) (см. Рисунок 8).

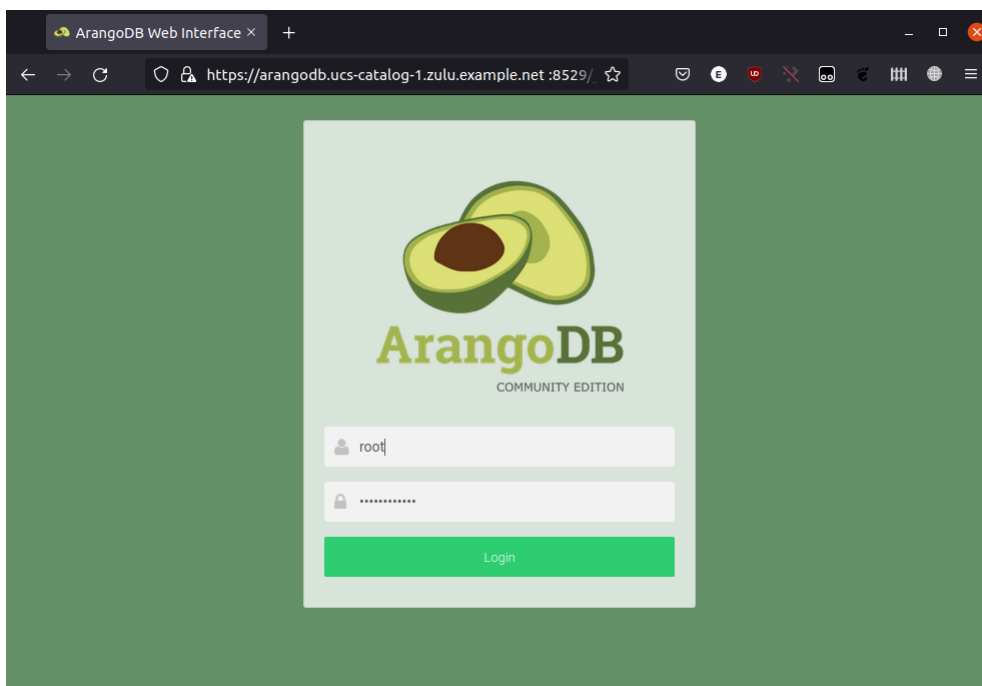


Рисунок 8 – Административная панель управления ArangoDB

Доступ в ArangoDB необходимо осуществлять по протоколу HTTPS из внутренней сети инсталляции.

Логинот является ключ `arangodb.users.root`, пароль – значение `arangodb_users.root.password`.

4.1.2 Rspamd

Rspamd – система управления антиспамом (конфигурация правил рейтингов, история обработки). Веб-интерфейс Rspamd доступен по адресу `http://rspamd.<mail_inventory_hostname>:11334/`, где `<mail_inventory_hostname>` – FQDN хоста из группы **ucs_mail** (см. Рисунок 9).

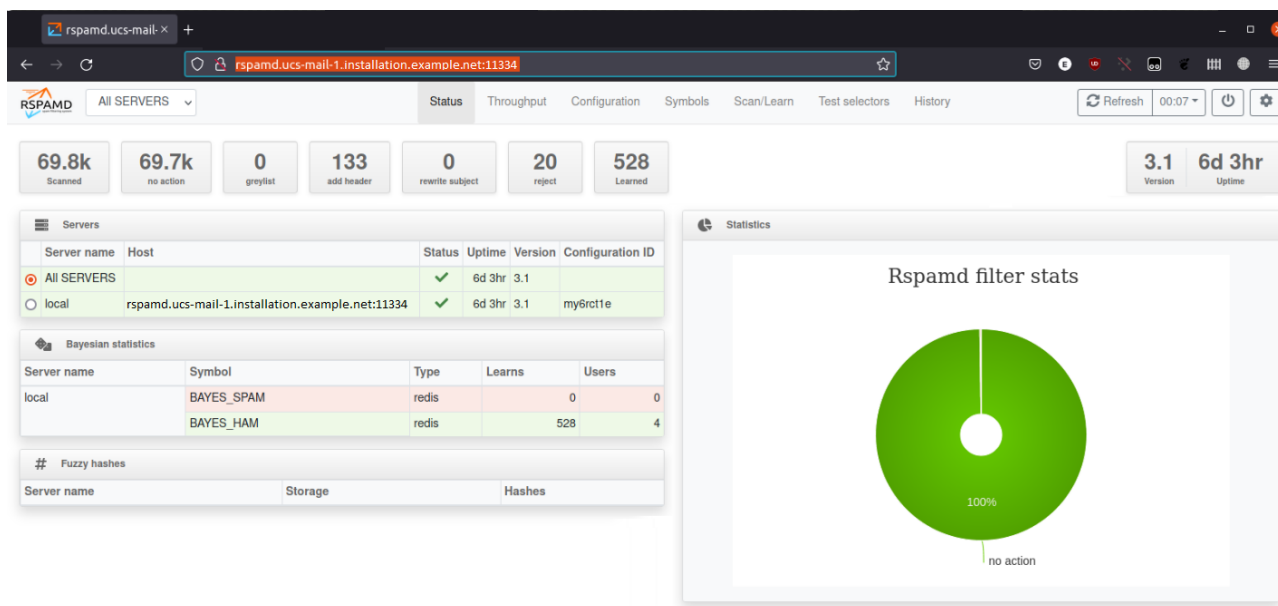


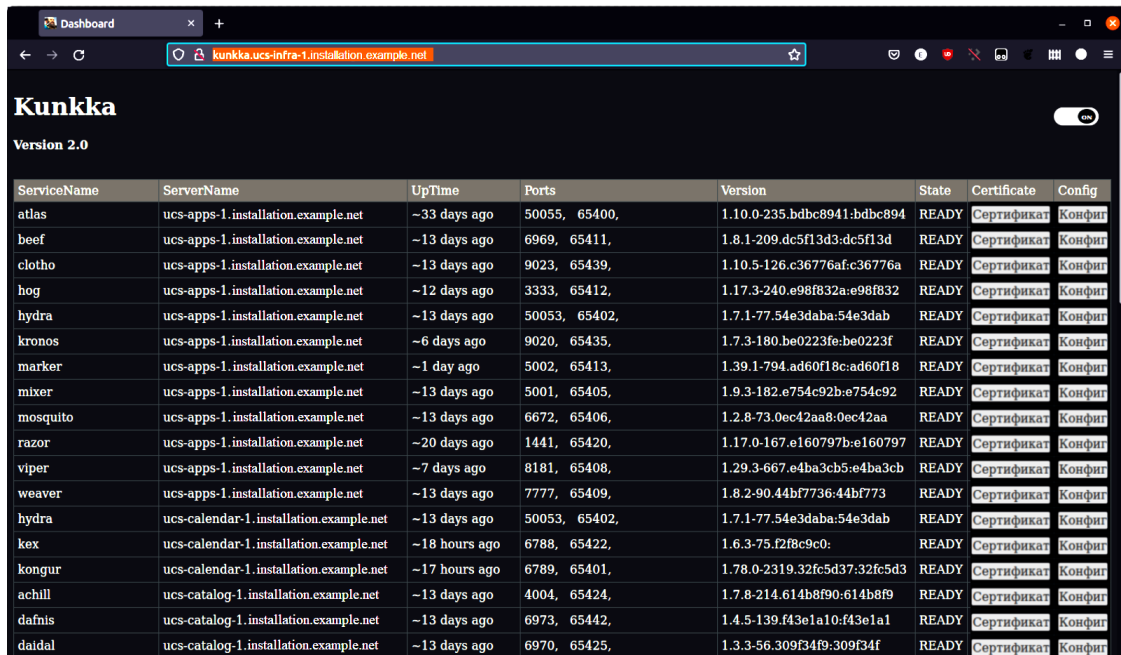
Рисунок 9 – Веб-интерфейс Rspamd

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

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

4.1.3 Kunkka

Kunkka – веб-страница с отображением подсистем на серверах. Веб-интерфейс Kunkka доступен по адресу `http://kunkka.<infrastructure_inventory_hostname>/`, где `<infrastructure_inventory_hostname>` – FQDN хоста группы **ucs_infrastructure** (см. Рисунок 10).



The screenshot shows a web browser window with the URL `kunkka.ucs-infra-1.installation.example.net`. The page title is "Kunkka" and the version is "Version 2.0". Below the header is a table with the following columns: ServiceName, ServerName, UpTime, Ports, Version, State, Certificate, and Config. The table lists 20 services, all with a "READY" state and "Сертификат" (Certificate) and "Конфиг" (Config) buttons.

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

Рисунок 10 – Веб-интерфейс Kunkka

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

4.1.4 Prometheus

Prometheus – система мониторинга. Веб-интерфейс Prometheus доступен по адресу `http://prometheus.<infrastructure_inventory_hostname>/`, где `<infrastructure_inventory_hostname>` – FQDN хоста группы `ucs_infrastructure` (см. Рисунок 11).

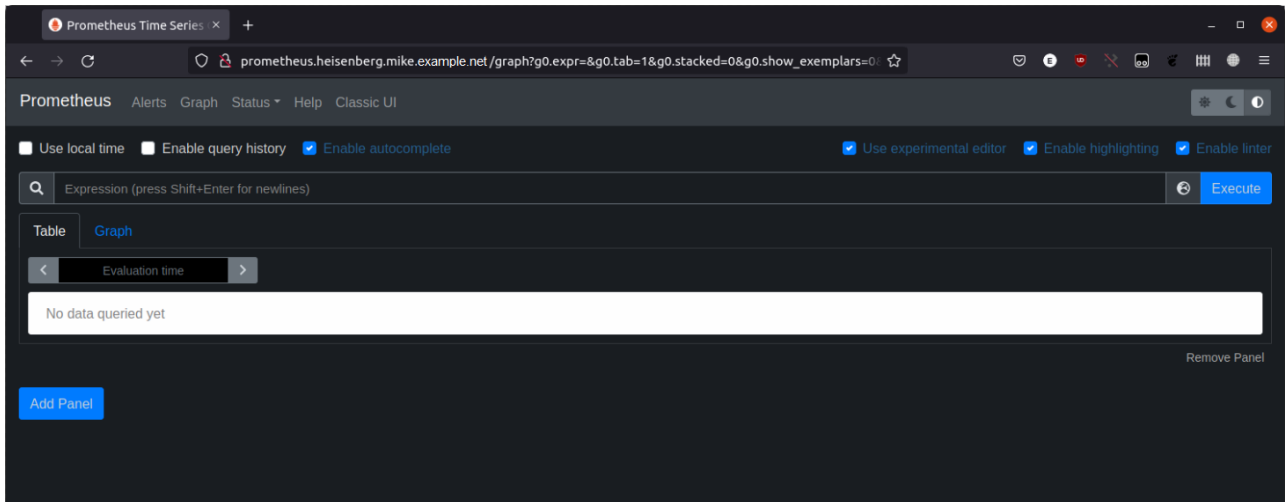


Рисунок 11 – Веб-интерфейс Prometheus

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

4.1.5 Alertmanager

Alertmanager – система алертинга. Веб-интерфейс Alertmanager доступен по адресу `http://alertmanager.<infrastructure_inventory_hostname>/`, где `<infrastructure_inventory_hostname>` – FQDN хоста группы **ucs_infrastructure** (см. Рисунок 12).

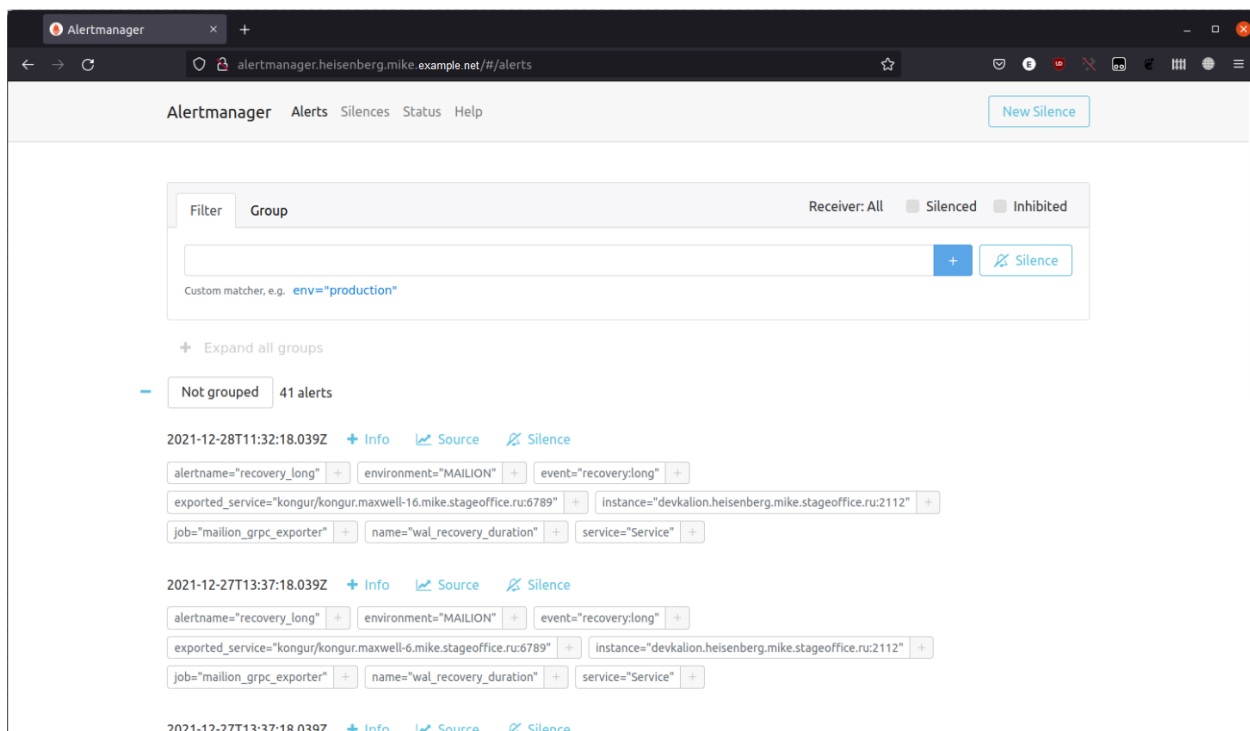


Рисунок 12 – Веб-интерфейс Alertmanager

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

4.1.6 Grafana

Grafana – система отображения метрик. Веб-интерфейс Grafana доступен по адресу `http://grafana.<infrastructure_inventory_hostname>`, где `<infrastructure_inventory_hostname>` – FQDN хоста группы **ucs_infrastructure** (см. Рисунок 13).

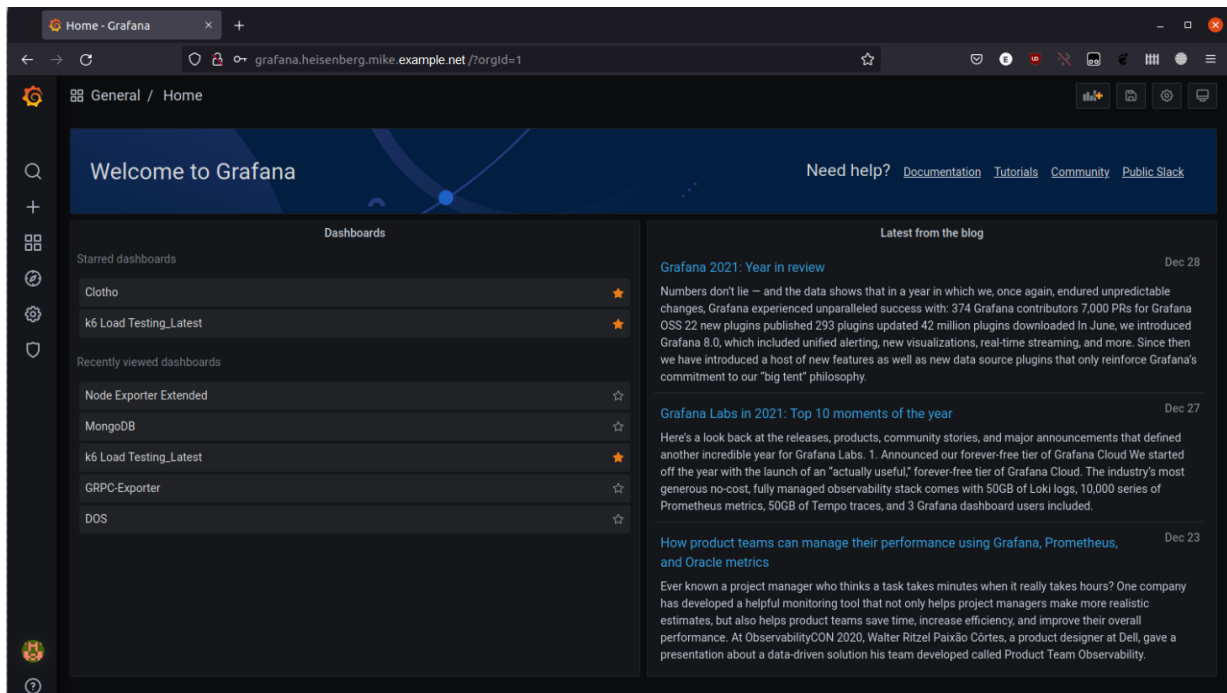


Рисунок 13 – Веб-интерфейс Grafana

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

4.2 Настройка взаимодействия со службой каталогов

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

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

Корректно заполненные параметры приведены ниже.

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

```
bind_password: "adUserPassword"
name: "AD"
servers:
  - endpoint: "dc.example.net:636"
    tls:
      ca_filename: "ca_example.net.pem"
      cert_file: ""
      key_file: ""
      use_tls: true
    use_dc: false
freeipa:
  "zuif6jeifiQueey5ahWato0o":
    dcs:
      base_dn: "dc=ipa-example,dc=net"
      bind_user: "uid=admin,cn=users,cn=accounts,dc=ipa-example,dc=net"
      bind_password: "adminPassword"
      name: "FreeIPA"
      servers:
        - endpoint: "freeipa.ipa-example.net:389"
          tls:
            ca_filename: ""
            cert_file: ""
            key_file: ""
            use_tls: false
          use_dc: false
samba_dc:
  "PeZh0WisXah5thooWhoo9bgG":
    smb:
      base_dn: "DC=samba-dc-test,DC=example,DC=com"
      bind_user: "Administrator"
      bind_password: "ahTh6uu7sah4so1C"
      name: "SAMBA_DC"
      servers:
        - endpoint: "samba-dc-test.example.com:389"
          tls:
            ca_filename: ""
            cert_file: ""
            key_file: ""
            use_tls: false
          use_dc: false
aldpro:
  "ALDh9ZisXah5thooWhoo9bgZ":
    ald:
      base_dn: "DC=domain,DC=test"
      bind_user: "admin"
      bind_password: "ahTh6uu7sah4so1C"
      name: "ALDPRO"
      servers:
```

```
- endpoint: "aldpro-test.example.com:389"
  tls:
    ca_filename: ""
    cert_file: ""
    key_file: ""
    use_tls: false
  use_dc: false
```

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

```
mailion_integrations:
  microsoft: true
```

Для включения интеграции с FreeIPA необходимо указать в групповых переменных:

```
mailion_integrations:
  freeipa: true
```

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

```
mailion_integrations:
  aldpro: true
```

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

```
mailion_integrations:
  samba_dc: true
```

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

4.3 Настройка антивирусного программного обеспечения

В ПО «Mailion» **Rspamd** поддерживает несколько сторонних антивирусных модулей, в том числе KSE (Kaspersky). Настройка данного модуля осуществляется через переменные роли **Rspamd**. Подробное описание этих ролей приведено в таблицах 50 и 51.

Таблица 50 – Настройка Rspamd role vars

Параметр	Пример заполнения	Описание
rspamd:		
kse_use_https:	false	Использование https для подключения к серверам Касперского

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

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

Таблица 51 – Настройка Rspamd role vars

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

Важно – Продукт Kaspersky Scan Engine не является частью поставки ПО «Mailion».

4.4 Настройка сервиса Vault

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

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

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

4.4.1 Установка сервиса Vault

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

Для этого необходимо установить и запустить первый экземпляр Vault.

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

4.4.1.1 Этапы установки

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

Пример – Если доменное имя **vault.example.ru**, то сертификаты должны быть выпущены либо на домен **vault.example.ru**, либо на ***.example.ru**. В последнем случае допустимо использовать сертификаты, уже подготовленные для инсталляции Mailion (см. раздел 3.2.2.4):

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

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

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

6. Выполнить команду установки:

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

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

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

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

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

4.4.1.2 Настройка Vault AppRole и доступа к кластеру для приложений

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

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

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

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

4.4.1.3 Инициализация секретов

Чтобы создать список секретов, необходимо выполнить следующие действия:

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

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

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

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

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

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

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

4. Также необходимо проанализировать `inventory` файл на наличие открытых паролей, указанных в открытом виде. В случае наличия таковых, можно поменять значения для них на маскированные значения и добавлять свои секреты в Vault. Подробная информация приведена в Приложении Б. Настройки `inventory` файла для работы с Vault.
5. В веб-браузере зайти на сервис Vault, используя полный адрес с портом.
6. Аутентифицироваться, используя `root` токен, полученный на этапе инициализации сервиса Vault.
7. Перейти во вкладку **Secrets**, в списке секретов перейти на **mailion** и далее на **installation**. Путь для секретов – **mailion/installation**.
8. Нажать кнопку **Create new version** и заполнить в соответствии с полученными ранее секретами.
9. Создать секрет **vault_token** в качестве значения, указать токен для доступа приложений, полученный ранее на этапе настройки Vault AppRole (см. раздел 4.4.1.2).
10. Для удобства можно заполнить в виде файла в формате JSON. Для этого есть специальная кнопка **JSON**, нужно ее включить.

4.4.1.4 Настройка `.ansible.cfg` для доступа к развернутому Vault-серверу

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

```
[hashi_vault_collection]
token_path = /Users/user/projects/secrets/
token_file = vault.token # Внутри файла необходимо указать токен для приложений,
полученный ранее на этапе настройки Vault AppRole
url = https://vault.server.company:8200 # URL, где будет доступен hosted vault – в случае с
НА vault достаточно одного из инстансов
```

4.4.1.5 Подготовка `inventory` файла

Для дальнейшей установки ПО «Mailion» необходимо подготовить `inventory` файл. Подробная информация приведена в Приложении Б. Настройки `inventory` файла для работы с Vault.

4.4.2 Установка на другие хосты

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

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

4.4.3 Создание доменных имен

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

- vault1.stageoffice.ru;
- vault2.stageoffice.ru;
- vault3.stageoffice.ru.

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

```
- type: "transparent"
  zone: "vault1.stageoffice.ru"
  local_data:
    - domain: "vault1.stageoffice.ru"
      type: "A"
      ip: "192.168.0.1"
- type: "transparent"
  zone: "vault2.stageoffice.ru"
  local_data:
    - domain: "vault2.stageoffice.ru"
      type: "A"
      ip: "192.168.0.2"
- type: "transparent"
  zone: "vault3.stageoffice.ru"
  local_data:
    - domain: "vault3.stageoffice.ru"
      type: "A"
      ip: "192.168.0.3"
```

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

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

Секции IP-адресов необходимо установить на соответствующие устанавливаемой конфигурации.

4.4.4 Генерация CA сертификата

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

В результате должны получиться три файла:

- server.crt;
- server.key;
- ca.pem.

4.4.5 Создание сертификатов для каждого инстанса

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

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

Если файлы в двоичном формате:

```
#для server.crt необходимо использовать:  
openssl x509 -inform DER -outform PEM -in server.crt -out server_cert.pem  
  
#для server.key необходимо использовать:  
openssl rsa -inform DER -outform PEM -in server.key -out server_key.pem
```

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

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

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

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

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

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

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

4.4.6 Настройка конфигурационного файла Vault для каждого инстанса

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

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

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

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

```
ssh infra # машина в кластере Mailion, на которой запущен первый Vault-инстанс

cat << HERE > /srv/docker/vault/config/vault.hcl

cluster_addr = "https://192.168.0.1:8201"
api_addr = "https://192.168.0.1:8200"
disable_mlock = true
ui = true

listener "tcp" {
  address = "0.0.0.0:8200"
  tls_client_ca_file = "/opt/vault/tls/ca.pem"
```

```
tls_cert_file = "/opt/vault/tls/server.pem"
tls_key_file = "/opt/vault/tls/server_key.pem"
}

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

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

ui = true

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

```
# секция raft содержит в себе ссылки на _все_ инстансы Vault,  
# доступные в кластере (включая инстанс, который установлен на данном хосте)  
storage "raft" {  
  path = "/opt/vault/data"  
  node_id = "vault2.stageoffice.ru"  
  
  retry_join {  
    leader_tls_servername = "vault1.stageoffice.ru"  
    leader_api_addr       = "https://192.168.0.1:8200"  
    leader_ca_cert_file   = "/opt/vault/tls/ca.pem"  
    leader_client_cert_file = "/opt/vault/tls/server.pem"  
    leader_client_key_file = "/opt/vault/tls/server_key.pem"  
  }  
  retry_join {  
    leader_tls_servername = "vault2.stageoffice.ru"  
    leader_api_addr       = "https://192.168.0.2:8200"  
    leader_ca_cert_file   = "/opt/vault/tls/ca.pem"  
    leader_client_cert_file = "/opt/vault/tls/server.pem"  
    leader_client_key_file = "/opt/vault/tls/server_key.pem"  
  }  
  retry_join {  
    leader_tls_servername = "vault3.stageoffice.ru"  
    leader_api_addr       = "https://192.168.0.3:8200"  
    leader_ca_cert_file   = "/opt/vault/tls/ca.pem"  
    leader_client_cert_file = "/opt/vault/tls/server.pem"  
    leader_client_key_file = "/opt/vault/tls/server_key.pem"  
  }  
}  
HERE
```

4.4.7 Рестарт, распечатка первого инстанса Vault

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

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


4.4.8 Запуск и распечатка остальных экземпляров Vault

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

Важно – Инициализация для данных экземпляров не требуется.

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

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

Для распечатки необходимо следовать процедуре, описанной в разделе 4.4.7. Использовать те же ключи распечатки, которые использовали для распечатки первого экземпляра. Пример **systemd** конфигурации для сервиса Vault (выполняется с помощью команды **nano /etc/systemd/system/vault.service**):

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

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

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

Запуск через systemd:

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

```
systemctl status vault.service
```

4.4.9 Верификация работы кластера

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

Необходимо авторизоваться с токеном, который был получен ранее:

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

Затем проверить статус хранилища:

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

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

4.4.10 Настройка стенда Mailion

Для интеграции с Vault-кластером необходимо перед установкой системы настроить inventory файл, указав через запятую список доступных Vault-инстансов, например в `group_vars/ucs_setup/main.yml`:

```
vault_integration:
  VAULT_TOKEN: "{{ vault_secrets['vault_token'] }}"
  VAULT_ADDRESS:
    "https://vault1.stageoffice.ru,https://vault2.stageoffice.ru,https://vault3.stageoffice.ru"
  VAULT_KV_VERSION: "v1"
  VAULT_SECRET_PATH: "mailion/data/stages/yankee/installation"
```

4.5 Рекомендации по безопасности

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

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

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

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

- type: "transparent"
  zone: "www.arangodb.com"
  local_data:
    - domain: "www.arangodb.com"
      type: "A"
      ip: "192.168.115.63"

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

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

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

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

4.6 Рекомендации по версии ядра Linux

Требуется ядро `mainline` (обновляется по умолчанию, если не передан флаг **UPGRADE_KERNEL=false**). С более старыми версиями ядер (lts) работоспособность не гарантируется из-за особенностей **Docker** (требуется полная поддержка `sgroup2` в ядре).

5 ПОДГОТОВКА К РАБОТЕ

5.1 Доступ к ПО «Mailion»

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

5.2 Запуск системы

Для запуска ПО «Mailion» необходимо выполнить следующие действия:

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

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

1. Проверить выполнение системных требований и, при необходимости, обратиться к системному администратору.
2. Установить и настроить следующее программное обеспечение в соответствии с инструкцией производителя (ООО "КРИПТО-ПРО"):
 - КриптоПро CSP (поддерживаемую версию согласно системным требованиям);
 - Библиотеку КриптоПро PKCS#11.
3. Если подготовка к работе с приложением «МойОфис Почта» осуществляется на ОС Windows, в registry необходимо сделать следующие изменения: в ветке `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\CryptoPro\Cryptography\CurrentVersion\PKCS11\slot0` (для 64-разрядной ОС) или `HKEY_LOCAL_MACHINE\SOFTWARE\CryptoPro\Cryptography\CurrentVersion\PKCS11\slot0` (для 32-разрядной ОС) создать строковый параметр с именем **Firefox**, не меняя остальные значения.

4. Установить приложение «МойОфис Почта» так, как это описано в разделе 2.5.
5. Запустить приложение и ввести данные той учетной записи, от имени которой будет осуществляться работа на текущем компьютере.
6. Добавить личный сертификат авторизованного пользователя так, как это описано в разделе 2.1.1 документа «Программное обеспечение «Корпоративная система электронной почты и планирования совместной работы команд «Mailion». Руководство оператора» RU.29144487.506900.001 34.

5.3 Проверка работоспособности системы

ПО «Mailion» считается работоспособным, если в результате действий пользователя, изложенных в разделах 5.1 и 5.2, на экране монитора отобразилась стартовая страница для входа в ПО «Mailion» без выдачи сообщений о сбое в работе (см. Рисунок 14).

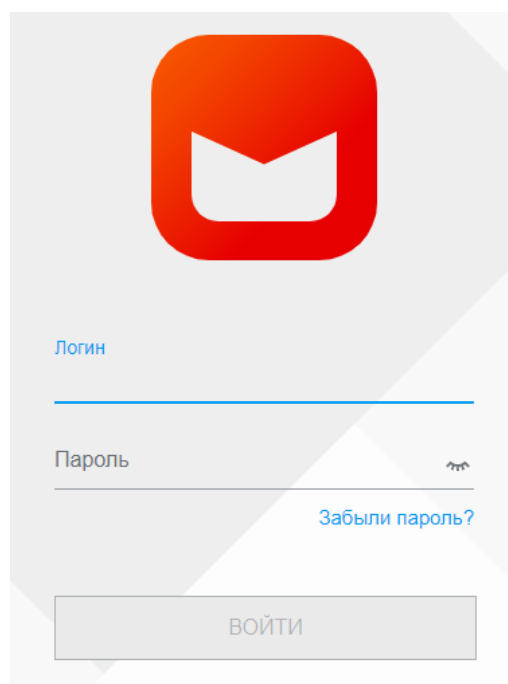


Рисунок 14 – Стартовая страница для входа в ПО «Mailion»

Приложение «МойОфис Почта» для ОС Windows считается работоспособным, если в результате действий, изложенных в разделе 2.5.1, на рабочем столе (см. Рисунок 15) и в главном меню ОС отображается ярлык, при активации которого программа корректно открывается без выдачи сообщений о сбое в работе.

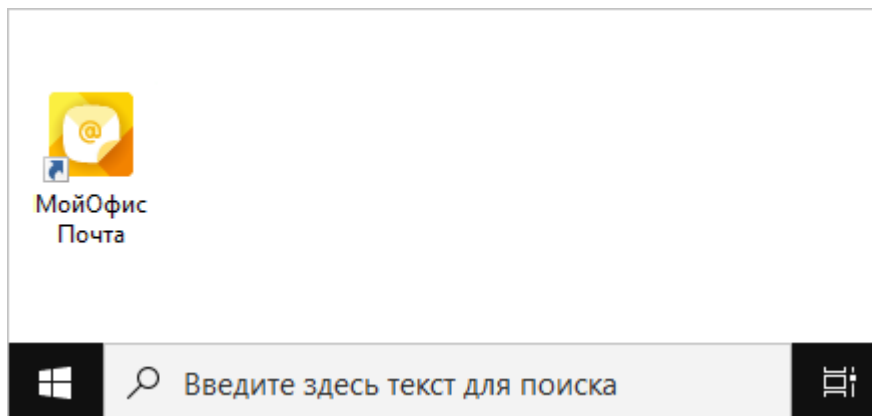


Рисунок 15 – Ярлык ПО «МойОфис Почта» на рабочем столе ОС Windows

Приложение «МойОфис Почта» для ОС Linux считается работоспособным, если в результате действий, изложенных в разделе 2.5.2, в меню приложений ОС (см. Рисунки 16, 17) отображается ярлык, при активации которого программа корректно открывается без выдачи сообщений о сбое в работе.

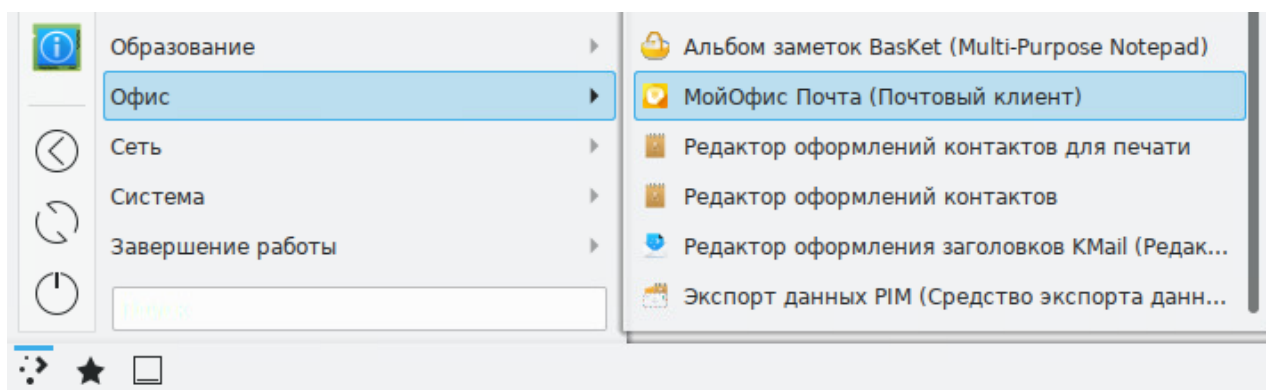


Рисунок 16 – Ярлык ПО «МойОфис Почта» в меню приложений ОС Linux

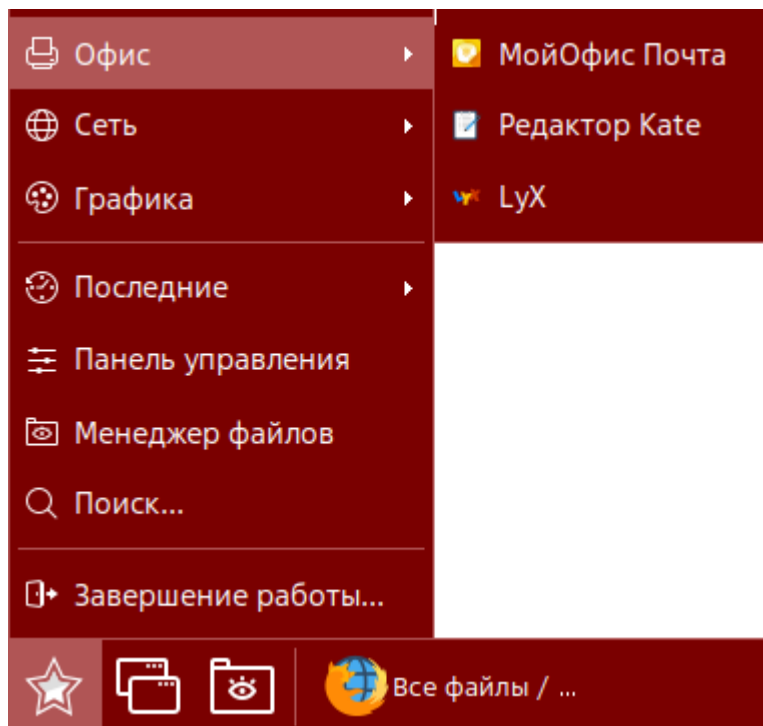



Рисунок 17 – Ярлык ПО «МойОфис Почта» в меню приложений ОС Astra Linux Special Edition

6 РАБОТА В ПАНЕЛИ АДМИНИСТРИРОВАНИЯ

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

Для перехода к работе с панелью администрирования ПО «Mailion» необходимо нажать на значок  в меню приложений (см. Рисунок 18).

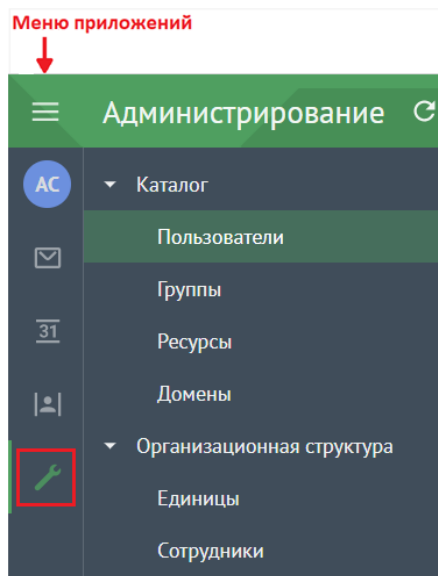


Рисунок 18 – Переход к Панели администрирования

6.1 Интерфейс приложения Панель администрирования

Интерфейс приложения **Панель администрирования** включает следующие элементы (см. Рисунок 19):

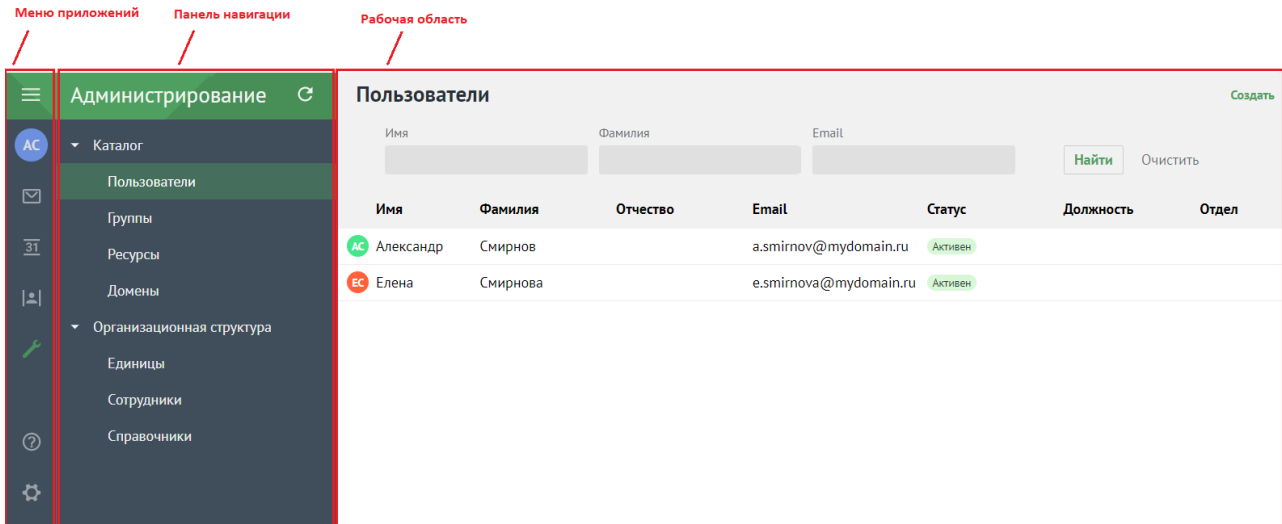


Рисунок 19 – Интерфейс приложения Панель администрирования

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

3. Рабочая область с содержимым выбранного раздела.

В верхней области Панели администрирования находится область с полями для поисковых запросов (см. Рисунок 20).

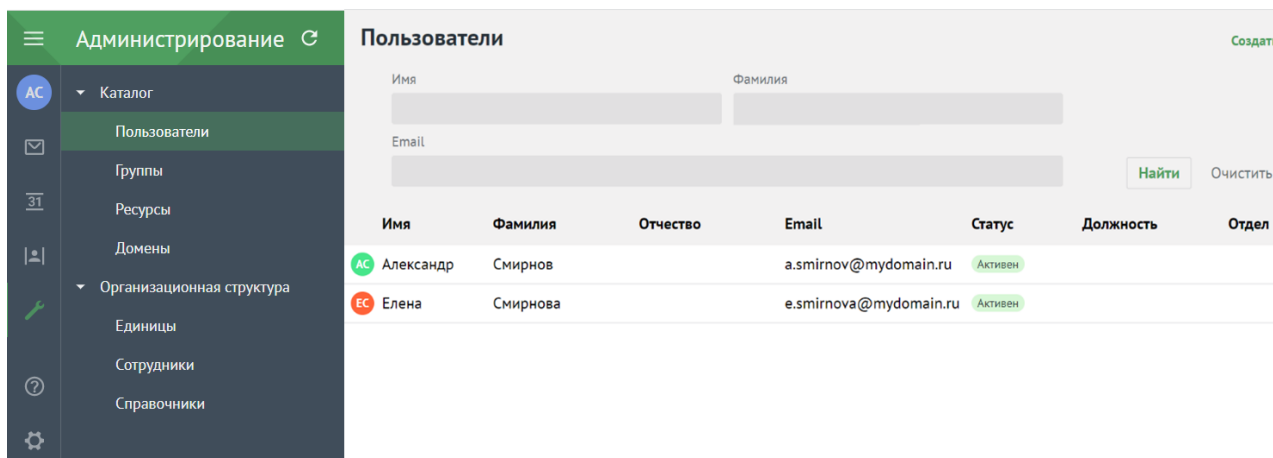


Рисунок 20 – Просмотр полей для поиска

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

6.2 Управление пользователями

6.2.1 Просмотр списка пользователей

Для просмотра списка пользователей необходимо авторизоваться в ПО «Mailion» и перейти в раздел **Пользователи**. После этого отобразится таблица с записями о пользователях и их параметрах (см. Рисунок 21):

- Имя;
- Фамилия;
- Отчество;
- E-mail;
- Статус;
- Должность;
- Отдел;
- Город;

– Логин.

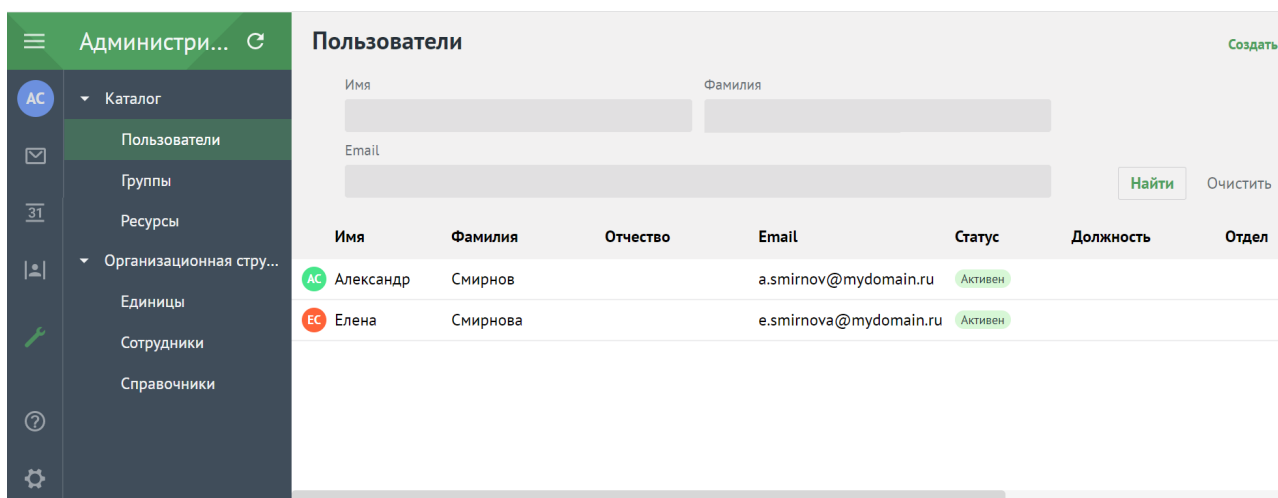


Рисунок 21 – Просмотр списка пользователей

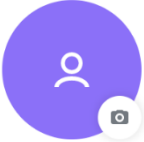
6.2.2 Просмотр записи о пользователе

Чтобы просмотреть подробную запись о пользователе, необходимо нажать на соответствующую строку и перейти на вкладку **Данные**. На этой же вкладке доступно редактирование записи о пользователе.

6.2.3 Создание пользователя

Для создания нового пользователя в разделе **Пользователи** необходимо нажать на кнопку **Создать** и в открывшейся форме выполнить следующие действия (см. Рисунок 22):

Новый пользователь



Личные данные

Имя (обязательно)	Отчество	
<input type="text"/>	<input type="text"/>	
Фамилия	Дата рождения	Пол
<input type="text"/>	<input type="text"/>	Не указан ▾

Аутентификация

Логин (обязательно)	Домен
<input type="text"/>	mydomain.ru ▾

Пароль (обязательно)
 Сгенерировать автоматически

[Копировать пароль](#)

[Добавить логин](#)

Почтовый ящик

Основной email (обязательно)	Домен
<input type="text"/>	mydomain.ru

[Добавить алиас](#)

Контакты

Резервный email

Телефон
 Рабочий ▾

[Добавить телефон](#)

Адреса

Название адреса

Страна	Город
<input type="text"/>	<input type="text"/>

Адрес	Индекс
<input type="text"/>	<input type="text"/>

Этаж
 Если несколько, разделять через « ; »

Кабинет
 Если несколько, разделять через « ; »

Место
 Если несколько, разделять через « ; »

Рисунок 22 – 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** (не более 10 учетных записей для одного пользователя) вручную с клавиатуры:
 - Логин. Можно ввести логин на латинице или кириллице;
 - Пароль. Можно придумать новый пароль пользователя и подтвердить его, либо использовать пароль, предложенный автоматическим генератором;
 - Повторите пароль.
3. Заполнить поле блока **Почтовый ящик** (не более 11 адресов электронной почты для одного пользователя) вручную с клавиатуры:
 - Основной E-mail. Можно ввести E-mail на латинице или кириллице;
 - Алиас. Для этого необходимо нажать на кнопку **Добавить алиас**.
4. Заполнить поля блока **Контакты** (опционально; не более 10 номеров телефонов различного назначения для одного пользователя) вручную с клавиатуры:
 - Резервный E-mail;
 - Телефон;
 - Тип телефона (выбрать из раскрывающегося списка).
5. Заполнить блок **Адреса** (опционально) вручную с клавиатуры:
 - Название адреса;
 - Страна;
 - Город;
 - Адрес;
 - Индекс;
 - Этаж;
 - Кабинет;
 - Место.

6. Заполнить поля блока **Организационная структура** (опционально) вручную с клавиатуры:

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

Важно – Для заполнения полей данного блока необходимо предварительно создать объекты организационной структуры (см. раздел 6.6).

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

Важно – В случае сбоя в процессе добавления пользователя данные сохраняются в систему, 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 7).

6.2.4 Поиск пользователя

Для поиска пользователя необходимо выполнить следующие действия:

1. В разделе **Пользователи** заполнить одно или несколько полей **Имя**, **Фамилия**, **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** (см. Рисунок 23).

The screenshot shows the 'Пользователи' (Users) management interface. At the top right is a 'Создать' (Create) button. Below it is a search bar with three input fields: 'Имя' (Name), 'Фамилия' (Surname), and 'Email'. The 'Фамилия' field contains 'Смирнов' and the 'Email' field contains 'mydomain'. To the right of these fields are 'Найти' (Find) and 'Очистить' (Clear) buttons. Below the search bar is a table with columns: 'Имя', 'Фамилия', 'Отчество', 'Email', 'Статус', 'Должность', 'Отдел', and 'Город'. The table contains two rows of user data.

Имя	Фамилия	Отчество	Email	Статус	Должность	Отдел	Город
Александр	Смирнов		a.smirnov@mydomain.ru	Активен			
Елена	Смирнова		e.smirnova@mydomain.ru	Активен			

Рисунок 23 – Поиск группы рассылки

3. Выбрать необходимого пользователя из динамически формируемого списка в области отображения найденных пользователей.

6.2.5 Блокировка и разблокировка пользователя

Для блокировки пользователя необходимо выбрать пользователя из общего списка и нажать на **Заблокировать** (см. Рисунок 24). После этого сессии пользователя в системе будут прерваны и вход в систему будет невозможен.

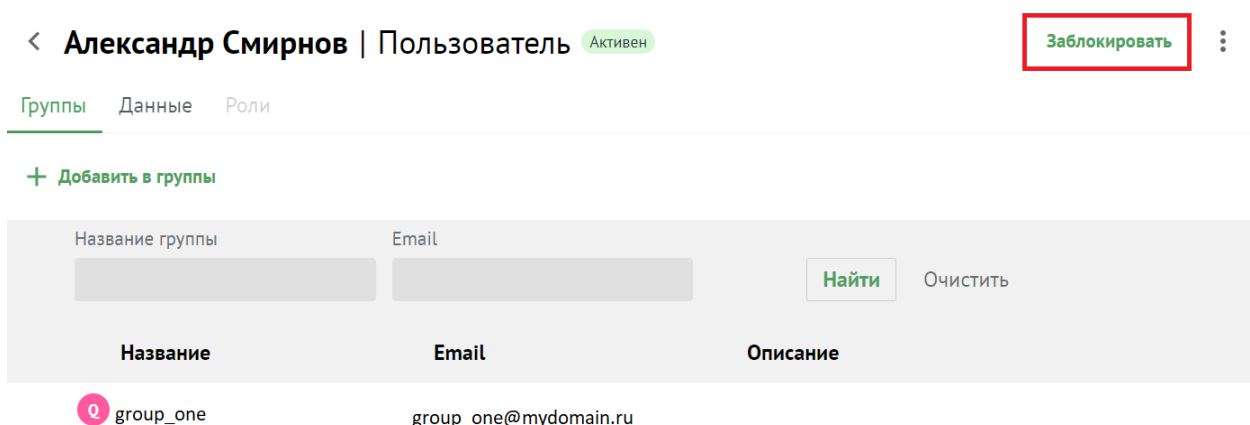


Рисунок 24 – Блокировка пользователя

Для разблокировки пользователя необходимо выбрать пользователя из общего списка и нажать на **Разблокировать** (см. Рисунок 25). После этого статус пользователя будет изменен.

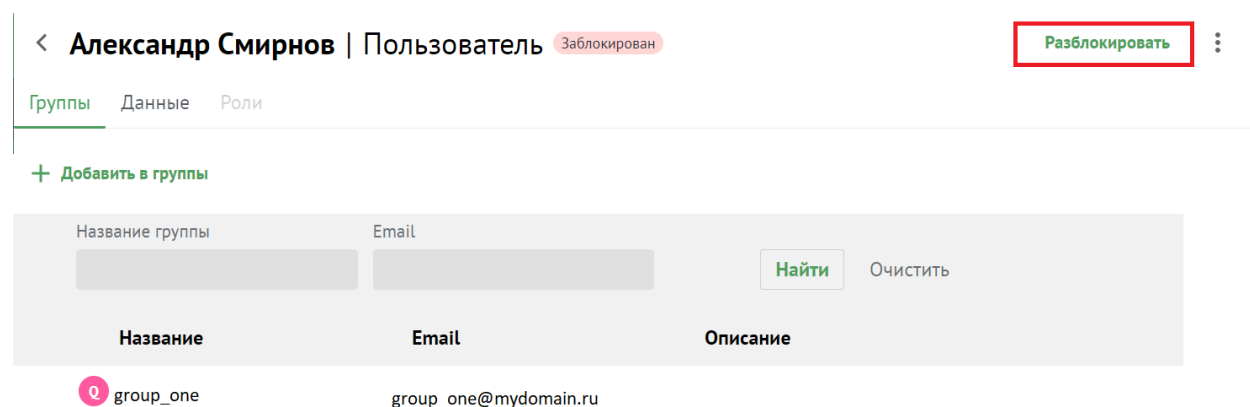


Рисунок 25 – Разблокировка пользователя

6.2.6 Удаление пользователя

Для удаления пользователя необходимо выполнить следующие действия:

1. Выбрать пользователя из общего списка и нажать на значок ⋮ .
2. Нажать на **Удалить** (см. Рисунок 26).

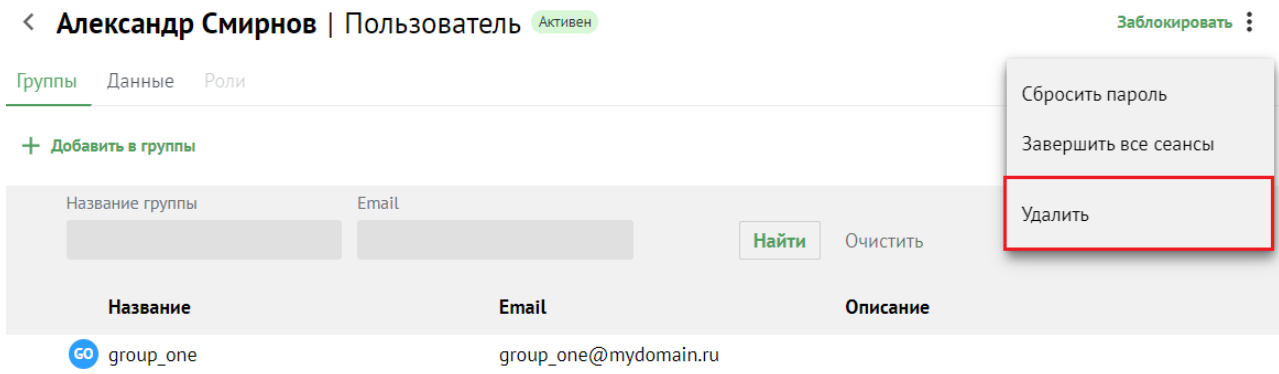


Рисунок 26 – Удаление пользователя

3. В окне подтверждения удаления необходимо нажать на кнопку **Удалить** (см. Рисунок 27).

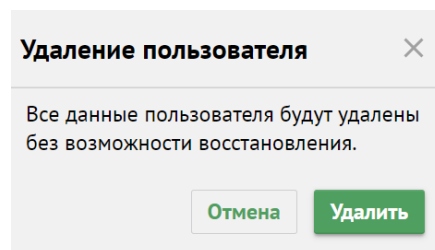


Рисунок 27 – Подтверждение удаления пользователя

6.2.7 Сброс пароля пользователя

Для сброса пароля пользователя необходимо выбрать пользователя из общего списка и нажать на **Сбросить пароль** (см. Рисунок 28).

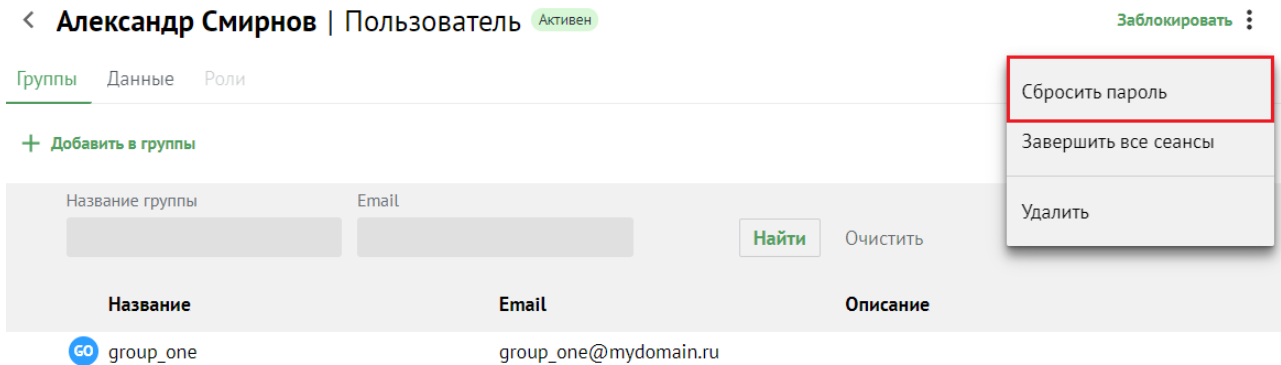


Рисунок 28 – Сброс пароля пользователя

После нажатия на кнопку **Сбросить пароль**, администратор должен ввести новый пароль пользователя и подтвердить его, либо использовать пароль, предложенный автоматическим генератором (см. Рисунок 29).

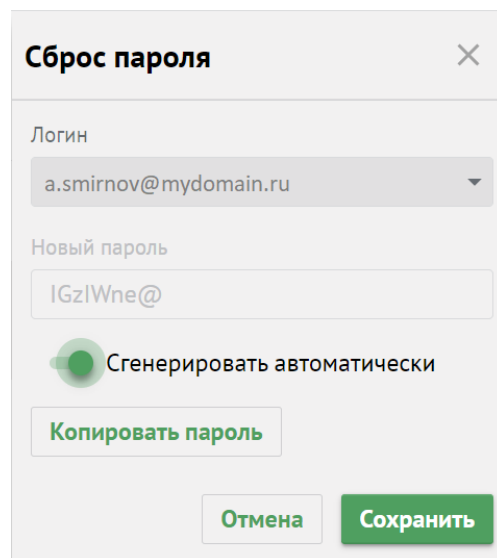


Рисунок 29 – Сгенерировать пароль автоматически

6.2.8 Завершение всех сеансов пользователя

Для завершения всех сеансов пользователя необходимо выбрать пользователя из общего списка и нажать на **Завершить все сеансы** (см. Рисунок 30).

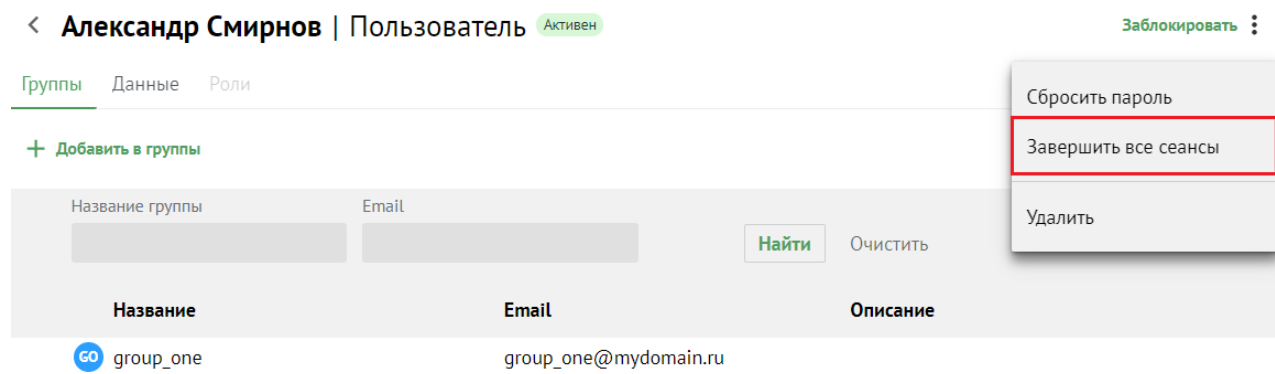


Рисунок 30 – Сброс пароля пользователя

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

6.2.9 Изменение членства пользователя в группах рассылки

Администратор ПО «Mailion» может исключить пользователя из групп рассылки или добавить в них.

Добавить пользователя в группу рассылки можно несколькими способами:

- В списке пользователей навести курсор мыши на запись о пользователе и нажать на кнопку **Добавить в группу** (см. Рисунок 31).

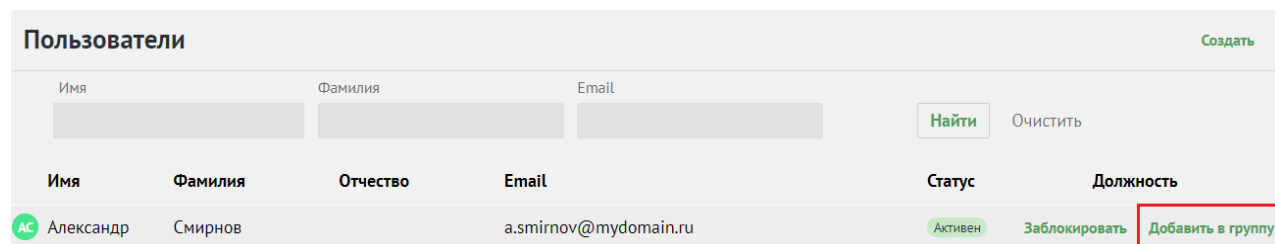


Рисунок 31 – Добавить пользователя в группы рассылки (1)

- При просмотре записи о пользователе на вкладке **Группы** нажать на кнопку **+ Добавить в группы**, находящуюся над таблицей групп пользователя (см. Рисунок 32).

< **Александр Смирнов** | Пользователь Активен Заблокировать ⋮

Группы Данные Роли

+ Добавить в группы

Название группы	Email		
<input type="text"/>	<input type="text"/>	<input type="button" value="Найти"/>	<input type="button" value="Очистить"/>
Название	Email	Описание	
Q group_one	group_one@mydomain.ru		

Рисунок 32 – Добавить пользователя в группы рассылки (2)

Для последующего добавления пользователя в группы рассылки необходимо установить галочку напротив необходимой группы рассылки и нажать на кнопку **Добавить в группы** (см. Рисунок 33). После этого пользователь будет добавлен в выбранные группы рассылки.

✕ Выбрано 2 ▾

Название группы	Email		
<input type="text"/>	<input type="text"/>	<input type="button" value="Найти"/>	<input type="button" value="Очистить"/>
<input type="checkbox"/> Название группы			
<input type="checkbox"/>			
<input checked="" type="checkbox"/> group_2			
<input checked="" type="checkbox"/> group_3			

Рисунок 33 – Добавить пользователя в группы рассылки (3)

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

Для исключения пользователя из группы рассылки необходимо выбрать пользователя из общего списка и нажать на **Удалить из группы** (см. Рисунок 34).

< **Александр Смирнов** | Пользователь Активен Заблокировать ⋮

Группы Данные Роли

+ [Добавить в группы](#)


Название группы	Email		
<input type="text"/>	<input type="text"/>	Найти	Очистить
Название	Email	Описание	
 group_one	group_one@mydomain.ru		Удалить из группы

Рисунок 34 – Удалить пользователя из группы рассылки

6.2.10 Редактирование данных пользователя

Для редактирования данных пользователя необходимо в разделе **Пользователи** перейти на вкладку **Данные** (см. Рисунок 35).

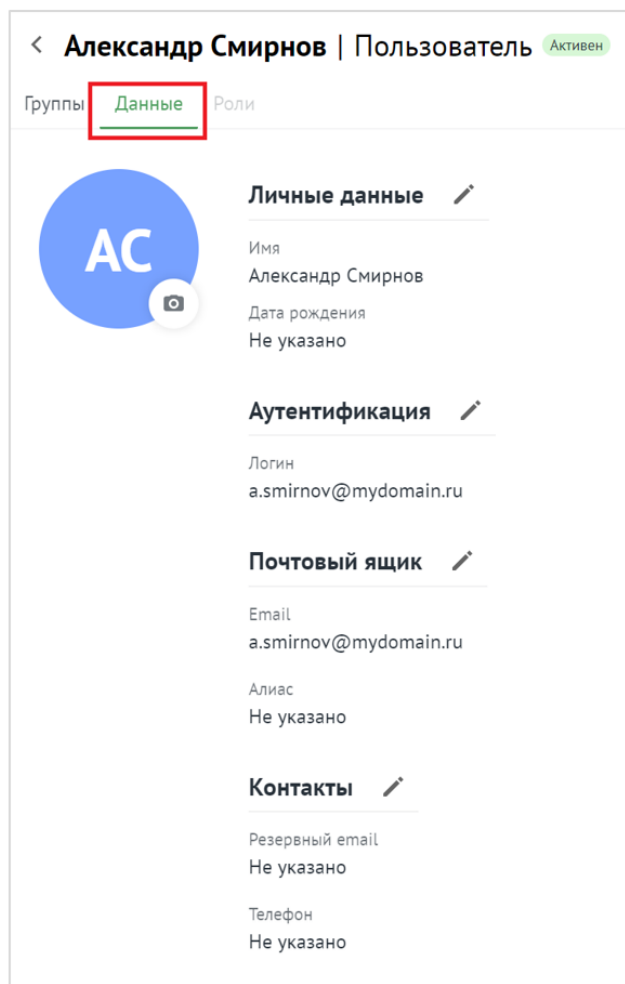





Рисунок 35 – Информация о пользователе, отображаемая на вкладке **Данные**

В результате отобразится информация, заполненная администратором при создании пользователя с иконкой  напротив названия каждого блока и строк, содержащихся в нем. При нажатии на иконку  блок становится редактируемым (см. Рисунок 36).

< Редактирование пользователя «Александр Смирнов» | Аутентификация Активен

Группы Данные Роли



Личные данные

Имя
Александр Смирнов

Дата рождения
Не указано

Аутентификация

Логин (обязательно)	Домен
<input type="text" value="a.smirnov"/>	mydomain.ru
<input type="button" value="Сбросить пароль"/>	
<input type="button" value="Добавить логин"/>	

Почтовый ящик

Email
a.smirnov@mydomain.ru

Алиас
Не указано

Рисунок 36 – Редактирование информации о пользователе

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

6.3 Управление группами рассылки

6.3.1 Просмотр списка групп рассылки

Для просмотра существующей группы в **Панели администрирования** необходимо выбрать раздел **Группы**. В рабочей области откроется перечень существующих групп (см. Рисунок 37). Об активной группе представлена следующая информация:

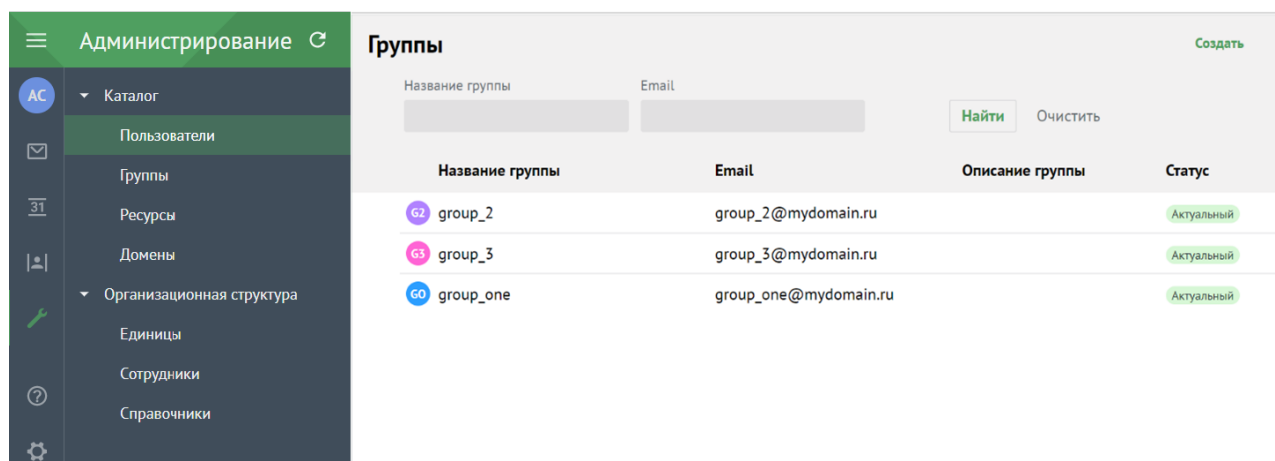


Рисунок 37 – Просмотр существующей группы рассылки

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

6.3.2 Просмотр записи о группе

Чтобы просмотреть подробную запись о группе необходимо нажать на соответствующую строку и перейти на вкладку **Сведения**. На этой же вкладке доступно редактирование записи о группе.

6.3.3 Создание группы рассылки

Для создания группы рассылки необходимо выполнить следующие действия:

1. В разделе **Группы** нажать на кнопку **Создать** (см. Рисунок 38).

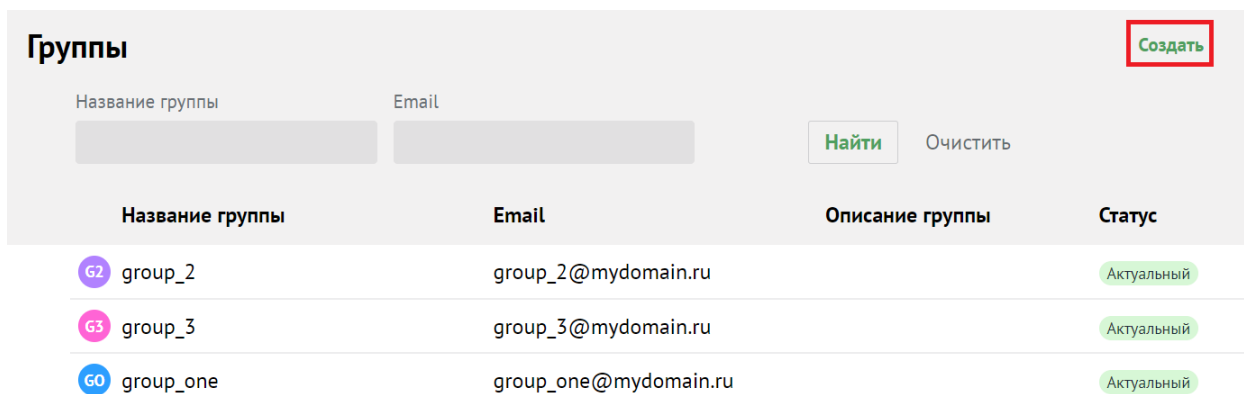
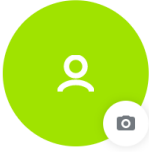


Рисунок 38 – Создание группы рассылки

2. В открывшейся форме создания группы необходимо заполнить следующие поля (см. Рисунок 39):

Новая группа ×



Данные

Название (обязательно)

Почтовый ящик (обязательно)

Описание

Родительские группы

[Расширенный поиск](#)

Добавить участников

Добавить участников

[Расширенный поиск](#)

Автоматически добавлять в группу

Обновление группы в соответствии с условиями может занять несколько часов

Рисунок 39 – Создание группы рассылки

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

- Поле **Почтовый ящик** обязательно к заполнению. Если введенный почтовый ящик уже существует, то поле **Почтовый ящик** подсветится красным цветом и под ним отобразится сообщение. Необходимо изменить название почтового ящика. В ином случае, после заполнения всех полей, группу сохранить не удастся, кнопка **Сохранить** будет неактивна (см. Рисунок 40).

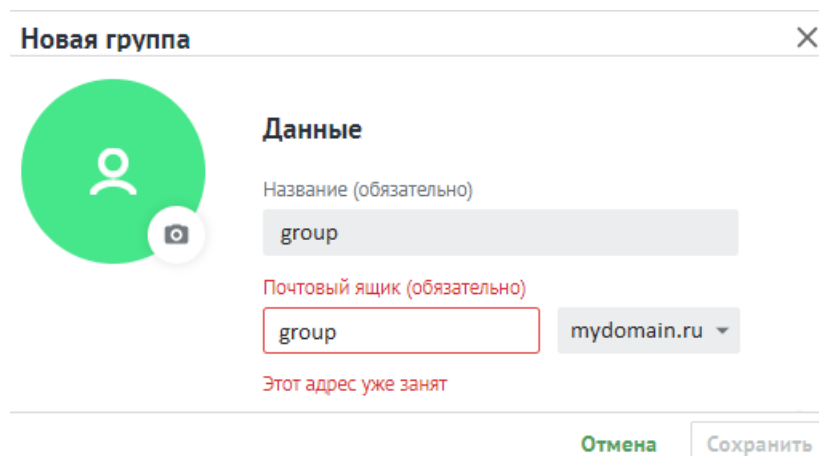

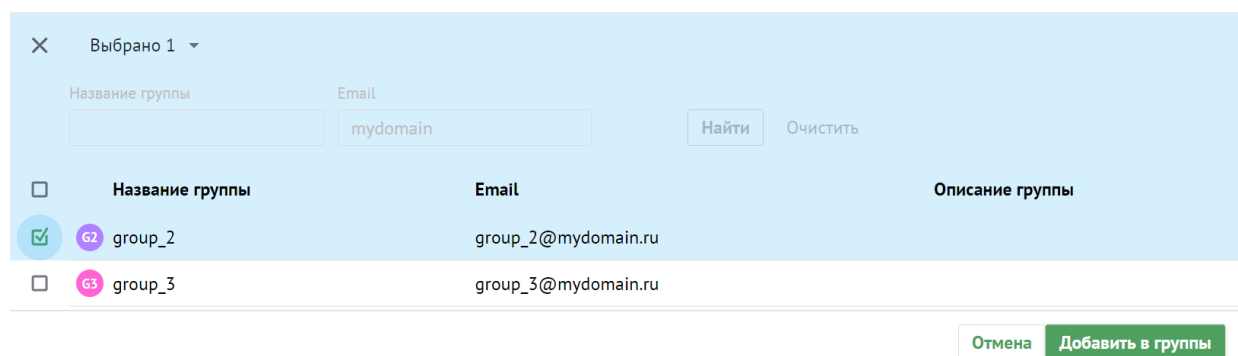


Рисунок 40 – Использование существующего названия почтового ящика

- Описание группы рассылки (опционально).
- Поле **Родительские группы** заполнить вручную или найти с помощью кнопки «» (**Расширенный поиск**);
 - установить курсор мыши на соответствующую группу и нажать **Добавить в группы** (см. Рисунок 41);





<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 41 – Добавить в группы

- выбрать группы с помощью отметки из перечня групп и нажать кнопку **Добавить в группы** (см. Рисунок 42);

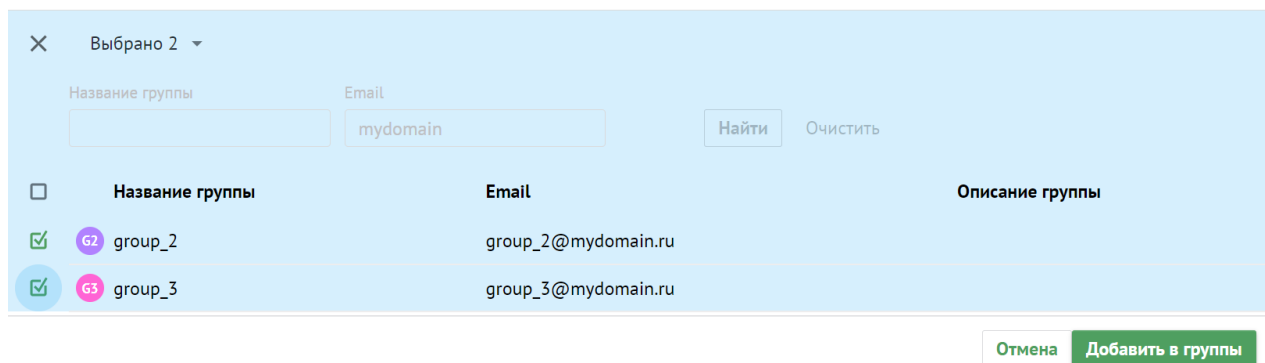


Рисунок 42 – Добавить в группы (2)

- нажать на < в левом верхнем углу окна **Добавление в группы**, чтобы вернуться к созданию группы;
- Поле **Добавить участников** заполнить аналогично полю **Родительские группы**.
- Добавьте одно или несколько условий группе нажатием на кнопку **+** **Новое условие**. Подробная информация о добавлении условия приведена в разделе 6.3.8.

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

6.3.4 Поиск группы рассылки

Для поиска группы рассылки необходимо выполнить следующие действия:

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

4. Выбрать необходимую группу рассылки из динамически формируемого списка в области отображения найденных групп (см. Рисунок 43).

Название группы	Email	Описание группы	Статус
G2 group_2	group_2@mydomain.ru		Актуальный
G3 group_3	group_3@mydomain.ru		Актуальный
G0 group_one	group_one@mydomain.ru		Актуальный

Рисунок 43 – Поиск группы рассылки

6.3.5 Добавление/исключение членов группы рассылки

Для добавления пользователя в группу рассылки необходимо выполнить следующие действия:

1. Выбрать соответствующую группу рассылки.
2. Нажать на кнопку **Добавить участников** (см. Рисунок 44).

group_one | Группа Актуальный

Добавить участников Изменить условия автодобавления

Участники Состоит в группах Сведения

Добавить участников Изменить условия автодобавления

Имя Фамилия Email

Найти Очистить

Рисунок 44 – Добавить участников в группу рассылки

3. В открывшемся окне установить флажки для тех пользователей, которых требуется добавить в группу рассылки.
4. Нажать на кнопку **Добавить в группу**.

Для исключения пользователя из группы рассылки необходимо выбрать соответствующего пользователя в группе рассылки и нажать на кнопку **Удалить из группы** (см. Рисунок 45).

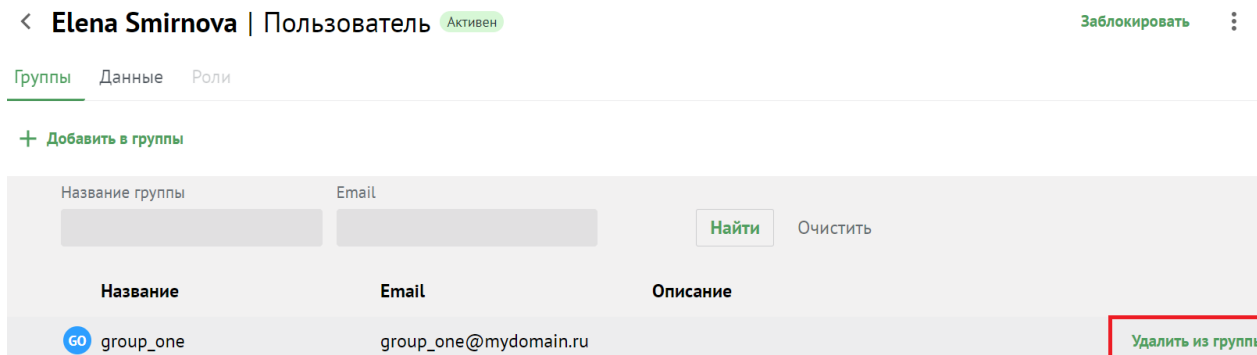



Рисунок 45 – Удаление участников из группы рассылки

6.3.6 Удаление групп рассылки

Для удаления группы рассылки необходимо выбрать группу рассылки из списка и нажать на иконку , а затем на **Удалить** (см. Рисунок 46).

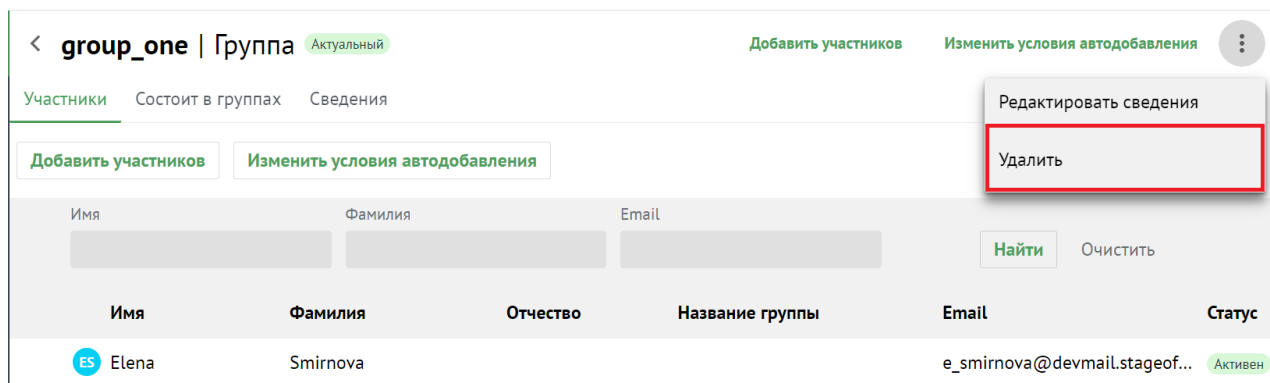



Рисунок 46 – Удаление группы рассылки

Подтвердить удаление группы рассылки, после чего группа будет удалена.

6.3.7 Редактирование группы рассылки

Для редактирования группы рассылки необходимо выполнить следующие действия:

1. Перейти в раздел **Группы**.

2. Выбрать соответствующую группу рассылки в области отображения созданных групп.
3. Нажать на иконку , а затем на кнопку **Редактировать сведения** (см. Рисунок 47).

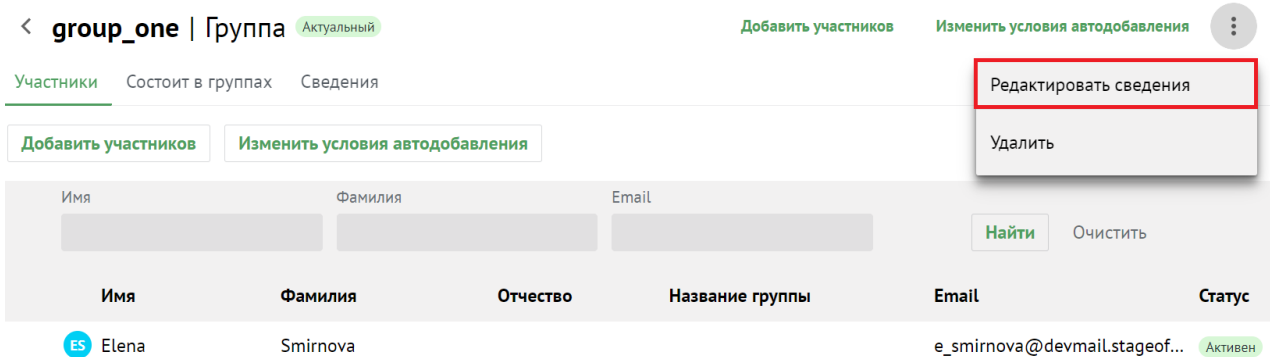


Рисунок 47 – Редактирование группы рассылки (1)

Для сохранения изменений нажать на кнопку **Сохранить**. Для отмены сохранения внесенных изменений нажать на кнопку **Отмена** (см. Рисунок 48).

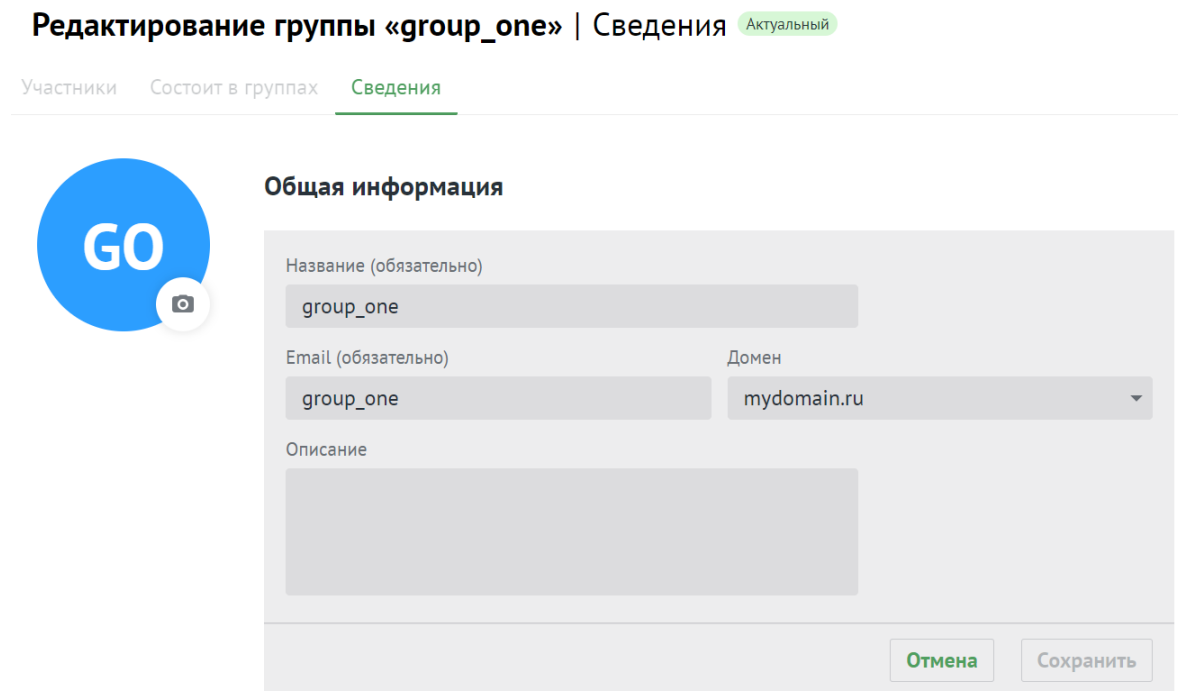


Рисунок 48 – Редактирование группы рассылки (2)

6.3.8 Настройка динамических групп рассылки

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

Чтобы добавить правила автоматического добавления необходимо выполнить следующие действия:

1. В разделе **Группы** выбрать соответствующую группу из перечня.
2. Вызвать окно настроек правил автоматического добавления одним из способов:
 - Открыть запись о группе нажатием на соответствующую группу левой кнопкой мыши и нажать на кнопку **Изменить условия автодобавления** (см. Рисунок 49);

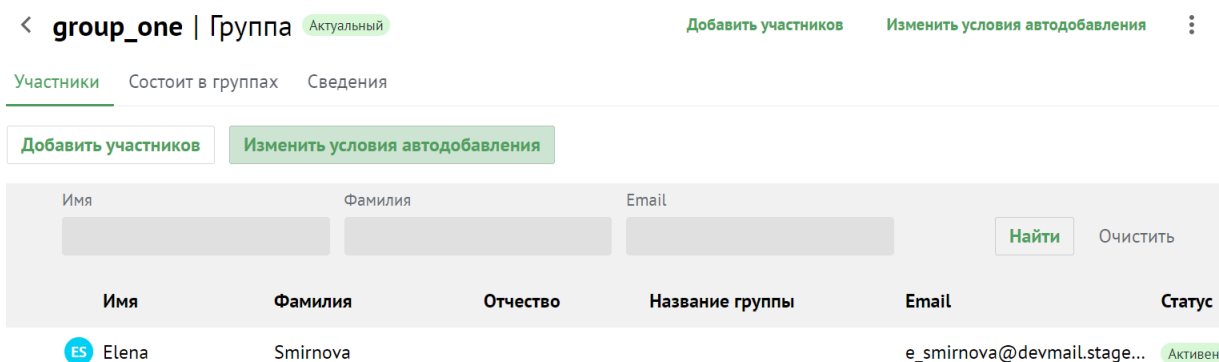


Рисунок 49 – Изменить условия автодобавления

- Навести курсор мыши на необходимую запись и выбрать команду **Изменить условия автодобавления** (см. Рисунок 50).

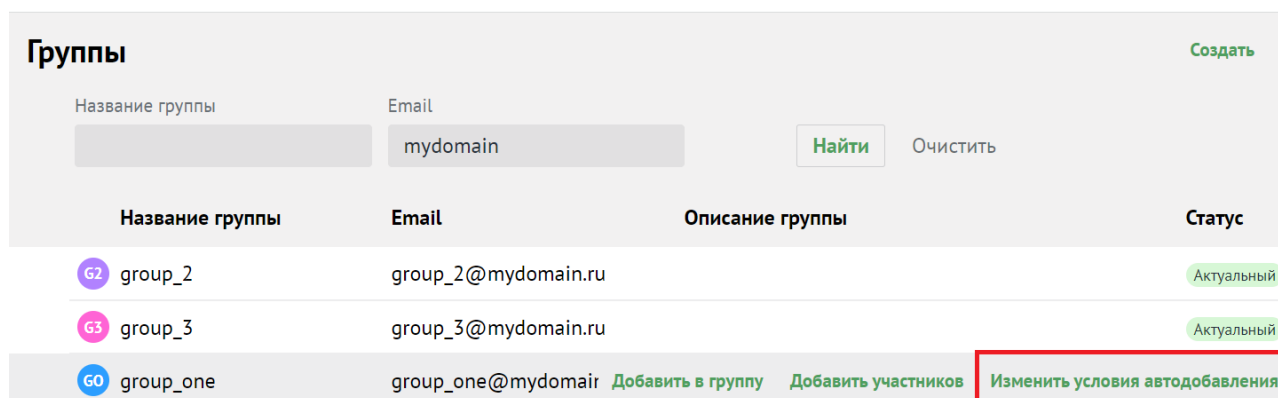





Рисунок 50 – Изменить условия автодобавления (2)

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

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

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

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

1. Выбрать соответствующее условие и нажать на кнопку  (**Еще**) напротив строки.
2. Выбрать значение:
 -  (**Переместить выше**);
 -  (**Переместить ниже**).

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

6.4 Управление ресурсами

6.4.1 Создание ресурса

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

1. Нажать на кнопку + **Создать** в списке ресурсов.

2. Задать параметры создаваемого пространства для встречи:
 - Заполнить блок **Общая информация**:
 - Ввести название пространства для встречи. Поле **Название** обязательно для заполнения.
 - Ввести текст описания пространства для встречи.
 - Указать минимальное количество участников пространства для встречи в поле **Вместимость**. По умолчанию задано значение 1.
 - Ввести адрес электронной почты. Если доменов несколько, в поле справа от поля **Электронная почта** нажать на кнопку 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** нажать на кнопку и выбрать домен.
 - Ввести и повторить пароль, либо использовать пароль, предложенный автоматическим генератором.
 - 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**.

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


6.4.2 Просмотр данных о пространстве для встречи

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


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

6.4.3 Поиск ресурса

Для поиска ресурса необходимо выполнить следующие действия:


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

6.4.4 Редактировать запись о пространстве для встречи

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


6.4.5 Фильтрация ресурсов

Чтобы отфильтровать список ресурсов необходимо выполнить следующие действия:

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

6.4.6 Удаление ресурса

Чтобы удалить пространства для встреч необходимо выполнить следующие действия:

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

Важно – Пространства для встречи удаляются безвозвратно.

6.5 Управление доменами

6.5.1 Создание домена

Чтобы создать новый домен, необходимо выполнить следующие действия:

1. Нажать на кнопку + **Добавить домен** в окне отображения доменов.
2. Задать параметры создаваемого домена:
 - Заполнить блок **Общая информация**:
 - Ввести название домена. Поле **Название** обязательно для заполнения.
 - Ввести текст описания.
 - Чтобы созданный домен впоследствии предлагался в качестве приоритетного, установить галочку в строке **Показывать в качестве приоритетного при добавлении новых пользователей**.

3. Заполнить поля блока **Напоминание о продлении срока регистрации**, предварительно убрав галочку **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, отобразившемся при нажатии в поле ввода.
- В поле **Отправить на электронную почту** ввести адрес почты, на которую необходимо получать напоминания.

Важно – При желании не напоминать о продлении срока регистрации следует оставить галочку в поле **Не напоминать**.

- Заполнить блок **DKIM-ключ**:
 - В поле **Длина ключа** выбрать значение из раскрывающегося списка.
 - В поле **Селектор** по умолчанию стоит префикс mail, рекомендуется его использовать. Поле обязательно для заполнения.


4. Нажать на кнопку **Сохранить**.

Все домены, отображаемые в Панели управления, могут быть созданы непосредственно через Панель управления или с помощью расширенного администрирования ПО «Mailion».

6.5.2 Поиск домена

Для поиска домена необходимо выполнить следующие действия:

1. Перейти в раздел **Домены**.

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


6.5.3 Просмотр данных о домене

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

Отобразится запись о домене, в которой содержится вся необходимая информация. На этой же вкладке доступно редактирование записи о домене.


6.5.4 Редактировать запись о домене

Чтобы отредактировать запись о домене необходимо выполнить следующие действия:

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

6.5.5 Фильтрация доменов

Чтобы отфильтровать список доменов необходимо выполнить следующие действия:

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

6.5.6 Удаление домена

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

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

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

Важно – Домены удаляются безвозвратно.

6.6 Управление единицами организационной структуры

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

Важно – Создание организации доступно только с помощью интерфейса командной строки. Подробная информация приведена в разделе 7.8.

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

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

6.6.1 Создание организационной единицы

Чтобы создать организационную единицу необходимо выполнить следующие действия:

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

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

6.6.2 Просмотр данных

Чтобы просмотреть организационную единицу необходимо выполнить следующие действия:

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

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

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

6.6.3 Редактирование записи о сотруднике

Чтобы отредактировать информацию о сотруднике необходимо выполнить следующие действия:

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

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

6.6.4 Поиск единицы организационной структуры

Для поиска единицы организационной структуры необходимо выполнить следующие действия:

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

6.6.5 Создание дочерней единицы

Чтобы создать дочернюю единицу необходимо выполнить следующие действия:

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

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

3. Нажать на кнопку **Сохранить**.

6.6.6 Удаление дочерней единицы

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

Чтобы удалить дочернюю единицу необходимо выполнить следующие действия:



1. Навести курсор на запись, нажать на кнопку  (**Еще**) и выбрать команду **Удалить**.

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

2. Нажать на кнопку **Удалить**.

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

6.6.7 Удаление организационной единицы



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

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

6.7 Управление сотрудниками

6.7.1 Добавление нового сотрудника

Чтобы добавить нового сотрудника необходимо выполнить следующие действия:

1. Нажать на кнопку + **Новый сотрудник**.
2. В открывшейся форме добавления нового сотрудника необходимо заполнить следующие поля:
 - Заполнить блок **Личные данные**: ввести имя, фамилию, отчество, дату рождения и выбрать пол сотрудника. Поле **Имя** обязательно для заполнения.
 - Заполнить блок **Аутентификация**:
 - Ввести логин. Если доменов несколько, в поле справа от поля **Логин** нажать на кнопку  (**Развернуть**) и выбрать домен.
 - Ввести и повторить пароль.
 - Заполнить блок **Почтовый ящик**:
 - В поле **Основной email** (обязательно для заполнения) ввести почтовый ящик сотрудника. Если доменов несколько, то в поле справа от поля **Логин** необходимо нажать на кнопку  (**Развернуть**) и выбрать домен.
 - При необходимости добавить алиас сотрудника нажатием кнопки + (**Добавить алиас**).
 - Заполнить блок **Контакты**:
 - Заполнить поле **Резервный email**.

- Ввести телефон, при необходимости несколько, и выбрать категорию из раскрывающегося списка:
 - Домашний;
 - Рабочий;
 - Для СМС;
 - Для голосовых звонков;
 - Факс;
 - Мобильный;
 - Для видеозвонков;
 - Пейджер;
 - Телетайп.
 - Заполнить блок **Адреса**. Заполнить данными сотрудника поля **Название адреса, Страна, Город, Адрес, Индекс, Этаж, Кабинет, Место**.
 - Заполнить поле **Организация**. После этого для заполнения станут доступны поля **Подразделение, Проектная группа и Должность**.
3. Нажать на кнопку **Сохранить**.

6.7.2 Редактирование 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**.

6.7.3 Поиск сотрудника

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

6.7.4 Удаление сотрудника

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

6.8 Управление справочниками

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

6.8.1 Создание записи в справочнике

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

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

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

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

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

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

6.8.2 Поиск записи в справочнике

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

6.8.3 Редактирование записи в справочнике

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

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

6.8.4 Удалить запись в справочнике

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

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

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

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

7 РАСШИРЕННОЕ АДМИНИСТРИРОВАНИЕ С ПОМОЩЬЮ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ

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

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

7.1 Информация для работы с интерфейсом командной строки

7.1.1 Установка

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

При необходимости установки на машину оператора необходимо использовать команду:

```
sudo yum install nct_ministerium
```

7.1.2 Просмотр команд

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

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

```
nct_ministerium  
--help
```

Для просмотра конкретной команды необходимо использовать запрос:

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


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

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

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

Важно – Администратор инсталляции создается при первичном развертывании системы. Удаление его с помощью интерфейса командной строки для расширенного администрирования невозможно.

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

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

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

Подробная информация о создании и удалении администратора тенанта приведена в разделах 7.3.5 и 7.20. Информация о добавлении роли администратора тенанта уже созданному пользователю приведена в разделе 7.3.7.

7.2 Установка общей квоты на тенант администратором инсталляции

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

Важно – Установить общую квоту может только пользователь с ролью администратора инсталляции.

Для этого необходимо выполнить запрос:

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

Описание параметров запроса приведено в таблице 52.

Таблица 52 – Описание параметров запроса на установку общей квоты

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_total.max_size	Str	+	Размер общей квоты тенанта
config	Str	+	Конфигурационный файл с параметрами сервиса 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"
}
```

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

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

Описание параметров запроса приведено в таблице 53.

Таблица 53 – Описание параметров запроса на установку общей квоты

Параметр	Тип	Обязательность	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": null,
  "tenat_total_quota": {
    "max_size": 42949672960
  }
}
```

Важно – Администратор инсталляции не может как устанавливать почтовую квоту **mail_total_quota**, так и получать ее текущее значение.

7.3 Операции над тенантом

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

Тенант представляет собой одну компанию и является учетной записью организации.

7.3.1 Создание тенанта

Для создания тенанта необходимо выполнить запрос:

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

Описание параметров запроса приведено в таблице 54.

Таблица 54 – Описание параметров запроса на создание тенанта

Параметр	Тип	Обязательность	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
display_name	Str	+	Имя тенанта
default_locale	Str	+	Локаль тенанта по умолчанию
password.default_hash_type	Int	+	Тип хэша паролей по умолчанию для пользователей тенанта
password.expiration_duration	Str	+	Срок действия паролей пользователей тенанта (задается в микросекундах)
password.password_expiration_remind	Str	+	Срок действия напоминания об истечении срока действия паролей (должен быть меньше expiration_duration)
password.last_number_must_differ	Int	+	Количество уникальных паролей в истории паролей пользователя

Пример ответа:

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

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

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

, где **tenant_id** является идентификатором тенанта.

Пример ответа:

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

7.3.2 Настройка уведомлений об истечении срока жизни пароля

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

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

```

--recurrence_rule.interval <>
--recurrence_rule.count
--retry_policy.count <>
--retry_policy.delay <>
--tenant_id <>

```

Описание параметров запроса приведено в таблице 55.

Таблица 55 – Описание параметров запроса на создание уведомления

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

После этого необходимо выполнить запрос на обновление тенанта:

```
nct_ministerium update_tenant
--admin.login <...>
--admin.password <...>
--tenant_id <...>
--password.expiration_duration
--password.expiration_remind
```

Описание параметров запроса приведено в таблице 56.

Таблица 56 – Описание параметров запроса на обновление тенанта

Параметр	Тип	Обязательность	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)

Пример ответа на данные команды:

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

7.3.3 Создание группы ALL для тенанта

Группа ALL обязательна к созданию для каждого тенанта. Для нее должны выполняться следующие условия:

- существующую связь между сущностью тенанта и группой ALL удалить нельзя;
- сущность из другого тенанта не может быть дочерней для группы ALL данного тенанта;
- группу ALL тенанта удалить нельзя;

- нельзя делать группу ALL дочерней для любой другой группы, каждый пользователь тенанта является дочерней сущностью по отношению к этой группе.

Для создания группы ALL для тенанта необходимо выполнить запрос:

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

Описание параметров запроса приведено в таблице 57.

Таблица 57 – Описание параметров запроса на создание группы ALL для тенанта

Параметр	Тип	Обязательность	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:

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

7.3.4 Создание GAL-пользователя в тенанте

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

Важно – Перед созданием GAL-пользователя должен быть создан тенант.

Для создания GAL-пользователя необходимо выполнить запрос:

```
nct_ministerium create_gal_user
--config ministerium.json
--admin.login <...>
```



```

--admin.password <...>
--locale ru_RU
--region_id 004bfd74-e829-4224-a28c-620b265b5bc1
--tenant_id ef28480f-0ee4-4f0c-af67-59f100727f31

```

Описание параметров запроса приведено в таблице 58.

Таблица 58 – Описание параметров запроса на создание GAL-пользователя в тенанте

Параметр	Тип	Обязательность	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
locale	Str	+	Локаль тенанта
region_id	Str	+	Идентификатор региона
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```

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

```

7.3.5 Создание администратора тенанта

Для создания администратора тенанта необходимо выполнить следующие действия:

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

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

Описание параметров запроса приведено в таблице 59.

Таблица 59 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательность	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": "11cd3c1a-9f14-4810-acc6-4a7b2aacb540",
        "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1"
      },
      "path": [
        "gal"
      ]
    }
  ]
}
```

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

2. Выполнить запрос на создание администратора тенанта:

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

Описание параметров запроса приведено в таблице 60.

Таблица 60 – Описание параметров запроса на создание администратора тенанта

Параметр	Тип	Обязательность	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	+	Идентификаторы GAL-тегов
login	Str	+	Логин создаваемого администратора тенанта
password	Str	+	Пароль создаваемого администратора тенанта
profile.first_name	Str	+	Имя создаваемого администратора тенанта
profile.last_name	Str	+	Фамилия создаваемого администратора тенанта

Пример ответа:

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

```
"id": "aa7287ad-b22d-4a2e-aaf7-fl23d71ad7e8"
}
```

, 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-fl23d71ad7e8
```

Пример ответа:

```
{
  "Response": {
    "msg": "ok"
  },
  "Entities": [
    {
      "id": "aa7287ad-b22d-4a2e-aaf7-fl23d71ad7e8",
      "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-fl23d71ad7e8",
          "login": "admin2.tenant2_test",
          "auth_type": 1
        }
      ],
      "Payload": {
        "User": {
          "locale": "ru_RU"
        }
      },
      "status": 2 ### ACTIVE ###
    }
  ]
}
```

Для удаления администратора тенанта необходимо выполнить действия, приведенные в разделе [7.20](#).

7.3.6 Создание пользователя тенанта

Важно – 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 61.

Таблица 61 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательность	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
--gal_tags 3eac9972-c634-4e5b-858a-1043386b4045
--login test@domain.ru
--password 'wx8y(LSpb_8$Duzq1HD'
--E-mail test@domain.ru
--profile.first_name Name
--profile.last_name Family

```

Описание параметров запроса приведено в таблице 62.

Таблица 62 – Описание параметров запроса на создание пользователя тенанта

Параметр	Тип	Обязательность	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	+	Идентификаторы GAL-тегов
login	Str	+	Логин создаваемого пользователя тенанта
password	Str	+	Пароль создаваемого пользователя тенанта
E-mail	Str	+	Почтовый ящик создаваемого пользователя тенанта
profile.first_name	Str	+	Имя создаваемого пользователя тенанта

Параметр	Тип	Обязательность	Описание
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-fl23d71ad7e8
```

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 63.

Таблица 63 – Описание параметров ответа на запрос на получение созданного пользователя по его идентификатору

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

Параметр	Тип	Обязательность	Описание
Entities.status	Int	+	Значение должно быть равно 2 (ACTIVE)

Важно – При сбое создания пользователя см. раздел 7.7.

7.3.7 Добавление роли администратора тенанта пользователю

Для добавления роли администратора тенанта необходимо выполнить следующие действия:

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

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

Пример ответа:

```
{
  "Response": {
    "msg": "ok"
  },
  "Entities": [
    {
      "id": "7b9d0558-f9b9-475b-9c52-1d63a30c3ed6",
      "type": 1,
      "tenant_id": "8c13a034-48f5-44e6-9a60-afecda033437",
      "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1",
      "roles": [
        "c4b1f72c-672d-5ace-8a6d-96edc21227de"
      ],
      ....
    } ] }
```

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

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

```
nct_ministerium update_roles
--admin.login <...>
```

```
--admin.password <...>
--entity_id 7b9d0558-f9b9-475b-9c52-1d63a30c3ed6
--add_roles 54718e3a-6c7b-5c9f-b4de-a897c356cb5e
```

Пример ответа:

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

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

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

7.3.8 Настройка квот в тенанте

Чтобы задать ограничения размеров отдельного почтового сообщения, общего объема почтовых сообщений в почтовом ящике или ограничить суммарный размер вложений в письме, в ПО «Mailion» используется механизм определения квот. Квоты могут быть назначены на разных уровнях – на уровне тенанта, а также на уровне отдельного пользователя. Квоты, заданные на уровне пользователя, имеют преимущество перед квотами на уровне тенанта.

Важно – Настройки квот в тенанте может выполнить только пользователь с ролью администратора тенанта.

Для настройки квот используются команды, приведенные в таблице 64.

Таблица 64 – Команды для настройки квот

Доступные команды	Описание
Create_tenant_quotas_profile	Создать квоты профиля тенанта
Create_user_quotas_profile	Создать квоты профиля пользователя
Delete_tenant_quotas_profile	Удалить квоты профиля тенанта
Get_recount_quotas_processes	Получить все запущенные процессы пересчета квот
Get_user_quotas_profile	Получить квоты профиля пользователя
Recount_quotas	Начать процесс напоминания о пересчете квот для одиночного объекта или всех объектов в тенанте

Доступные команды	Описание
Remove_user_quotas_profile	Удалить квоты профиля пользователя
Stop_recount_quotas	Остановить процесс пересчета квоты. Некоторые объекты могли иметь непредвиденные упоминания о квотах
Update_tenant_quotas_profile	Обновить квоты профиля тенанта
Update_user_quotas_profile	Обновить квоты профиля пользователя
Get_total_quotas	Получить размер общей квоты, выделенной на тенант
Update_total_quotas	Обновить общую квоту

7.3.8.1 Создание квот профиля

Пример запроса на создание квот профиля тенанта:

```
nct_ministerium create_tenant_quotas_profile
--admin.login <...>
--admin.password <...>
--tenant_id 9d5dc502-51d8-4dc0-a7a8-0856639ec0d1
--quotas {"ONE_MAIL_SIZE": "1M"}
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=False
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=True
--cox.use_tls_balancer=False
--tls_settings.ca_file ../certs/ca.pem
--tls_settings.client_cert_file ../certs/client_cert.pem
--tls_settings.key_file ../certs/client_key.pem
```

Описание параметров запроса на создание квот профиля тенанта приведено в таблице 65.

Таблица 65 – Описание параметров запроса на создание квот профиля тенанта

Параметр	Тип	Обязательность	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);

Параметр	Тип	Обязательность	Описание
			– ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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
}
```

7.3.8.2 Удаление квот профиля

Пример запроса на удаления квот профиля тенанта:

```
nct_ministerium delete_tenant_quotas_profile
--admin.login <...>
--admin.password <...>
--tenant_id 9d5dc502-51d8-4dc0-a7a8-0856639ec0d1
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=False
--cox.request_timeout=10s
```

```

--cox.service_name=cox
--cox.use_tls=True
--cox.use_tls_balancer=False
--tls_settings.ca_file ../certs/ca.pem
--tls_settings.client_cert_file ../certs/client_cert.pem
--tls_settings.key_file ../certs/client_key.pem

```

Описание параметров запроса на удаление квот профиля тенанта приведено в таблице 66.

Таблица 66 – Описание параметров запроса на удаление квот профиля тенанта

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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
}

```

7.3.8.3 Обновление квот профиля

Пример запроса на обновление квот профиля тенанта:

```
nct_ministerium update_tenant_quotas_profile
--admin.login <...>
--admin.password <...>
--tenant_id 9d5dc502-51d8-4dc0-a7a8-0856639ec0d1
--quotas {"ONE_MAIL_SIZE": "15M", "ALL_MAILS_SIZE": "35M",
"ALL_MAIL_ATTACHMENTS_SIZE": "15M"}
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=False
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=True
--cox.use_tls_balancer=False
--tls_settings.ca_file ../certs/ca.pem
--tls_settings.client_cert_file ../certs/client_cert.pem
--tls_settings.key_file ../certs/client_key.pem
```

Описание параметров запроса на обновление квот профиля приведено в таблице 67.

Таблица 67 – Описание параметров запроса на обновление квот профиля

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
quotas	Str	+	Список квот для пользователей: – ONE_MAIL_SIZE (размер письма); – ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут запроса к сервису
cox.service_name	Str	+	Имя сервиса

Параметр	Тип	Обязательность	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 на данный запрос:

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

7.3.8.4 Создание квот профиля пользователя

Пример запроса на создание квот профиля пользователя:

```
nct_ministerium create_user_quotas_profile
--admin.login <...>
--admin.password <...>
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--entity_id 8b3c878b-9e26-440f-84db-aabce7e5e75f
--quotas {"ONE_MAIL_SIZE": "1M", "ALL_MAILS_SIZE": "1M",
"ALL_MAIL_ATTACHMENTS_SIZE": "1M"}
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=False
--cox.request_timeout=10s
--cox.service_name=cox --cox.use_tls=True
--cox.use_tls_balancer=False
--tls_settings.ca_file ../certs/ca.pem
--tls_settings.client_cert_file ../certs/client.crt.pem
--tls_settings.key_file ../certs/client_key.pem
```

Описание параметров запроса на создание квот профиля пользователя приведено в таблице 68.

Таблица 68 – Описание параметров запроса на создание квот профиля пользователя

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
entity_id	Str	+	Идентификатор пользователя
quotas	Str	+	Список квот для пользователей: – ONE_MAIL_SIZE (размер письма); – ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса

Параметр	Тип	Обязательность	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

Пример ответа на данный запрос:

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

7.3.8.5 Удаление квот профиля пользователя

Пример запроса на удаление квот профиля пользователя:

```
nct_ministerium remove_user_quotas_profile
--admin.login <...>
--admin.password <...>
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--entity_id e1257024-5dc4-446a-abae-e15eb4273297
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=False
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=True
--cox.use_tls_balancer=False
--tls_settings.ca_file ../certs/ca.pem
--tls_settings.client_cert_file ../certs/client.crt.pem
--tls_settings.key_file ../certs/client_key.pem
```

Описание параметров запроса на удаление квот профиля приведено в таблице 69.

Таблица 69 – Описание параметров запроса на обновление квот профиля пользователя

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
entity_id	Str	+	Идентификатор пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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
}
```

7.3.8.6 Обновление квот профиля пользователя

Пример запроса на обновления квот профиля пользователя:

```
nct_ministerium update_user_quotas_profile
--admin.login <...>
--admin.password <...>
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--entity_id 0e1e6928-bf56-460e-a8b7-b16c681913d7
```

```

--quotas {"ONE_MAIL_SIZE": "2M", "ALL_MAILS_SIZE": "2M",
"ALL_MAIL_ATTACHMENTS_SIZE": "2M"}
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=False
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=True
--cox.use_tls_balancer=False
--tls_settings.ca_file ../certs/ca.pem
--tls_settings.client_cert_file ../certs/client_cert.pem
--tls_settings.key_file ../certs/client_key.pem

```

Описание параметров запроса на обновление квот профиля приведено в таблице 70.

Таблица 70 – Описание параметров запроса на обновление квот профиля пользователя

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
entity_id	Str	+	Идентификатор пользователя
quotas	Str	+	Список квот для пользователей: – ONE_MAIL_SIZE (размер письма); – ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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	Обязательность	Описание
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа на данный запрос:

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

7.3.8.7 Получение квот профиля

Пример запроса на получение квот профиля пользователя:

```
nct_ministerium get_user_quotas_profile
--admin.login <...>
--admin.password <...>
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
--entity_id b8740313-c64e-427f-8635-ecbb083d2435
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=False
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=True
--cox.use_tls_balancer=False
--tls_settings.ca_file ../certs/ca.pem
--tls_settings.client_cert_file ../certs/client_cert.pem
--tls_settings.key_file ../certs/client_key.pem
```

Описание параметров запроса приведено в таблице 71.

Таблица 71 – Описание параметров запроса на получение квот профиля пользователя

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
entity_id	Str	+	Идентификатор пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия

Параметр	Тип	Обязательность	Описание
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.service_name	Str	+	Имя сервиса
cox.use_tls_balancer	Bool	+	Защищенная передача данных при подключении к балансировщику
tls_settings.ca_file	Str	+	Путь к 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": {}
}
```

7.3.8.8 Установка общей квоты тенанта на почту

Пользователь с ролью администратора тенанта может установить общую квоту тенанта на почту. Если данная квота не установлена, то лимитировать размер почтовой квоты на тенант будет общая квота тенанта, установленная администратором инсталляции.

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 72.

Таблица 72 – Описание параметров запроса на установку общей почтовой квоты

Параметр	Тип	Обязательность	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"
}
```

7.3.8.9 Получение общей квоты на тенант и общей квоты тенанта на почту

Пользователь с ролью администратора тенанта может получить размер общей квоты на тенант и общей квоты тенанта на почту.

Пример запроса на получение размера общей квоты на тенант и общей квоты тенанта на почту:

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

Описание параметров запроса приведено в таблице 73.

Таблица 73 – Описание параметров запроса на получение размера общей квоты

Параметр	Тип	Обязательность	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
  }
}
```

7.3.8.10 Нулевая квота пользователя

Если задана общая квота тенанта, то при создании пользователя в ней может не хватить места на его квоту. В таком случае для нового пользователя будет создан профиль квот, где его квота будет равна нулю. Он не будет занимать место в общей квоте тенанта, но не сможет писать или получать письма.

Чтобы узнать перечень пользователей, получивших нулевую квоту, необходимо выполнить запрос:

```
get_users_with_zero_quota
```

```
--config cfg.json
--tenant_id <>
--admin.login <>
--admin.password <>
```

Описание параметров запроса приведено в таблице 74.

Таблица 74 – Описание параметров запроса на просмотр пользователей с нулевой квотой

Параметр	Тип	Обязательность	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", ...}
}
```

7.3.9 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 75.

Таблица 75 – Описание параметров запроса на удаление администратора тенанта

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout			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

Важно – При выполнении команды удаления тенанта удаляются все объекты, входящие в данный тенант.

7.3.10 Удаление письма у всех получателей в рамках тенанта

Важно – Удаление письма выполняется пользователем с ролью администратора тенанта.

Для удаления письма у всех получателей в рамках тенанта необходимо выполнить следующие действия:

1. В представлении **Почта** необходимо выбрать письмо из любой папки. Подробная информация приведена в документе «Программное обеспечение «Корпоративная система электронной почты и планирования совместной работы команд «Mailion». Руководство оператора» RU.29144487.506900.001 34.
2. При открытии письма в консоли браузера формируется запрос **build_message**. Необходимо скопировать идентификаторы письма из сообщения вида:

```
{"msg":{"id":"61c45c6c-937f-4065-a204-04b0e0091dbb","region_id":"2dbacea3-5889-4021-8f38-bc2214dd7423"}}
```

3. Выполнить запрос на удаление письма:

```
nct_ministerium delete_all_related_messages_by_message_id
--config nct-ministerium.json
--message_id 61c45c6c-937f-4065-a204-04b0e0091dbb
--region_id 2dbacea3-5889-4021-8f38-bc2214dd7423
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b
```

Описание параметров запроса приведено в таблице 76.

Таблица 76 – Описание параметров запроса на удаление письма

Параметр	Тип	Обязательность	Описание
message_id	Str	+	Идентификатор сообщения, которое необходимо удалить
region_id	Str	+	Регион, в котором находится сообщение
tenant_id	Str	+	Идентификатор тенанта, в рамках которого удаляются сообщения

Пример ответа:

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

После этого выбранное письмо удалится.

7.4 Создание пользовательских GAL-тегов

Пользовательский GAL-тег – это тег глобальной адресной книги, который обозначает категорию, метку или дополнительные атрибуты, присваиваемые контактам.

Важно – 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 77.

Таблица 77 – Описание параметров запроса на получение созданного пользователя по его идентификатору

Параметр	Тип	Обязательность	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
tenant_id	Str	+	Идентификатор тенанта

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "gal": {
    "id": {
      "id": "559368c3-2ee4-43a4-966d-0904341f05f0",
      "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1"
    },
    "path": [
      "april_26_gal_tag"
    ]
  }
}
```

, где **gal.id.id** – идентификатор GAL-тега.

2. Выполнить запрос на получение GAL-тегов тенанта:

```
nct_ministerium get_tenant_gals
--config ministerium.json
--tenant_id 8c13a034-48f5-44e6-9a60-afecda033437
```

Пример ответа:

```
{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "gals": [
    ...
    {
      "id": {
        "id": "559368c3-2ee4-43a4-966d-0904341f05f0",
        "region_id": "004bfd74-e829-4224-a28c-620b265b5bc1"
      },
      "path": [
        "april_26_gal_tag"
      ]
    },
    ...
  ]
}
```

Для добавления пользователя в GAL-тег необходимо использовать команду **add_users_to_gal_tag**.

7.5 Настройка двухфакторной аутентификации

Важно – 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 78.

Таблица 78 – Описание параметров исключения пользователя

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
login			Идентификатор логина
second_factor_login.status	Str	+	Статус работы двухфакторной аутентификации для логина

От значений аргумента **second_factor_login.status** зависит статус работы двухфакторной аутентификации:

- DEFAULT – аналогично параметрам, заданным для тенанта;
- LIST_ENABLED – спрашивать всегда, кроме случая, когда запрос второго фактора для тенанта полностью отключен;
- LIST_DISABLED – никогда не запрашивать второй фактор.

Пример ответа:

```
{
```

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

Для настройки двухфакторной аутентификации пользователей необходимо выполнить следующие действия:

1. Установить параметры двухфакторной аутентификации тенанта:

```
nct_ministerium update_tenant
--config ministerium_demo.json
--admin.login <...>
--admin.password <...>
--tenant_id 1ddccc69-e32e-461f9cba-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 79.

Таблица 79 – Описание параметров двухфакторной аутентификации тенанта

Параметр	Тип	Обязательность	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
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

Параметр	Тип	Обязательность	Описание
second_factor_params.period_time	Str	Обязательный для типа TOTP, для HOTP не требуется	Время жизни одноразового пароля. Рекомендуется установить 30 секунд
second_factor_params.status	Str	+	Статус работы двухфакторной аутентификации
second_factor_params.sync_step	Str	+	Максимальная разница между значением счетчика на сервере и у пользователя
second_factor_params.type	Str	+	Тип второго фактора, TOTP (одноразовый пароль на основе времени) или HOTP (одноразовый пароль на основе хеш-функции)

Важно – Клиентские приложения чаще всего используют параметры, установленные по умолчанию. Необходимо использовать рекомендуемые параметры, указанные в таблице.

От значений аргумента **second_factor_params.status** зависит статус работы двухфакторной аутентификации:

- DISABLED – выключена;
- ENABLED_FOR_ALLOWED_LIST – включена для определенных пользователей;
- ENABLED_FOR_ALL – включена для всех пользователей.

Пример ответа:

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

2. Сбросить пользователю второй фактор, если он утратил к нему доступ:

```
nct_ministerium two_factor_auth_reset_user
--config ministerium.json
--admin.login <...>
--admin.password <...>
--entity_id
```

Описание параметров запроса приведено в таблице 80.

Таблица 80 – Описание параметров двухфакторной аутентификации тенанта

Параметр	Тип	Обязательность	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
entity_id	Str	+	Идентификатор пользователя, для которого необходимо сбросить второй фактор

Пример ответа:

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

7.6 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 81.

Таблица 81 – Описание параметров запроса на создание домена без делегирования

Параметр	Тип	Обязательность	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 82.

Таблица 82 – Описание параметров запроса на получение параметров созданного домена

Параметр	Тип	Обязательность	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Сох и настройками tls. Формируется автоматически на сервере с ролью

Параметр	Тип	Обязательность	Описание
			ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.pass word	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 83.

Таблица 83 – Описание параметров ответа

Параметр	Тип	Обязательность	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	Boolean	+	Значение должно быть равно значению, указанному при создании домена
domains.features.is_authorization	Boolean	+	Значение должно быть равно значению, указанному при создании домена
domains.features.is_service	Boolean	+	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.

Для создания домена необходимо выполнить следующие действия:

1. 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 84.

Таблица 84 – Описание параметров запроса на создание домена с делегированием

Параметр	Тип	Обязательность	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
hostname	Str	-	Имя домена
features.is_authorization	Bool	+	Если значение true, домен можно использовать для авторизации
features.is_mail	Bool	+	Если значение true, домен может принимать почтовые сообщения
features.is_service	Bool	+	Если значение true, домен можно использовать для авторизации по умолчанию
features.is_delegated	Bool	-	Если значение true, домен делегирован внешней системе

Параметр	Тип	Обязательность	Описание
<code>external.delegate_id</code>	Str	-	Идентификатор делегата, используемый для внешней авторизации
<code>external.domain_alias</code>	Str	-	Имя контроллера делегируемого домена
<code>external.default_region_id</code>	Str	-	Идентификатор региона по умолчанию для автоматического создания пользователей

Пример ответа:

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

7.7 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 52). Объект Организационной структуры необходимо создать для получения возможности создания объектов **Организаций**.

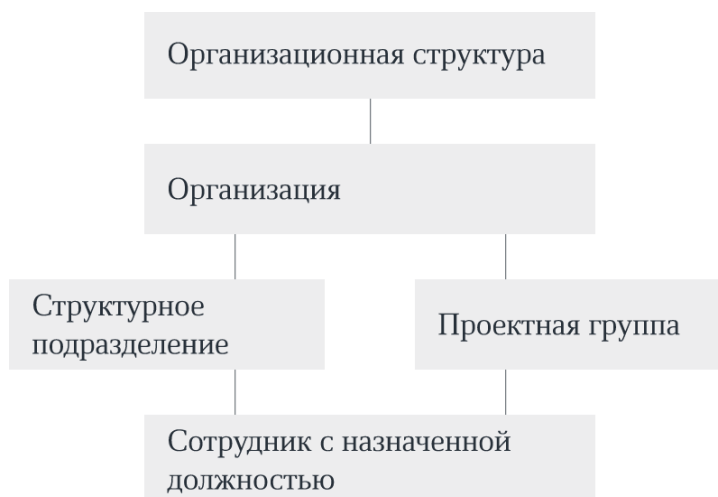


Рисунок 52 – Примерная схема организационной структуры

Важно – 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 получение конфигурационного файла **config_admin_example.json**, содержащего логин и пароль администратора установки:

```
nct_ministerium get_user_quotas_profile
--config /srv/ministerium/conf/config_admin_example.json
--entity_id 5fbe5408-fb8-4b64-800c-60ca4ac4081b
--tenant_id "01068ade-1cce-4125-ab6b-91d977ecf85b"
```

Описание параметров запроса приведено в таблице 85.

Таблица 85 – Описание параметров запроса на получение конфигурационного файла **config_admin_example.json**

Параметр	Тип	Обязательность	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
entity_id	Str	+	Идентификатор ресурса
tenant_id	Str	+	Идентификатор тенанта

2. Выполнить запрос на получение конфигурационного файла **config.json**:

```
nct_ministerium
--config /srv/ministerium/config.json list_tenants
```

Описание параметров запроса приведено в таблице 86.

Таблица 86 – Описание параметров запроса на получение конфигурационного файла config_admin_example.json

Параметр	Тип	Обязательность	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

3. 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 87.

Таблица 87 – Описание параметров запроса на создание оргструктуры

Параметр	Тип	Обязательность	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
element	Str	+	Данные сохраняемого объекта оргструктуры (строка в формате json)
element_type	Str	+	Тип элемента в оргструктуре на выбор

4. 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 88.

Таблица 88 – Описание параметров запроса на установку связи с тенантом

Параметр	Тип	Обязательность	Описание
config	Str	+	Конфигурационный файл с параметрами сервиса Cox и настройками tls. Формируется автоматически на сервере с ролью ucs_infrastructure и находится по пути /srv/ministerium/config.json
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
parent_id	Str	+	Идентификатор родительского элемента в оргструктуре
parent_type	Str	+	Тип родительского элемента оргструктуры
child_id	Str	+	Идентификатор дочернего элемента в оргструктуре
child_type	Str	+	Тип дочернего элемента оргструктуры

После создания объекта оргструктуры в Панели администрирования «Mailion» станет доступна функция создания организаций и подразделений.

7.8 Создание организации

Администратор может создать несколько организаций.

Важно – Нельзя создать организации с одинаковым именем в рамках одной оргструктуры.

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

Важно – Выполнять команду необходимо от имени администратора тенанта.

Для создания организации необходимо выполнить 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 89.

Таблица 89 – Описание параметров запроса на создание организации

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
element	Str	+	Данные сохраняемого объекта оргструктуры (строка в формате json)
element_type	Str	+	Тип элемента в оргструктуре на выбор
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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
tls_settings.ca_file	Bool	+	Путь к CA файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента

Пример ответа:

```

{
  "Response": {

```



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

7.9 Операции над пользователями, группами и ресурсами

При первой попытке создания пользователя, группы или ресурса с помощью интерфейса командной строки предусмотрено автоматическое выполнение следующих запросов:

- создание пользователя;
- создание E-mail;
- создание логина;
- создание пароля и токена к логину;
- добавление роли;
- активация.

При неудачном выполнении какого-либо из шагов необходимо выполнить запросы вручную. Примеры выполнения запросов приведены ниже:

1. Создание пользователя:

```
nct_ministerium create_user
--admin.login <...>
--admin.password <...>
--email <...>
--login <...>
--password lbpvOqD(8)j90YL+U7Jx
--region_id 05fc39ce-9b06-4437-ae09-f1276468a0b9
--tenant_id ff11f0a0-dcd5-4392-8a34-b18036640a08
--gal_tags 91e3f772-4828-5da3-957e-73fdbbc07ae8d
--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_cert.pem
--tls_settings.key_file /home/ps/work/first/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 90.

Таблица 90 – Описание параметров запроса на создание пользователя

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
email	Str	+	Основной электронный адрес
login	Str		Логин пользователя
password	Str	+	Пароль для логина пользователя
region_id	Str	+	Идентификатор региона
tenant_id	Str	+	Идентификатор тенанта
gal_tags	Str	+	Идентификаторы GAL-тегов
profile.first_name	Str	+	Имя создаваемого пользователя
profile.last_name	Str	+	Фамилия создаваемого пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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

Важно – При первом шаге создается объект (пользователь). При ошибке выполнения данного шага следующие запросы также не будут выполнены.

2. Создание E-mail:

```
nct_ministerium add_email
--admin.login <...>
--admin.password <...>
--email <...>
--entity_id 540712cd-0723-4dd3-9424-0912322eebbd
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none --cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false --cox.request_timeout=10s --cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/ps/work/first/mail-back-tests/certs/ca.pem
--tls_settings.client_cert_file /home/ps/work/first/mail-back-tests/certs/client_cert.pem
--tls_settings.key_file /home/ps/work/first/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 91.

Таблица 91 – Описание параметров запроса на создание E-mail

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
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 92.

Таблица 92 – Описание параметров запроса на создание логина

Параметр	Тип	Обязательность	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 93.

Таблица 93 – Описание параметров запроса на создание пароля и токена к логину

Параметр	Тип	Обязательность	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_cert.pem
--tls_settings.key_file /home/ps/work/first/mail-back-tests/certs/client_key.pem

```

Описание параметров запроса приведено в таблице 94.

Таблица 94 – Описание параметров запроса на создание профиля

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя профиля
gal_region_id	Str	+	Идентификатор региона, в котором создан GAL-тег
gal_tags	Str	+	Идентификаторы GAL-тегов
create	Str	-	Создание нового профиля
profile.birthday	Str	+	Дата рождения, в формате: ГГГГ-ММ-ДД
profile.addresses	Str	+	Список адресов пользователя профиля
profile.department	Str	+	Наименование подразделения компании профиля
profile.first_name	Str	+	Имя создаваемого пользователя профиля
profile.gender	Str	+	Пол пользователя профиля
profile.last_name	Str	+	Фамилия создаваемого пользователя профиля
profile.locale	Str	+	Локаль профиля
profile.middle_name	Str	+	Отчество пользователя профиля
profile.phones	Str	+	Список телефонных адресов пользователя профиля
profile.preferred_phone	Str	+	Признак предпочтительного номера пользователя профиля
profile.title	Str	+	Должность пользователя профиля
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса

Параметр	Тип	Обязательность	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
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

6. Добавление роли:

```
nct_ministerium update_roles
--admin.login <...>
--admin.password <...>
--entity_id 8c88d3b1-2c01-4dc7-bfe0-9182e291444c
--add_roles 54718e3a-6c7b-5c9f-b4de-a897c356cb5e
--remove_roles
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-mydomain.ru:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true -
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/ps/work/first/mail-back-tests/certs/ca.pem
--tls_settings.client_cert_file /home/ps/work/first/mail-back-tests/certs/client_cert.pem
--tls_settings.key_file /home/ps/work/first/mail-back-tests/certs/client_key.pem
```

Описание параметров запроса приведено в таблице 95.

Таблица 95 – Описание параметров запроса на добавление роли

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя профиля
add_roles	Str	+	Добавление ролей
remove_role	Str	+	Удаление ролей

Параметр	Тип	Обязательность	Описание
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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
tls_settings.ca_file	Bool	+	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

7. Активация:

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

Описание параметров запроса приведено в таблице 96.

Таблица 96 – Описание параметров запроса на активацию

Параметр	Тип	Обязательность	Описание
entity_id	Str	+	Идентификатор статуса
status	Str	+	Статус

В а ж н о – У несозданных объектов необходимо вручную выполнить те запросы, которые остались невыполненными автоматически.

7.10 Делегирование управления группами

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

Для этого необходимо выполнить запрос на выдачу прав на управление группой, назначив пользователю соответствующую роль:

```
nct_ministerium shared_access_grant
--admin.login <...>
--admin.password <...>
--emails autotest_1680079691.97499@installation.exaple.net,
autotest_1680079700.613669@installation.exaple.net,autotest_1680079668.730608@installat
ion.exaple.net,autotest_1680079682.528347@installation.exaple.net,autotest_1680079359.89
922@installation.exaple.net,autotest_1680079373.50339@installation.exaple.net,autotest_168
0079536.010099@installation.exaple.net
--delegate_email test_group_delegate_2@installation.exaple.net
--sharing_roles
GROUP_ADMINISTRATOR,GROUP_ADMINISTRATOR,GROUP_ADMINISTRATOR,
GROUP_ADMINISTRATOR,GROUP_ADMINISTRATOR,GROUP_ADMINISTRATOR,
GROUP_ADMINISTRATOR
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.exaple.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.exaple.net:3142
--cox.load_balanced=false
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=true
--cox.use_tls_balancer=false
--tls_settings.ca_file /home/user/mail-back-tests/certs/ca.pem
--tls_settings.client_cert_file /home/user/mail-back-tests/certs/client_cert.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 97.

Таблица 97 – Описание параметров запроса на выдачу прав на управление группой

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
emails	Str	+	Email пользователя/пользователей, которым будут делегированы права управления группой
delegate_email		+	Email группы, права на управление которой необходимо делегировать пользователю/пользователям
sharing_roles		+	Выбор из разрешенных к назначению ролей: – GROUP_EDITOR (Редактор группы); – GROUP_ADMINISTRATOR (Администратор группы)

Параметр	Тип	Обязательность	Описание
			Примечание – Обе представленные роли позволяют делегировать произвольному пользователю права на управление составом участников и редактирование данных группы.
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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

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

Пример ответа:

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

Важно – Процесс выдачи прав на управление группой может занять до одной минуты. По истечении данного времени пользователю станут доступны функции назначенной роли.

Чтобы отозвать права у пользователя/пользователей необходимо выполнить запрос:

```
nct_ministerium shared_access_revoke
--admin.login <...>
--admin.password <...>
--delegate_email group_1681355902_pwbgdstsrx@installation.exaple.net
--emails autotest_1681355888.981403@installation.exaple.net
```

Описание параметров запроса на отзыв прав в таблице 98.

Таблица 98 – Описание параметров запроса на отзыв прав

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
delegate_email		+	Email делегированной на управление группы
emails	Str	-	Email пользователя/пользователей, права на управление группой у которых будут отозваны

Примечание – Если необходимо отозвать права у всех пользователей, которым предварительно они были назначены, то следует оставить поле **emails** пустым.

Пример ответа:

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

7.11 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 99.

Таблица 99 – Описание параметров запроса на создание организационной группы

Параметр	Тип	Обязательность	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	+	Идентификаторы GAL-тегов
gal_region_id	Str	+	Идентификатор региона GAL
profile.name	Str	+	Имя создаваемой группы
profile.description	Str	+	Описание создаваемой группы

Пример ответа:

```

{
  "Response": {
    "msg": "ok",
    "changed": true
  },
  "id": "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 100.

Таблица 100 – Описание параметров запроса на создание динамической группы

Параметр	Тип	Обязательность	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».

Примечание – 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
}
```

7.12 Массовое создание пользователей в каталоге

Важно – 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 Г).
- Файл импорта, содержащий импортируемых в систему пользователей, в формате JSON (**user_profiles.json**) или CSV (**user_profiles.csv**). Пример заполняемых полей в файле приведен в разделе 7.12.1.

Примечание – Для каждого отдельного пользователя перед импортом система выполняет поиск пользователя по электронным адресам почты (emails) и логинам (logins). Если найдено совпадение, то вместо создания нового пользователя выполняется обновление данных. Обновляются все поля пользователя, за исключением электронных адресов и логинов – они будут добавлены.

2. Выполнить команду запуска импорта **import_users**. Перед выполнением непосредственного импорта выполнить первоначальную проверку данных, предоставляемых для импорта и настроек подключения к ПО «Mailion»:

- Выполнить непосредственный запуск импорта пользователей:

```
nct_ministerium import_users
--config import_config.json
```

Описание параметров запроса приведено в таблице 101.

Таблица 101 – Описание параметров запроса на импорт пользователей

Параметр	Тип	Обязательность	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 Г).

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

Описание параметров запроса приведено в таблице 102.

Таблица 102 – Описание параметров запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательность	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

Параметр	Тип	Обязательность	Описание
check	Str	+	Выполнение базовых проверок перед отправкой данных на сервер.

Пример ответа:

```
{
  "Response": {
    "msg": "ok"
  },
  "responses": [
    {
      "msg": "validation done, users to import: 1"
    }
  ]
}
```

Примечание – Команда **import_users** реализована таким образом, что поддерживает неоднократный запуск с одними и теми же параметрами, включая файл импорта.

3. Выполнить запрос на получение списка глобальных адресных книг, чтобы определить в какой GAL-тег определить создаваемых пользователей:

```
nct-ministerium get_tenant_gals
--config get_tenant_gals.json
```

Описание параметров запроса приведено в таблице 103.

Таблица 103 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательность	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 Г).

7.12.1 Подготовка файла импорта

Важно – 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 104.

Таблица 104 – Описание параметров файла импорта **user_profiles.json**

Параметр	Тип	Обязательность	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
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

Параметр	Тип	Обязательность	Описание
phones	Str	-	Список телефонных адресов
phones.number	Str	-	Номер телефона
phones.preferable	Str	-	Признак предпочтительного номера
phones.type	Str	-	Список типов номера
e mails	Str	+	Список электронных адресов пользователя
e mails.e mail	Str	+	Электронный адрес
e mails.primary	Str	+	Признак основного адреса
logins	Str	+	Список логинов пользователя
logins.login	Str	+	Логин
logins.password	Str	+	Пароль

Важно – Каждый отдельный пользователь проверяется по JSON-схеме записи пользователя, приведенной в приложении (см. раздел «Схема записи пользователя» в Приложении Г).

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

Описание параметров файла импорта **user_profiles.csv** приведено в таблице 105.

Таблица 105 – Описание параметров файла импорта **user_profiles.csv**

Параметр	Обязательность	Описание
correlation_id	+	Пользовательский идентификатор, уникальный в пределах файла импорта
first_name	+	Имя пользователя
e mail	+	Основной электронный адрес и логин
password	+	Пароль для логина, заданного полем e mail

7.12.2 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 106.

Таблица 106 – 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 «ок» 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 Г)
import procedure summary	Итог импорта, сообщает количество пользователей, которые были обработаны системой, количество пользователей с ошибками и количество успешно импортированных пользователей. В любом случае количество, указанное в полях «users to import» и «total reported results», должно быть одинаковым

7.12.3 Возможные ошибки при импорте пользователей

Описания возможных ошибок при импорте пользователя приведены в таблице 107.

Таблица 107 – 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
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: fl b97e81-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) "flb97e81-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: fl b97e81-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>{</pre>	Еще один пример проверки, выполняемой перед отправкой файла импорта на сервер. Здесь говорится о том, что у записей пользователя с идентификаторами (correlation_id)

Название ошибки	Вид в интерфейсе командной строки	Описание
	<pre>"msg": "import file validation: duplicate email found: 433bfcea-5adf-49ee-88e5- cfca9a575b6b@example.com (users correlation IDs: flb97e81-e4a3-4ebd- ba59-e4b864ef4797, 1d567e35-31ce- 461e-8a35-5efd2012362c)", "failed": true }</pre>	<pre>"flb97e81-e4a3-4ebd-ba59- e4b864ef4797" и "1d567e35-31ce- 461e-8a35-5efd2012362c" найдено повторение электронного адреса, его значение: "433bfcea-5adf-49ee- 88e5-cfca9a575b6b@example.com". Необходимо исправить электронный адрес у одного из пользователей</pre>
<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": "flb97e81-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 пользователя на стороне сервера, например по причине отказа сетевого окружения</p>

Название ошибки	Вид в интерфейсе командной строки	Описание
	<pre> }] } </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>
Ошибка проверки локали в записи пользователя	<pre> { "msg": "import file validation: user correlation ID: flb97e81-e4a3-4ebd-ba59-e4b864ef4797, check user locale: language: tag is not well-formed", "failed": true } </pre>	<p>Пример ошибки, которая выдается если локаль (locale) в записи пользователя не задана или задана 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**.

Примечание – Пользователи, не импортированные или частично импортированные в систему, записываются в файл **rejected_users.json**. При этом для каждого такого пользователя система выдаст сообщение об ошибке на экран. Найти конкретного пользователя в файле **rejected_users.json** можно по **correlation_id**.

7.13 Массовое создание групп в каталоге

Важно – Массовое создание пользователей выполняется пользователем с ролью администратора тенанта.

Массовое создание групп в каталоге осуществляется с помощью импорта групп из файла в формате **JSON** или **CSV**, [выгруженного из внешнего каталога](#) заранее или созданного любым другим способом.

Импорт групп из файла в систему осуществляется в два этапа:

- импорт групп непосредственно;
- импорт связей данных групп.

7.13.1 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 Г).
- Файл импорта, содержащий импортируемые в систему группы, в формате **JSON (groups.json)** или **CSV (groups.csv)**. Пример заполняемых полей в файлах приведен в разделе 7.13.3.

Примечание – Для каждой отдельной группы, перед импортом, система выполняет поиск группы по электронным адресам почты (**emails**) и логинам (**logins**). Если найдено совпадение, то вместо создания новой группы выполняется обновление данных. Обновляются все поля группы, за исключением электронных адресов и логинов – они будут добавлены. В результате импорта также может измениться основной электронный адрес на вновь импортированный. То есть, вновь импортированный станет основным (**primary**).

2. Выполнить команду запуска импорта **import_groups**. Перед выполнением непосредственного импорта необходимо выполнить первоначальную проверку данных, предоставляемых для импорта и настроек подключения к ПО «Mailion»:

- Выполнить непосредственный запуск импорта групп:

```
nct_ministerium import_groups
--config settings.json
```

Описание параметров запроса приведено в таблице 108.

Таблица 108 – Описание параметров запроса на импорт групп

Параметр	Тип	Обязательность	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 Г).

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

Описание параметров запроса приведено в таблице 109.

Таблица 109 – Описание параметров запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательность	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 to import: 1"
    }
  ]
}
```

Примечание – Команда **import_groups** реализована таким образом, что поддерживает неоднократный запуск с одними и теми же параметрами, включая файл импорта.

3. Выполнить запрос на получение списка глобальных адресных книг, чтобы определить в какой GAL-тег определить создаваемые группы:

```
nct-ministerium get_tenant_gals
--config get_tenant_gals.json
```

Описание параметров запроса приведено в таблице 110.

Таблица 110 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательность	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 Г).

7.13.2 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 Г).
 - Файл импорта, содержащий импортируемые в систему группы, в формате JSON (**groups_links.json**) или CSV (**groups_links.csv**). Пример заполняемых полей в файле приведен в разделе 7.13.3.
2. Выполнить команду запуска импорта **import_groups_links**. Перед выполнением непосредственного импорта выполнить первоначальную проверку данных, предоставляемых для импорта и настроек подключения к ПО «Mailion»:
 - Выполнить непосредственный запуск импорта пользователей:

```
nct_ministerium import_groups_links
--config settings.json
```

Описание параметров запроса приведено в таблице 111.

Таблица 111 – Описание параметров запроса на импорт связей групп

Параметр	Тип	Обязательность	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 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 Г).

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

Описание параметров запроса приведено в таблице 112.

Таблица 112 – Описание параметров запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательность	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"
  }
]
}

```

7.13.3 Подготовка файла импорта

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

Описание параметров файла импорта **groups.json** приведено в таблице 113.

Таблица 113 – Описание параметров файла импорта **groups.json**

Параметр	Тип	Обязательность	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 114.

Таблица 114 – Описание параметров файла импорта **groups.csv**

Параметр	Обязательность	Описание
correlation_id	+	Идентификатор группы. Должен быть уникален в пределах файла импорта. Система ссылается на этот идентификатор при информировании пользователя об успешности импорта отдельной группы или об ошибках, возникших в процессе импорта. Может быть произвольной строкой, например, идентификатор группы в системе, из которой производится перенос групп или случайно сгенерированный UUID
name	+	Название группы

Параметр	Обязательность	Описание
description	-	Описание группы
email	+	Электронная почта группы

7.13.4 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 115.

Таблица 115 – 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 «ок» 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 Г)
import procedure summary	Итог импорта, сообщает количество групп, которые были обработаны системой, количество групп с ошибками и количество успешно импортированных групп

7.13.5 Возможные ошибки при импорте групп

Описания возможных ошибок при импорте групп приведены в таблице 116.

Таблица 116 – 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
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>{</pre>	Сообщение выводится в случае, если группа с идентификатором

Название ошибки	Вид в интерфейсе командной строки	Описание
	<pre>"msg": "import file validation: group correlation ID: f1b97e81-e4a3-4ebd-ba59-e4b864ef4797: emails.0.email: Does not match format 'email", "failed": true }</pre>	(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>	Еще один пример проверки, выполняемой перед отправкой файла импорта на сервер. Здесь говорится о том, что у записей группы с идентификаторами (correlation_id) "f1b97e81-e4a3-4ebd-ba59-e4b864ef4797" и "1d567e35-31ce-461e-8a35-5efd2012362c" найдено повторение электронного адреса, его значение: "433bfcea-5adf-49ee-88e5-cfca9a575b6b@example.com". Необходимо исправить электронный адрес у одного из пользователей
Ошибка, возникшая в процессе импорта группы на стороне сервера	<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": {</pre>	Пример ошибки возникшей в процессе импорта группы на стороне сервера, например по причине отказа сетевого окружения

Название ошибки	Вид в интерфейсе командной строки	Описание
	<pre> "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>	
	<pre> group error </pre>	<p>В этом сообщении говорится о том, что группа с идентификатором, 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`.

Примечание – Группы, не импортированные или частично импортированные в систему, записываются в **rejected_groups.json**. При этом для каждой такой группы система выдаст сообщение об ошибке на экран. Найти конкретную группу в файле **rejected_groups.json** можно по **correlation_id**.

7.13.6 Автоматизация переноса групп и их связей из LDAP-каталогов в каталог ПО «Mailion»

При автоматизации экспорта необходимых групп и их связей из LDAP-каталога администратор использует утилиты, позволяющие выполнить следующие действия:

- отфильтровать необходимые для импорта в каталог ПО «Mailion» группы, задав фильтры LDAP Search;
- сохранить файл с результатами операции LDAP Search в формате LDIF (поддерживаются только записи **changetype: add**, записи **changetype: modify** не поддерживаются).

Пример команды экспорта из каталога Microsoft Active Directory (AD):

```
ldifde -f OUTPUT.LDF
-b администратор test-forest *
-s 10.1.1.50 -d "dc=test-forest,dc=local"
-r "(objectClass=group)"
```

Пример команды экспорта из каталога OpenLDAP/FreeIPA (командная строка Linux):

```
ldapsearch
-H ldap://10.1.1.50:389 -x
-D 'test-forest\администратор'
-w '****'
-b 'dc=test-forest,dc=local'
-s sub
-a always '(objectClass=group)' '*' > OUTPUT.LDF
```

Важно – Особенности экспорта из LDAP-каталога при помощи утилиты **ldifde**: такую утилиту обязательно нужно использовать без опции **"-m"**. **nct_ldif_converter** не обрабатывает **changetype**, отличный от **add**.

Для автоматизации импорта в каталог ПО «Mailion» предназначена утилита **nct_ldif_converter**. Полученный файл в формате LDIF может быть использован при запуске данной утилиты.

Пример корректной записи в LDIF файле (changetype: add):

```
dn: CN=TestGroup1,CN=Users,DC=test-forest,DC=local
changetype: add
objectClass: top
objectClass: group
cn: TestGroup1
description: PervayaGruppa opisanie
member: CN=GLOBALgroup,CN=Users,DC=test-forest,DC=local
member: CN=TestGroup2,CN=Users,DC=test-forest,DC=local
member: CN=UserTest1 a,CN=Users,DC=test-forest,DC=local
distinguishedName: CN=TestGroup1,CN=Users,DC=test-forest,DC=local
instanceType: 4
whenCreated: 20220725234749.0Z
whenChanged: 20220726211521.0Z
uSNCreated: 18915
info: PervayaGruppa zametka
memberOf: CN=GLOBALgroup,CN=Users,DC=test-forest,DC=local
memberOf: CN=TestGroup4,CN=Users,DC=test-forest,DC=local
memberOf: CN=TestGroup3,CN=Users,DC=test-forest,DC=local
uSNChanged: 19160
name: TestGroup1
objectGUID:: WjCoO3Tf40GUOw9s8N+ytw==
objectSid:: AQUAAAAAAAAUVA AAAVUO/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.

7.14 Массовое создание ресурсов в каталоге

Важно – 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 Г).
- Файл импорта, содержащий импортируемых в систему пользователей, в формате JSON (**resources.json**) или CSV (**resources.csv**). Пример заполняемых полей в файле приведен в разделе 7.12.1.

Примечание – 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 117.

Таблица 117 – Описание параметров запроса на импорт ресурсов

Параметр	Тип	Обязательность	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 Г).

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

Описание параметров запроса приведено в таблице 118.

Таблица 118 – Описание параметров запроса на проверку файла импорта, конфигурации и подключения к ПО «Mailion»

Параметр	Тип	Обязательность	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"
    }
  ]
}
```

Примечание – Команда **import_resources** реализована таким образом, что поддерживает неоднократный запуск с одними и теми же параметрами, включая файл импорта.

3. Выполнить запрос на получение списка глобальных адресных книг, чтобы определить в какой GAL-тег определить создаваемые ресурсы:

```
nct-ministerium get_tenant_gals
--config get_tenant_gals.json
```

Описание параметров запроса приведено в таблице 119.

Таблица 119 – Описание параметров запроса на получение GAL-тегов тенанта

Параметр	Тип	Обязательность	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 Г).

7.14.1 Подготовка файла импорта

Важно – 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 120.

Таблица 120 – Описание параметров файла импорта **user_profiles.json**

Параметр	Тип	Обязательность	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
room	Str	-	Кабинет
workplace	Str	-	Рабочее место
login	Str	+	Логин ресурса (с доменом или нет)

Параметр	Тип	Обязательность	Описание
password	Str	+	Пароль
autobook	Str	-	Автоматическое бронирование ресурса
minimal_participation_number	Str	+	Минимальное количество участников

Важно – Каждый отдельный объект ресурса проверяется по JSON-схеме записи пользователя, приведенной в приложении (см. раздел «Схема записи ресурса» в Приложении Г).

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

Описание параметров файла импорта **user_profiles.csv** приведено в таблице 121.

Таблица 121 – Описание параметров файла импорта **user_profiles.csv**

Параметр	Обязательность	Описание
correlation_id	+	Идентификатор ресурса, уникальный в пределах файла импорта
name	+	Название ресурса
email	+	Основной электронный адрес и логин
password	+	Пароль для логина, заданного полем email

7.14.2 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 122.

Таблица 122 – Описание сообщений системы

Сообщение	Описание
import file verification starts, it will take some time	Процесс локальной проверки файла импорта запущен. Такая проверка осуществляется при каждом запуске, до отправки файла импорта на сервер. Время проверки зависит от количества пользователей, переданных для импорта, и может занимать значительное время
resource imported	Сообщение о том, что ресурс успешно импортирован. Об этом говорит маркер «ok» в поле «status». Идентификатор импортируемой записи сообщается в поле «correlation_id»
validation done, resources to import	Сообщает о том, что проверка файла импорта прошла успешно и обнаружен один ресурс для импорта. Это сообщение появится только в том случае, если все ресурсы прошли проверку по схеме
import procedure summary	Итог импорта, сообщает количество ресурсов, которые были обработаны системой, количество ресурсов с ошибками и количество успешно импортированных ресурсов

7.14.3 Возможные ошибки при импорте объектов ресурсов

Описания возможных ошибок при импорте объектов ресурсов приведены в таблице 123.

Таблица 123 – Описание возможных ошибок

Название ошибки	Вид в интерфейсе командной строки	Описание
Ошибка декодирования JSON	{	Сообщение выводится в случае, если утилита не может

Название ошибки	Вид в интерфейсе командной строки	Описание
	<pre>"msg": "import file validation: decode next user: decode JSON: invalid character '}' looking for beginning of value", "failed": true }</pre>	<p>декодировать файл импорта, в этом случае необходимо проверить корректность синтаксиса JSON или CSV</p>
Повторяющийся correlation ID	<pre>{ "changed": false, "failed": true, "msg": "import file validation: duplicate correlation_id found: 00025fe9-1fb5- 4fda-a6ac-c8fb5572b88f" }</pre>	<p>Сообщение выводится в случае, если две записи ресурса в файле имеют одинаково заполненное поле correlation ID</p>
Пустой correlation ID	<pre>{ "changed": false, "failed": true, "msg": "import file validation: resource correlation ID: : resource CorrelationId is empty" }</pre>	<p>Сообщение выводится в случае, если поле correlationID не заполнено</p>
Ошибка создания Email	<pre>{ "Response": { "changed": true, "failed": false, "msg": "ok" }, "responses": [{ "changed": false, "failed": false, "msg": "validation done, resources to import: 1" }, { "changed": true, "failed": false, "msg": "import procedure summary: total reported results: 1, errors: 1, success: 0" }] }</pre>	<p>Сообщение выводится в случае ошибки создания Email</p>

Возможен сценарий, при котором файл импорта выгружается несколько раз с какими-либо уточнениями из системы-источника и каждый раз (кроме первого) происходит обновление объектов ресурсов в ПО «Mailion». Кроме повторного запуска с исправленными/уточненными данными в исходном файле импорта также допускается импорт файла **rejected_resources.json**, после исправлений ошибок о которых система оповестила в процессе импорта. Для этого путь к файлу **rejected_resources.json** нужно указать в параметре `user_data_path`, не допустив при этом пересечения имени с параметром **rejected_resources_path**.

Примечание – Ресурсы, не импортированные в систему или частично импортированные, записываются в **rejected_resources.json**. При этом для каждого такого объекта ресурса система выдаст сообщение об ошибке на экран. Найти конкретный объект ресурса в файле **rejected_resources.json** можно по **correlation_id**.

7.15 Настройка миграции данных календаря

Важно – Для миграции данных необходимо использовать Microsoft Exchange версии 2013 и выше.

Для запуска миграции календаря необходимо выполнить следующие действия:

1. Зайти на машину через SSH, например `ssh <username>@<host>`, где `<host>` - имя хоста из inventory, где расположен сервис kex.
2. Выполнить команду **docker exec -ti kex bash**.
3. Внутри контейнера с kex перейти в каталог **cd /usr/local/bin**. В каталоге **/usr/local/bin** находятся утилиты для миграций календаря:
 - `ucs-exch-to-mln-migrator` (подробнее о запуске миграции календаря из Microsoft Exchange в ПО «Mailion», см. раздел 7.15.1);
 - `ucs-mln-to-exch-migrator` (подробнее о запуске миграции календаря из ПО «Mailion» в Microsoft Exchange, см. раздел 7.15.2).
4. Внутри контейнера kex перейти в каталог **/etc/ucs/kex**. В нем находятся конфигурационные файлы для миграции календаря:
 - `/etc/ucs/kex/calendar_exch_to_mln_migrator.json`;

– /etc/ucs/kex/calendar_mln_to_exch_migrator.json.

Важно – Выполнение миграции вместе с включенной синхронизацией невозможно. Перед началом миграции необходимо отключить синхронизацию. Начиная с версии Malion 1.5.1 миграция не будет стартовать при включенной синхронизации. Примеры команд для отключения синхронизации приведены ниже:

Пример команды отключения синхронизации для домена:

```
nct_ministerium update_domain \
--config ministerium.json
--id= <...>
--features.is_mail=true \
--features.is_authorization=true \
--features.is_service=true \
--external.is_sync_enabled=false \
```

Описание параметров отключения синхронизации для домена приведено в таблице 124.

Таблица 124 – Описание параметров отключения синхронизации для домена

Параметр	Тип	Обязательность	Описание
config	Str	+	Логин администратора тенанта
id	Str	+	Идентификатор домена
features.is_mail	Bool	+	Если значение true , домен может принимать почтовые сообщения
features.is_authorization	Bool	+	Если значение true , домен можно использовать для авторизации
features.is_service	Bool	+	Если значение true , домен можно использовать для авторизации по умолчанию
external.is_sync_enabled	Bool	+	Включение/отключение синхронизации. Если значение false , то выключена. Если значение true , то включена

Пример ответа:

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

Пример команды отключения синхронизации для конкретного пользователя:

```
nct_ministerium set_sync_block_setting_for_user \
--config <путь до конфигурационного файла>
--login <...>
--setBlock=true \
--enableImmediatly=false
```

Описание параметров отключения синхронизации для конкретного пользователя приведено в таблице 125.

Таблица 125 – Описание параметров отключения синхронизации для конкретного пользователя

Параметр	Тип	Обязательность	Описание
config	Str	+	Путь до конфигурационного файла
login	Str	+	Логин пользователя
setBlock	Bool	+	Установка блокировки синхронизации (для тенанта или пользователя). Если значение true , то заблокирована, false – разблокирована
enableImmediatly	Bool	+	Снять/проставить галочки в настройках. Если значение false , то галочки сняты, true – галочки установлены

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "changed_entity_id": "ид измененного пользователя"
}
```

Пример команды отключения синхронизации для тенанта:

```
nct_ministerium set_sync_block_setting_for_all_users_in_tenant \
--config <путь до конфигурационного файла>
--tenantId <...>
--setBlock=true \
--enableImmediatly=false \
```

Описание параметров отключения синхронизации для тенанта приведено в таблице

Таблица 126 – Описание параметров отключения синхронизации для тенанта

Параметр	Тип	Обязательность	Описание
config	Str	+	Путь до конфигурационного файла
login	Str	+	Логин пользователя
tenantId	Str	+	Идентификатор тенанта
enableImmidiately	Bool	+	Снять/проставить галочки в настройках. Если значение false , то галочки сняты, true – галочки установлены

Пример ответа:

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

7.15.1 Миграция данных календаря из Microsoft Exchange в ПО «Mailion»

Мигратор представляет собой отдельный исполняемый файл. Для запуска мигратора необходимо выполнить запрос:

```
./ucs-exch-to-mln-migrator
--from user@user@ad.example.net
--to user@user@installation.example.net
--ignore-errors=true
--from-time 2022-07-17T15:04:05Z
--to-time time 2023-07-17T15:04:05Z
-c /path/to/config.json
```

Важно – Миграция пользователей должна производиться только в одноименные аккаунты.

Описание параметров запроса приведено в таблице 127.

Таблица 127 – Описание параметров запроса на вызов мигратора

Параметр	Тип	Обязательность	Описание
from	Str	+	Почтовый адрес пользователя Microsoft Exchange, чьи календарные данные будут мигрировать. Пример записи пользователя в данном параметре для однодоменной делегации: user@ad.example.net.

Параметр	Тип	Обязательность	Описание
			Пример записи пользователя в данном параметре для мультидоменной делегации: – пользователь Microsoft Exchange – user@ad.example.net; – пользователь ПО «Mailion» – user@installation.example.net
to	Str	+	Почтовый адрес пользователя, на который мигрируют календарные данные. Пример записи пользователя в данном параметре для однодоменной делегации: user@ad.example.net. Пример записи пользователя в данном параметре для мультидоменной делегации: – пользователь Microsoft Exchange – user@ad.example.net; – пользователь ПО «Mailion» – user@installation.example.net
ignore-errors	Bool	+	Значение по умолчанию true . Отвечает за продолжение работы мигратора в случае ошибок (ошибки попадают в журнал работы системы. Пример записи в журнале работы системы приведен ниже). Если значение false , процесс миграции останавливается при первой ошибке
from-time	Str	-	Параметр для указания даты, начиная с которой необходимо перенести события из календаря. Пример формата времени: 2015-07-17T15:04:05Z (RFC3339)
to-time	Str	-	Параметр для указания даты, до которой необходимо перенести события из календаря. Пример формата времени: 2015-07-17T15:04:05Z (RFC3339)
c	Str	+	Путь к конфигурационному файлу (по умолчанию "internal/config/config.local.json")

Важно – Можно указать только один параметр времени: **from-time** или **to-time**.
Временной промежуток может быть не более двух лет. При указании одного из параметров, второй будет вычислен автоматически путем прибавления или вычитания двух лет.

Пример записи в журнале работы системы:

```
./ 2023-07-18T19:56:18.342+0200INFOexch-to-mln-migrator/main.go: 151 {
  "migration": {
    "date": "2023-07-18 19:56:10.06591495 +0200 CEST m=+2.050583246",
    "mailion_email": "bdad1@installation.example.net",
```

```

"exchange_email": "bdad1@ad.example.net",
"errors": {
  "num_folders": 1,
  "folders": {
    "AmazingCal": [
      {
        "error": "send request: 1: import event
AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmlwNDk5ZABGAAAAAAB
OC/xo0g9rQr2266gF2feqBwDBZPRHK3THT7Vxk0IMFP/sAAASj75BAADBZPRHK3THT7Vxk01
MFP/sAAASj8YVAAA="
      },
      {
        "error": "send request: 2: import event
AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmlwNDk5ZABGAAAAAAB
OC/xo0g9rQr2266gF2feqBwDBZPRHK3THT7Vxk0IMFP/sAAASj75BAADBZPRHK3THT7Vxk01
MFP/sAAASj8YUAAA="
      },
      {
        "error": "send request: 3: import event
AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmlwNDk5ZABGAAAAAAB
OC/xo0g9rQr2266gF2feqBwDBZPRHK3THT7Vxk0IMFP/sAAASj75BAADBZPRHK3THT7Vxk01
MFP/sAAASj8YTAAA="
      }
    ],
  }
},
"current_status": {
  "exchange": {
    "folders": {
      "AmazingCal": {
        "num_objects": 3,
        "ews_id":
"AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmlwNDk5ZAAuAAAAAAB
OC/xo0g9rQr2266gF2feqAQDBZPRHK3THT7Vxk0IMFP/sAAASj75BAAA="
      },
      "Дни рождения": {
        "num_objects": 0,
        "ews_id":
"AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmlwNDk5AGQALgAAA04L
/GjSD2tCvbbrrqAXZ96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIbTAAAAA=="
      },
      "Задачи": {
        "num_objects": 0,

```

```

    "ews_id":
    "AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmlwNDk5AGQALgAAA04L
    /GjSD2tCvbbrrqAXZ96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBegAAAA=="
  },
  "Календарь": {
    "num_objects": 4,
    "ews_id":
    "AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmlwNDk5AGQALgAAA04L
    /GjSD2tCvbbrrqAXZ96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBDQAAAA=="
  }
},
"num_folders": 4
},
"mailion": {
  "folders": {
    "AmazingCal": {
      "num_objects": 3,
      "ews_id":
      "AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmlwNDk5ZAAuAAAAAAB
      OC/xo0g9rQr2266gF2feqAQDBZPRHK3THT7Vxk0IMFP/sAAASj75BAAA="
    },
    "Дни рождения": {
      "num_objects": 0,
      "ews_id":
      "AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmlwNDk5AGQALgAAA04L
      /GjSD2tCvbbrrqAXZ96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBTAAAAA=="
    }
  },
  "num_folders": 3
}
}
}
}

```

Пример конфигурационного файла приведен в приложении (см. раздел «Конфигурационный файл для миграции календаря из Microsoft Exchange в ПО "Mailion"» в Приложении Г).

7.15.2 Миграция данных календаря из ПО «Mailion» в Microsoft Exchange

Мигратор представляет собой отдельный исполняемый файл. Для запуска мигратора необходимо выполнить запрос:

```
./ucs-mln-to-exch-migrator
--from user@user@installation.example.net
--to user@user@ad.example.net
--ignore-errors=true
--from-time 2023-07-17T15:04:05Z
-c /path/to/config.json
```

Описание параметров запроса приведено в таблице 128.

Таблица 128 – Описание параметров запроса на вызов мигратора

Параметр	Тип	Обязательность	Описание
from	Str	+	Почтовый адрес пользователя Microsoft Exchange, чьи календарные данные будут мигрировать. Пример записи пользователя в данном параметре для однодоменной делегации: user@ad.example.net. Пример записи пользователя в данном параметре для мультидоменной делегации: – пользователь Microsoft Exchange – user@ad.example.net; – пользователь ПО «Mailion» – user@installation.example.net
to	Str	+	Почтовый адрес пользователя, на который мигрируют календарные данные. Пример записи пользователя в данном параметре для однодоменной делегации: user@ad.example.net. Пример записи пользователя в данном параметре для мультидоменной делегации: – пользователь Microsoft Exchange – user@ad.example.net; – пользователь ПО «Mailion» – user@installation.example.net
ignore-errors	Bool	+	Значение по умолчанию true . Отвечает за продолжение работы мигратора в случае ошибок (ошибки попадают в журнал работы системы. Пример записи в журнале работы системы приведен ниже). Если значение false , процесс миграции останавливается при первой ошибке
from-time	Str	-	Параметр для указания даты, начиная с которой необходимо перенести события из календаря

Параметр	Тип	Обязательность	Описание
to-time	Str	-	Параметр для указания даты, до которой необходимо перенести события из календаря
c	Str	+	Путь к конфигурационному файлу (по умолчанию "internal/config/config.local.json")

Важно – Можно указать один параметр времени: **from-time** или **to-time**. Если указан только параметр **from-time**, то перенесутся все события, начиная с указанной даты, и за последующие пять лет. Если указан только параметр **to-time**, то перенесутся все события с начала до указанной даты.

Пример записи в журнале работы системы:

```
./ 2023-07-18T19:56:18.342+0200INFOexch-to-mln-migrator/main.go: 151 {
  "migration": {
    "date": "2023-07-18 19:56:10.06591495 +0200 CEST m+=+2.050583246",
    "mailion_email": "bdad1@installation.example.net",
    "exchange_email": "bdad1@ad.example.net",
    "errors": {
      "num_folders": 1,
      "folders": {
        "AmazingCal": [
          {
            "error": "send request: 1: import event
AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmIwNDk5ZABGAAAAAAB
OC/xo0g9rQr2266gF2feqBwDBZPRHK3THT7Vxk0IMFP/sAAASj75BAADBZPRHK3THT7Vxk01
MFP/sAAASj8YVAAA="
          },
          {
            "error": "send request: 2: import event
AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmIwNDk5ZABGAAAAAAB
OC/xo0g9rQr2266gF2feqBwDBZPRHK3THT7Vxk0IMFP/sAAASj75BAADBZPRHK3THT7Vxk01
MFP/sAAASj8YUAAA="
          },
          {
            "error": "send request: 3: import event
AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmIwNDk5ZABGAAAAAAB
OC/xo0g9rQr2266gF2feqBwDBZPRHK3THT7Vxk0IMFP/sAAASj75BAADBZPRHK3THT7Vxk01
MFP/sAAASj8YTAAA="
          }
        ],
      }
    },
    "current_status": {
```

```

"exchange": {
  "folders": {
    "AmazingCal": {
      "num_objects": 3,
      "ews_id":
"AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmlwNDk5ZAAuAAAAAB
OC/so0g9rQr2266gF2feqAQDBZPRHK3THT7Vxk0IMFP/sAAASj75BAAA="
    },
    "Дни рождения": {
      "num_objects": 0,
      "ews_id":
"AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmlwNDk5AGQALgAAA04L
/GjSD2tCvbbrrqAXZ96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBTAAAAA=="
    },
    "Задачи": {
      "num_objects": 0,
      "ews_id":
"AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmlwNDk5AGQALgAAA04L
/GjSD2tCvbbrrqAXZ96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBegAAAA=="
    },
    "Календарь": {
      "num_objects": 4,
      "ews_id":
"AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmlwNDk5AGQALgAAA04L
/GjSD2tCvbbrrqAXZ96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBDQAAAA=="
    }
  },
  "num_folders": 4
},
"mailion": {
  "folders": {
    "AmazingCal": {
      "num_objects": 3,
      "ews_id":
"AAMkADdhOGQ1YThmLWE1NTUtNDZmMy04NmExLTc4YjgxMmlwNDk5ZAAuAAAAAB
OC/so0g9rQr2266gF2feqAQDBZPRHK3THT7Vxk0IMFP/sAAASj75BAAA="
    },
    "Дни рождения": {
      "num_objects": 0,
      "ews_id":
"AQMkADdhOGQ1YThmLWE1NQEtNDZmMy04NmExLTc4YjgxMmlwNDk5AGQALgAAA04L
/GjSD2tCvbbrrqAXZ96oBAMFk9EcrdMdPtXGTSUwU/+wAAAIBTAAAAA=="
    },
    "Календарь": {
      "num_objects": 4
    }
  },
}

```

```
"num_folders": 3
}
}
}
```

Пример конфигурационного файла приведен в приложении (см. раздел «**Конфигурационный файл для миграции календаря из ПО «Mailion» в Microsoft Exchange**» в Приложении Г).

Важно – Событие мигрирует только для организатора и в календарь, выбранный по умолчанию.

7.16 Настройка миграции почты

Важно – Для миграции данных необходимо использовать Microsoft Exchange версии 2013 и выше.

Для запуска миграции почты необходимо выполнить следующие действия:

1. Зайти на машину через SSH, например `ssh <username>@<host>`, где <host> - имя хоста из inventory, где расположен сервис viper.
2. Выполнить команду `docker exec -ti viper bash`.
3. Внутри контейнера с viper перейти в каталог `cd /usr/local/bin`. В каталоге `/usr/local/bin` находится утилита для миграции почты: `ucs-mail-mln-exch-migrator` (подробнее о запуске миграции почты из ПО «Mailion» в Microsoft Exchange см. 7.15.2).
4. Внутри контейнера viper перейти в каталог `/etc/ucs/viper`. В нем находится конфигурационный файл для миграции почты: `/etc/ucs/viper/mail_exch_mln_migrator.json`.

Важно – **Выполнение миграции вместе с включенной синхронизацией невозможно. Перед началом миграции необходимо отключить синхронизацию.** Начиная с версии Mailion 1.5.1 миграция не будет стартовать при включенной синхронизации. Примеры команд для отключения синхронизации приведены ниже:

Пример команды отключения синхронизации для домена:

```
nct_ministerium update_domain \
```



```
--config ministerium.json
--id= <...>
--features.is_mail=true \
--features.is_authorization=true \
--features.is_service=true \
--external.is_sync_enabled=false \
```

Описание параметров отключения синхронизации для домена приведено в таблице 129.

Таблица 129 – Описание параметров отключения синхронизации для домена

Параметр	Тип	Обязательность	Описание
config	Str	+	Логин администратора тенанта
id	Str	+	Идентификатор домена
features.is_mail	Bool	+	Если значение true , домен может принимать почтовые сообщения
features.is_authorization	Bool	+	Если значение true , домен можно использовать для авторизации
features.is_service	Bool	+	Если значение true , домен можно использовать для авторизации по умолчанию
external.is_sync_enabled	Bool	+	Включение/отключение синхронизации. Если значение false , то выключена. Если значение true , то включена

Пример ответа:

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

Пример команды отключения синхронизации для конкретного пользователя:

```
nct_ministerium set_sync_block_setting_for_user \
--config <путь до конфигурационного файла>
--login <...>
--setBlock=true \
--enableImmidiately=false
```

Описание параметров отключения синхронизации для конкретного пользователя приведено в таблице 130.

Таблица 130 – Описание параметров отключения синхронизации для конкретного пользователя

Параметр	Тип	Обязательность	Описание
config	Str	+	Путь до конфигурационного файла
login	Str	+	Логин пользователя
setBlock	Bool	+	Установка блокировки синхронизации (для тенанта или пользователя). Если значение true , то заблокирована, false – разблокирована
enableImmediatly	Bool	+	Снять/проставить галочки в настройках. Если значение false , то галочки сняты, true – галочки установлены

Пример ответа:

```
{
  "Response": {
    "changed": true,
    "failed": false,
    "msg": "ok"
  },
  "changed_entity_id": "ид измененного пользователя"
}
```

Пример команды отключения синхронизации для тенанта:

```
nct_ministerium set_sync_block_setting_for_all_users_in_tenant \
--config <путь до конфигурационного файла>
--tenantId <...>
--setBlock=true \
--enableImmediatly=false \
```

Описание параметров отключения синхронизации для тенанта приведено в таблице 131.

Таблица 131 – Описание параметров отключения синхронизации для тенанта

Параметр	Тип	Обязательность	Описание
config	Str	+	Путь до конфигурационного файла
login	Str	+	Логин пользователя
tenantId	Str	+	Идентификатор тенанта
enableImmediatly	Bool	+	Снять/проставить галочки в настройках. Если значение false , то галочки сняты, true – галочки установлены

Пример ответа:

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

7.16.1 Миграция данных почты из Microsoft Exchange в ПО «Mailion»

Мигратор представляет собой отдельный исполняемый файл. Для вызова мигратора выполнить запрос:

```
./ucs-mail-exch-mln-migrator
-c mail_exch_mln_migrator.json
-from userexch1@installation.example.net
-to usermln2@installation.example.net
-direction to-mln
```

Описание параметров запроса приведено в таблице 132.

Таблица 132 – Описание параметров запроса на вызов мигратора

Параметр	Тип	Обязательность	Описание
from	Str	+	Учетная запись (principal name) пользователя Microsoft Exchange, чьи почтовые данные будут мигрировать
to	Str	+	Учетная запись пользователя, на который мигрируют данные почты
c	Str	+	Путь к конфигурационному файлу (по умолчанию "internal/config/config.local.json")
direction	Str	+	Направление миграции может быть либо to-ex либо to-mln, в случае миграции из Microsoft Exchange в ПО «Mailion» указывать to-mln

Пример конфигурационного файла приведен в приложении (см. раздел «Конфигурационный файл для миграции почты из Microsoft Exchange в ПО «Mailion», из ПО «Mailion» в Microsoft Exchange» в Приложении Г).

Примечание – При миграции данных почты из Microsoft Exchange в ПО «Mailion» также происходит миграция всех созданных пользователем текстовых подписей и почтовых правил.

7.16.2 Поддерживаемые правила при миграции данных почты

При миграции данных почты из Microsoft Exchange в ПО «Mailion» поддерживается перенос правил (фильтров) со следующими условиями:

- получено в течение указанного периода;
- моего имени нет в поле «Кому»;
- мое имя присутствует в поле «Копия»;
- мое имя содержится в поле «Кому»;
- в списке получателей указано только мое имя;
- мое имя присутствует в строке «Кому» или «Копия»;
- адрес получателя содержит эти слова»;
- адрес отправителя содержит»;
- тема содержит эти слова»;
- получатель ...;
- получено от ...;
- с вложением.

При миграции данных почты из Microsoft Exchange в ПО «Mailion» поддерживается перенос правил со следующими действиями:

- пометить сообщение как прочтенное;
- перенаправлять сообщения;
- пересылать сообщения;
- пометить как нежелательное;
- удалять сообщение;
- перемещать сообщения в папку.

При миграции присутствуют следующие ограничения:

1. Если почтовое правило было изменено в Microsoft Exchange, то при повторной миграции данных почты из Microsoft Exchange правило не изменится в ПО «Mailion».
2. В ПО «Mailion» отсутствует:
 - поддержка исключения из правил;
 - условие «Для всех входящих»;

- действие «Применить ко всем сообщениям», но есть функционал применения правила к папке;
- классификация сообщений: тип, категория, конфиденциальность, флаг;
- поддержка нескольких уровней важности: у сообщений в ПО «Mailion» один уровень важности, а в Microsoft Exchange три (в веб-интерфейсе ПО «Mailion» три уровня важности, но в сервисе этот параметр имеет тип **bool**);
- функционал голосовых сообщений.
- функционал отправки SMS-сообщений.

7.16.3 Миграция данных почты из ПО «Mailion» в Microsoft Exchange

Мигратор представляет собой отдельный исполняемый файл. Для запуска мигратора необходимо выполнить запрос:

```
./ucs-mail-mln-exch-migrator
-c mail_exch_mln_migrator.json
--from usermln1@installation.example.net
--to userexch1@installation.example.net
-direction to-ex
```

Описание параметров запроса приведено в таблице 133.

Таблица 133 – Описание параметров запроса на вызов мигратора

Параметр	Тип	Обязательность	Описание
from	Str	+	Учетная запись пользователя ПО «Mailion», чьи почтовые данные будут мигрировать
to	Str	+	Учетная запись (principal name) пользователя, на почтовый ящик которого мигрируют данные почты
c	Str	+	Путь к конфигурационному файлу (по умолчанию "internal/config/config.local.json")
direction	Str	+	Направление миграции может быть либо to-ex либо to-mln, в случае миграции в exchange из mailion указывать to-ex

Пример конфигурационного файла приведен в приложении (см. раздел «Конфигурационный файл для миграции почты из Microsoft Exchange в ПО «Mailion», из ПО «Mailion» в Microsoft Exchange» в Приложении Г).

7.17 Управление делегированием учетных записей

Важно – Управление делегированием учетной записи выполняется пользователем с ролью администратора тенанта.

Делегирование учетной записи пользователя другому пользователю может быть выполнено с разными уровнями доступа. При выполнении запроса на делегирование учетной записи в параметре **permissions_by_emails** можно установить значения 0, 1 и 2 уровня доступа:

- 0 – уровень доступа «Не может» (Cannot). Пользователь, которому предоставлены права на учетную запись, получает доступ к учетной записи, права совладельца на все почтовые папки, календари и адресные книги, но не может писать письма от имени делегированной учетной записи.
- 1 – уровень доступа «От имени» (OnBehalf). Пользователь, которому предоставили права на учетную запись, получает доступ к учетной записи, 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 «Отправить как» (SendAs). Пользователь, которому предоставили права на учетную запись, получает доступ к учетной записи, права совладельца на все почтовые папки, календари и адресные книги, также он может отправлять письма от имени делегированной учетной записи.

7.17.1 Делегирование с уровнем доступа «Не может» (Cannot)

Для делегирования учетной записи пользователя другому пользователю с уровнем доступа «Не может» (Cannot) 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 134.

Таблица 134 – Описание параметров запроса на делегирование учетной записи пользователя с уровнем доступа «Не может» (Cannot)

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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 установки доступа: 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"
  }
}
```

7.17.2 Делегирование с уровнем доступа «От имени» (OnBehalf)

Для делегирования учетной записи пользователя другому пользователю с уровнем доступа «От имени» (OnBehalf) 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 135.

Таблица 135 – Описание параметров запроса на делегирование учетной записи пользователя с уровнем доступа «От имени» (OnBehalf)

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия

Параметр	Тип	Обязательность	Описание
cox.endpoint	Str	+	Endpoint 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 установки доступа: 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"
  }
}
```

7.17.3 Делегирование с уровнем доступа «Отправить как» (SendAs)

Для делегирования учетной записи пользователя другому пользователю с уровнем доступа «Отправить как» (SendAs) 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 136.

Таблица 136 – Описание параметров запроса на делегирование учетной записи пользователя с уровнем доступа «Отправить как» (SendAs)

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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 установки доступа: 0 – разрешение «Не может» (Cannot), 1 – разрешение «От имени» (OnBehalf), 2 – разрешение «Отправить как» (SendAs)

Параметр	Тип	Обязательность	Описание
<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

Пример ответа:

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

7.17.4 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 137.

Таблица 137 – Описание параметров запроса на отзыв доступа к делегированной учетной записи у всех делегатов

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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
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:

```
net_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 138.

Таблица 138 – Описание параметров запроса на проверку наличия делегатов

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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
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
}
```

7.17.5 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 139.

Таблица 139 – Описание параметров запроса на отзыв доступа к делегированной учетной записи у определенного делегата

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint сервиса

Параметр	Тип	Обязательность	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
emails	Str	+	Учетная запись пользователя, которому делегируют
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"
  }
}
```

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 140.

Таблица 140 – Описание параметров запроса на проверку наличия делегатов

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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
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
}
```

7.17.6 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 141.

Таблица 141 – Описание параметров запроса на проверку всех пользователей, которым делегирована учетная запись

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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 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": "user2@example.net",
          "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2",
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "primary": true
        }
      ],
      "logins": [
        {
          "id": "95622080-5064-5ee4-b6fb-26594a2f9387",
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "login": "user2@example.net",
          "auth_type": 1,
          "attributes": {
            "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2"
          }
        },
        "SecondFactorParams": null
      ]
    },
    "Payload": {
      "User": {
        "locale": "ru_RU"
      }
    },
    "status": 2,
    "shared_access": {}
  }
],
```

```
"Count": 1  
}
```

В случае отсутствия делегированных пользователей у учетной записи ожидается ответ вида:

```
{  
  "Response": {  
    "changed": false,  
    "failed": false,  
    "msg": "ok"  
  },  
  "Entities": null,  
  "Count": 0  
}
```

7.17.7 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 142.

Таблица 142 – Описание параметров запроса на проверку всех делегированных учетных записей выбранного пользователя

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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 ползователя

Параметр	Тип	Обязательность	Описание
<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

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "Entities": [
    {
      "id": "925c704b-1815-4250-890c-a4048feb748a",
      "type": 1,
      "tenant_id": "a3bbba13-686a-485b-8878-3d0642018cc8",
      "region_id": "2dbacea3-5889-4021-8f38-bc2214dd7423",
      "roles": [
        "c4b1f72c-672d-5ace-8a6d-96edc21227de"
      ],
      "emails": [
        {
          "id": "95622080-5064-5ee4-b6fb-26594a2f9387",
          "email": "user1@example.net",
          "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2",
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "primary": true
        }
      ],
      "logins": [
        {
          "id": "95622080-5064-5ee4-b6fb-26594a2f9387",
          "entity_id": "925c704b-1815-4250-890c-a4048feb748a",
          "login": "user1@example.net",
          "auth_type": 1,
          "attributes": {
            "domain_id": "6bb5e324-9e1f-5cde-9844-504d2465ddf2"
          }
        },
        "SecondFactorParams": null
      ]
    }
  ],
  "Payload": {
    "User": {
```

```

    "locale": "ru_RU"
  }
},
"status": 2,
"shared_access": {
  "permissions": {
    "d59ed675-0218-486c-8941-c245b3e3a306": {
      "account": {
        "role": 3
      },
      "mail": {
        "send_policy": 2
      }
    }
  }
}
},
],
"Count": 1
}

```

В случае отсутствия делегированных учетных записей ожидается ответ вида:

```

{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "Entities": null,
  "Count": 0
}

```

7.18 Поиск писем по заданным критериям

Важно – Поиск писем всех пользователей в тенанте по заданным критериям выполняется пользователем с ролью администратора тенанта.

Поиск писем всех пользователей в тенанте по заданным критериям выполняется с помощью команды **search_mails_by_tenant_id**.

Пример выполнения поиска письма по заданным критериям:

```

nct_ministerium search_mails_by_tenant_id \
--admin.login <...>

```

```

--admin.password <...>
--output_json /home/admin/certs/installation/output.json \
--query.text.operation>equals \
--query.text.value=семь \
--tenant_id 01068ade-1cce-4125-ab6b-91d977ecf85b \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=False \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=True \
--cox.use_tls_balancer=False \
--tls_settings.ca_file /home/user/ministerium_certs/installation/ca.pem \
--tls_settings.client_cert_file /home/user/ministerium_certs/installation/client.crt.pem \
--tls_settings.key_file /home/user/ministerium_certs/installation/client_key.pem \

```

Описание параметров поиска приведено в таблице 143.

Таблица 143 – Описание параметров поиска письма по заданным критериям

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
output_json	Str	+	Путь к файлу, в который будет записан результат поиска. Этот файл может быть использован в команде удаления (delete_mails) и указан в параметре --source
query.text.operation	Str	-	Поиск в тексте письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.text.value	Str	-	Значение поиска
tenant_id	Str	+	Идентификатор тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут запроса к сервису

Параметр	Тип	Обязательность	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

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 144.

Таблица 144 – Описание всех параметров поиска

Параметр	Тип	Обязательность	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	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут запроса к сервису

Параметр	Тип	Обязательность	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
help	Str	+	Помощь при выполнении команды search_mails_by_tenant_id
output_json	Str	+	Путь к файлу, в который будет записан результат поиска. Этот файл может быть использован в команде удаления (delete_mails) и указан в параметре --source
query.attachment_names.operation	Str	-	Поиск по названию вложений. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.attachment_names.values	Str	-	Поиск по названию вложений
query.bcc.operation	Str	-	Оператор для поиска значения в поле письма «Скрытая копия». Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.bcc.values	Str	-	Поиск указанного значения в поле письма «Скрытая копия»
query.cc.operation	Str	-	Оператор для поиска значения в поле письма «Копия». Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.cc.values	Str	-	Поиск указанного значения в поле письма «Копия»

Параметр	Тип	Обязательность	Описание
query.created_time.additional	Int	-	Время создания письма. Микросекунды UTC. Справа от диапазона, если операция равна «in_range», в противном случае игнорируется
query.created_time.operation	Str	-	Время создания письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.created_time.unixmicro	Int	-	Время создания письма. Микросекунды UTC. Операнд ИЛИ слева от диапазона
query.flag_draft	Str	-	Письмо помечено как «Черновик». Возможные значения: «true» или «false»
query.flag_flagged	Str	-	Письмо имеет метку-флаг. Возможные значения: «true» или «false»
query.flag_seen	Str	-	Письмо помечено как «Прочитано». Возможные значения: «true» или «false»
query.from.operation	Str	-	Оператор запроса для поиска значения в поле письма «От кого». Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.from.values strings	Str	-	Поиск указанного значения в поле письма «От кого»
query.from_to_cc_text_subject.operation	Str	-	Поиск указанного значения в заголовках «от кого», «кому», «копия», «тема» и в тексте письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.from_to_cc_text_subject.value	Str	-	Поиск указанного значения в заголовках «от кого», «кому», «копия»,

Параметр	Тип	Обязательность	Описание
			«тема» и в тексте письма
query.has_attachments	Str	-	Письмо имеет вложения. Возможные значения: «true» или «false»
query.importance.operation	Str	-	Фильтр по важности письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.importance.value	Str	-	Фильтр по важности письма. Возможные поисковые значения: – low (низкий); – normal (нормальный); – high (высокий);
query.mail_size.additional	Str	-	Размер письма. Справа от диапазона, если операция равна «in_range», в противном случае игнорируется
query.mail_size.operation	Str	-	Размер письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.mail_size.value	Int	-	Размер письма. Операнд ИЛИ слева от диапазона
query.modified_time.operation	Str	-	Время последнего редактирования письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.modified_time.additional	Int	-	Время последнего редактирования письма. Микросекунды UTC. Справа от диапазона, если операция равна «in_range», в противном случае игнорируется
query.modified_time.unixmicro	Int	-	Время последнего редактирования письма Микросекунды UTC. Операнд

Параметр	Тип	Обязательность	Описание
			ИЛИ слева от диапазона
query.subject.operation	Str	-	Поиск в теме письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.subject.value	Str	-	Поиск в теме письма
query.subject_and_text.operation	Str	-	Поиск в теме письма и в тексте. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.subject_and_text.value	Str	-	Поиск значений в теме письма и в тексте
query.text.operation	Str	-	Поиск в тексте письма. Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.text.value	Str	-	Поиск в тексте письма
query.to.operation	Str	-	Оператор для поиска значения в поле письма «Кому». Оператор запроса. Возможные значения: – less (меньше); – greater (больше); – in_range (в диапазоне); – equals (равно); – contains (содержит)
query.to.values	Str	-	Поиск указанного значения в поле письма «Кому»
tenant_id	Str	+	Идентификатор тенанта
tls_settings.ca_file	Str	+	Путь к СА файлу
tls_settings.client_cert_file	Str	+	Путь к файлу сертификата клиента

Параметр	Тип	Обязательность	Описание
tls_settings.key_file	Str	+	Путь к файлу с ключом клиента
token-name	Str	+	Имя токена для подключения
c	Str	+	Цветной вывод на консоль
check	Str	+	Выполнить проверку без выполнения команды
config	Str	+	По умолчанию используется nct_ministerium.yaml или nct_ministerium.json , расположенный в PWD
diff	Str	+	Показать изменения
v	Str	+	Подробное ведение журнала

7.19 Массовое удаление писем

Важно – Удаление писем по списку выполняется пользователем с ролью администратора тенанта.

Для удаления писем по списку необходимо выполнить команду **delete_mails**. Для выполнения данной команды потребуется JSON файл с идентификаторами письма. Подготовить файл можно двумя способами:

1. Самостоятельно подготовить входной JSON файл с данными письма:

```
[
  {
    "user_id": "c6ce44a7-7d81-4598-a727-02852bd149c4",
    "mails": [
      {
        "mail_id": "3bcf4651-c98d-4d65-b04d-17c0ca05ec14"
      }
    ]
  }
]
```

2. Получить информацию для JSON файла из ответа на команду **search_mails_by_tenant_id**. Для этого выполнить запрос на поиск письма по заданным критериям с помощью команды **search_mails_by_tenant_id** (пример команды и описание параметров запроса приведены в разделе 7.18).

3. После этого необходимо выполнить команду **delete_mails**:

```
nct_ministerium delete_mails \
--admin.login <...>
--admin.password <...>
--source /home/user/mail_list.json \
--reject /home/user/rejected.json \
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053 \
--cox.compression=none \
--cox.endpoint=grpc-installation.example.net:3142 \
--cox.load_balanced=False \
--cox.request_timeout=10s \
--cox.service_name=cox \
--cox.use_tls=True \
--cox.use_tls_balancer=False \
--tls_settings.ca_file /home/user/ca.pem \
--tls_settings.client_cert_file /home/user/client.crt.pem \
--tls_settings.key_file /home/user/client_key.pem \
```

Описание параметров запроса приведено в таблице 145.

Таблица 145 – Описание параметров запроса на удаление писем по заданным критериям

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
source	Str	+	Путь к json файлу со списком удаляемых писем
reject	Str	+	В этот файл сохраняются идентификаторы писем (mail_id) и причины (reason), по которым письмо не получилось удалить
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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

Параметр	Тип	Обязательность	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"
  },
  "deleted": 1,
  "failed": 0
}
```

7.20 Удаление пользователя, группы и ресурса

Для удаления пользователя, группы и ресурса выполнить запрос **change_status** на смену статуса объекта:

```
nct-ministerium change_status
--entity_id <entity_id>
--status <MARK_DELETED> ...
```

Описание параметров запроса приведено в таблице 146.

Таблица 146 – Описание параметров запроса на смену статуса объекта

Параметр	Тип	Обязательность	Описание
entity_id	Str	+	Идентификатор пользователя
statuses	Str	+	Статусы

Примечание – Сущность будет помечена на удаление и впоследствии будет удалена в соответствии с retention policy механизмом сборки мусора (garbage collector).

7.21 Восстановление удаленных писем в почтовом ящике пользователя

Для восстановления удаленных писем в почтовом ящике пользователя необходимо выполнить следующие действия:

1. Выполнить запрос на поиск удаленных писем. С помощью данной команды осуществляется поиск писем пользователей на основании следующих фильтров:
 - идентификатор пользователя;
 - лимит на количество писем, необходимых для восстановления;
 - временной диапазон «с» и «до».

Важно – Должен быть установлен минимум один фильтр.

Пример запроса на поиск удаленных писем:

```
./nct_ministerium get_deleted_mails
--config=config.json
--user_id 596c43b8-234d-4229-a138-b3f2e6555b0f
--limit 3
--timestamp_from 2012-11-01T22:08:41+00:00 --timestamp_to 2032-11-01T22:08:41+00:00
```

Описание параметров запроса приведено в таблице 147.

Таблица 147 – Описание параметров запроса на поиск удаленных писем

Параметр	Тип	Обязательность	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-b0ac-36ef8b52ae7e

```

Описание параметров запроса приведено в таблице 148.

Таблица 148 – Описание параметров запроса на восстановление письма по идентификатору

Параметр	Тип	Обязательность	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 149.

Таблица 149 – Описание параметров запроса на восстановление по лимиту на количество писем

Параметр	Тип	Обязательность	Описание
config	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>
limit	Str	-	Лимит на количество писем, необходимых для восстановления
user_id	Str	-	Идентификатор пользователя

Примечание – Если в этой команде указать параметры **limit** и **user_id**, то восстановится определенное количество последних удаленных писем конкретного пользователя. Если в этой команде указать только параметр **user_id**, то восстановятся все удаленные письма конкретного пользователя. Если в этой команде указать только параметр **limit**, то восстановится определенное количество последних удаленных писем всех пользователей.

Пример ответа:

```

{
"changed": true,
"failed": false,

```

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

- Восстановить письма, удаленные в определенный диапазон времени, указанный пользователем. С помощью данной команды можно восстановить последние удаленные письма пользователей в заданный диапазон времени. Пример запроса на восстановление писем, удаленных в заданный диапазон времени:

```
./nct_ministerium restore_mails_by_period
--config=config.json
--timestamp_from 2012-11-01T22:08:41+00:00 --timestamp_to 2032-11-
01T22:08:41+00:00
--user_id ddd4a809-ea14-407c-b4ea-60ac90214630
```

Описание параметров запроса приведено в таблице 150.

Таблица 150 – Описание параметров запроса на восстановление писем, удаленных в определенный диапазон времени, указанный пользователем

Параметр	Тип	Обязательность	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
timestamp_from timestamp_to	Str	-	Временной диапазон «с» и «до»
user_id	Str	-	Идентификатор пользователя

Примечание – Если в этой команде указать параметры **timestamp_from**, **timestamp_to** и **user_id**, то восстановятся письма конкретного пользователя за определенный временной диапазон. Если в этой команде указать только параметры **timestamp_from** и **timestamp_to**, то восстановятся последние удаленные письма всех пользователей за определенный временной диапазон. Если в этой команде указать только параметр **user_id**, то восстановятся все удаленные письма конкретного пользователя.

Пример ответа:

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

7.22 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 151.

Таблица 151 – Описание параметров запроса на просмотр истории комментариев

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
entity_id	Str	+	Идентификатор пользователя
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint сервиса
cox.load_balanced	Bool	+	Балансировщик нагрузки сервиса
cox.request_timeout	Str	+	Таймаут запроса к сервису

Параметр	Тип	Обязательность	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 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": {
    "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": "yamyamk"
},
{
  "id": "d8359c94-eeb3-40d7-8dbd-0a6ef669a074",
  "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
  "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
  "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
  "timestamp": "2023-01-11T16:21:58+03:00",
  "action": "USER_UNBLOCKED"
},
{
  "id": "f7ef3298-f455-4ddf-9359-d1e9a1485434",
  "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
  "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
  "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
  "timestamp": "2023-01-11T16:51:08+03:00",
  "action": "USER_BLOCKED"
},
{
  "id": "bd6d8af9-766d-4734-999f-b1238d84fc3e",
  "tenant_id": "01068ade-1cce-4125-ab6b-91d977ecf85b",
  "actor_id": "e0e788c4-2b10-4375-86f6-1726b0c274a1",
  "user_id": "041ab13d-f419-4412-9670-ed0339b919ed",
  "timestamp": "2023-01-11T16:51:10+03:00",
  "action": "ADDED_BLOCKING_REASON",
  "reason": "7890"
}
]
}
```

7.23 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.

Важно – 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.

Важно – 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 152.

Таблица 152 – Описание параметров запроса на создание подписи

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
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 создается 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. Примечание – Email-ы необходимо указывать через запятую, без пробела.
tenant_id	Str	+	Идентификатор тенанта
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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	Обязательность	Описание
<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

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

```

Описание параметров запроса приведено в таблице 153.

Таблица 153 – Описание параметров запроса на удаление подписи

Параметр	Тип	Обязательность	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

Параметр	Тип	Обязательность	Описание
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. Примечание – Email-ы необходимо указывать через запятую, без пробела.
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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
}
```

7.24 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**.

Важно – 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 154.

Таблица 154 – Описание параметров запроса на добавление отправителей в список

Параметр	Тип	Обязательность	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
}
...
]
```

7.24.1 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 155.

Таблица 155 – Описание параметров запроса на добавление отправителей в список

Параметр	Тип	Обязательность	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
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 156.

Таблица 156 – Описание параметров запроса на проверку отправителей

Параметр	Тип	Обязательность	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

Параметр	Тип	Обязательность	Описание
admin.password	Str	+	Пароль администратора тенанта
tenant_id	Str	+	Идентификатор тенанта
email	Str	+	Основной электронный адрес

Пример ответа:

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

7.24.2 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 157.

Таблица 157 – Описание параметров запроса на обновление списка пользователей

Параметр	Тип	Обязательность	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
address	Str	+	Email или домен отправителей, которых необходимо добавить в список

status	Str	+	Статус отправителя: WHITELIST (белый список) или BLACKLIST (черный список)
---------------	-----	---	--

Пример ответа:

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

Чтобы проверить наличие вновь добавленных отправителей в списке, необходимо выполнить проверку с помощью команды **check_email**, описанной в разделе 7.24.1.

7.24.3 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 158.

Таблица 159 – Описание параметров запроса на удаление отправителей в списках

Параметр	Тип	Обязательность	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
address	Str	+	Email или домен отправителей, которых необходимо добавить в список

Пример ответа:

```
{
  "Response": {
    "changed": true,
  }
}
```

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

Чтобы проверить наличие вновь добавленных отправителей в списке, необходимо выполнить проверку с помощью команды **check_email**, описанной в разделе 7.24.1.

8 СОПОСТАВЛЕНИЕ LDAP АТТРИБУТОВ КАТАЛОГА

Чтобы подключиться к внешним каталогам необходимо выполнить сопоставление данных или маппинг данных. Сопоставление (маппинг) данных — это выстраивание соотношений между моделями данных, которые находятся в разных источниках или системах. В записи данные содержатся в парах атрибут-значение. Каждый атрибут имеет имя (или короткую форму имени) и принадлежит одному или нескольким объектным классам, то есть входит в их состав.

Маппинг LDAP атрибутов внешнего каталога и каталога ПО «Mailion» настраивается для доменов, делегированных на внешний LDAP каталог. Для каждого делегированного домена может быть настроен свой маппинг.

Маппинг необходимо настроить самостоятельно через файл (см. раздел 8.1) и передать с помощью команд (см. раздел 8.2).

8.1 Настройка маппинга через файл

Для упрощения работы и быстрого выполнения маппинга можно выполнить его настройку через файл-шаблон, доступный для любого внешнего каталога. Путь до этого файла передается в любую из описанных в разделе 5.2 команд, которая поддерживает добавление маппинга, и маппинг подтянется из этого файла.

Чтобы получить шаблон файла необходимо выполнить запрос:

```
nct_ministerium get_default_ldap_attribute_mappings
--output_filepath AD.json
--preset_name AD
--admin.login <...>
--admin.password <...>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142
--cox.load_balanced=False
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=True
--cox.use_tls_balancer=False
--tls_settings.ca_file ...
--tls_settings.client_cert_file ...
```

```
--tls_settings.key_file ...
```

Описание параметров запроса приведено в таблице 160.

Таблица 160 – Описание параметров запроса на получение файла-шаблона для маппинга

Параметр	Тип	Обязательность	Описание
output_filepath	Str	+	Путь до файла-шаблона для маппинга
preset_name	Str	+	Имя шаблона маппинга для необходимого каталога. Например, AD
admin.login	Str	+	Логин администратора
admin.password	Str	+	Пароль администратора
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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 необходимо открыть файл AD.json, в котором выполнить настройку полей. Пример данного файла:

```
{
  "attributes_mapping": {
    "avatar": "thumbnailPhoto",
    "department": "department",
    "first_name": "givenName",
    "first_name_alt": "givenName",
    "group_description": "description",
    "group_name": "displayName",
    "last_changed": "whenChanged",
    "last_name": "sn",
    "last_name_alt": "sn",
    "locale": "localeID",
```

```

"login": "sAMAccountName",
"mail": "mail",
"middle_name": "middleName",
"middle_name_alt": "middleName",
"phone_number_work": "telephoneNumber",
"principal_name": "userPrincipalName",
"status": "userAccountControl",
"title": "title"
},
  "search_filter_user": "(&(&(objectCategory=person)(objectClass=user))((
(givenName={{.Name}}*)(sn={{.Name}}*)(middleName={{.Name}}*)
(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))",
  "search_filter_group": "(&(&(objectCategory=group)((groupType=8)(groupType=-
2147483646)(groupType=-2147483640))(mail=*)(!(msExchHideFromAddressLists=TRUE)))
((displayName={{.Name}}*)(description={{.Name}}*)(mail={{.Name}}*)))",
  "search_filter_resource": "(&((msExchResourceMetaData=ResourceType:Room))((
(givenName={{.Name}}*)(sn={{.Name}}*)(middleName={{.Name}}*)
(sAMAccountName={{.Name}}*)(mail={{.Name}}*)))",
  "search_filter_exact_user_by_name": "(&(&(objectCategory=person)(objectClass=user))
(sAMAccountName={{.Name}}*))",
  "search_filter_exact_user_by_email": "(&(&(objectCategory=person)(objectClass=user))
(mail={{.Email}}*))"
}

```

Описание параметров поля **attributes_mapping** приведено в таблице 161.

Таблица 161 – Описание параметров запроса на получение файла-шаблона для маппинга

Значение для ПО «Mailion»	Значение для AD	Описание атрибута
avatar	thumbnailPhoto	Фотография пользователя
department	department	Отдел пользователя
first_name	givenName	Имя пользователя
first_name_alt	givenName	Имя пользователя, если задано, имеет приоритет над first_name
group_description	description	Описание группы
group_name	displayName	Имя группы
last_changed	whenChanged	Время последнего изменения
last_name	sn	Фамилия пользователя
last_name_alt	sn	Фамилия пользователя, если задано, имеет приоритет над last_name
locale	localeID	Язык
login	sAMAccountName	Логин пользователя

Значение для ПО «Mailion»	Значение для AD	Описание атрибута
mail	mail	Email пользователя
middle_name	middleName	Отчество пользователя
middle_name_alt	middleName	Отчество пользователя, если задано, имеет приоритет над middle_name
phone_number_work	telephoneNumber	Рабочий телефон пользователя
principal_name	userPrincipalName	Имя принципала. Принципал – сущность, заведенная в каталоге. Имя используется как логин, который нельзя изменять. Этот атрибут – особенность AD, но также присутствует во FreeIPA
status	userAccountControl	Статус пользователя
title	title	Должность пользователя

Описание полей фильтров:

1. **SearchFilterUser** – шаблон для LDAP-фильтра, с помощью которого будет производиться поиск пользователя во внешнем каталоге. С его помощью можно понять, как искать того или иного пользователя. Доступные переменные шаблона:
 - {{.Name}} – имя пользователя;
 - {{.Email}} – Email пользователя.
2. **SearchFilterGroup** – шаблон для LDAP-фильтра, с помощью которого будет производиться поиск группы во внешнем каталоге. Доступные переменные шаблона:
 - {{.Name}} – имя группы;
 - {{.Email}} – Email группы.
3. **SearchFilterResource** – шаблон для LDAP-фильтра, с помощью которого будет производиться поиск ресурса во внешнем каталоге. Доступные переменные шаблона:
 - {{.Name}} – имя ресурса;
 - {{.Email}} – Email ресурса.
4. **SearchFilterExactUserByName** – шаблон для LDAP-фильтра, с помощью которого будет производиться точный поиск пользователя по имени во внешнем каталоге. Доступные переменные шаблона:
 - {{.Name}} – имя пользователя.

5. **SearchFilterExactUserByEmail** – шаблон для LDAP-фильтра, с помощью которого будет производиться точный поиск пользователя по имени во внешнем каталоге.
- Доступные переменные шаблона:
- `{{.Name}}` – Email пользователя.

8.2 Добавление маппинга через команды

Управление маппингом LDAP атрибутов осуществляется с помощью команд расширенного администрирования:

- **create_domain** – создание домена. Если в этом запросе добавляется делегирование домена, то можно сразу же задать маппинг.
- **add_domain_delegation** – добавление делегированного на внешний LDAP каталог домена.
- **update_domain_delegation** – обновление делегации домена.

Команды имеют общий список аргументов для маппинга. Пример таких аргументов приведен в таблице 162.

Таблица 162 – Общий список аргументов маппинга

Аргумент	Тип	Описание
<code>--external.ldap_attributes_mapping.custom_from_file</code>	Str	Заполнить маппинг из файла. Если указан путь к файлу с маппингом, параметры ниже не нужно заполнять, они в любом случае будут проигнорированы
<code>--external.ldap_attributes_mapping.mapping_preset_name</code>	Str	Доступные значения: AD, FreeIPA, SambaDC
<code>--external.ldap_attributes_mapping.mapping_type</code>	Str	Доступные значения: MAPPING_TYPE_PRESET (маппинг с помощью шаблона), MAPPING_TYPE_CUSTOM (маппинг, который необходимо заполнить самостоятельно)

Важно – Для команд `add_domain_delegation` и `update_domain_delegation` опция для задания файла будет `--delegation.ldap_attributes_mapping.custom_from_file`.

8.2.1 Добавление маппинга при создании домена

Для добавления маппинга через команду создания домена необходимо выполнить запрос:

```
nct_ministerium create_domain
--tenant_id <...>
--hostname <...>
--external.default_region_id <...>
--external.delegate_id <...>
--external.domain_alias <...>
--external.domain_auth_name <...>
--external.domain_short_name <...>
--external.is_sync_enabled=true \
--external.ldap_attributes_mapping.custom_from_file "AD.json"
--features.is_authorization=true
--features.is_mail=true
--features.is_service=true
--is_prioritized=false
--admin.login <...>
--admin.password <...>
--cox.balancer_endpoint=hydra.ucs-apps-1.installation.example.net:50053
--cox.compression=none
--cox.endpoint=grpc-installation.example.net:3142
--cox.load_balanced=False
--cox.request_timeout=10s
--cox.service_name=cox
--cox.use_tls=True
--cox.use_tls_balancer=False
--tls_settings.ca_file ...
--tls_settings.client_cert_file ...
--tls_settings.key_file ...
```

Описание параметров запроса приведено в таблице 163.

Таблица 163 – Описание параметров запроса на создание домена

Параметр	Тип	Обязательность	Описание
<code>tenant_id</code>	Str	+	Идентификатор тенанта
<code>hostname</code>	Str	+	Имя домена

Параметр	Тип	Обязательность	Описание
external.default_region_id	Str	-	Идентификатор региона по умолчанию для автоматического создания пользователей
external.delegate_id	Str	+	Идентификатор делегата, используемый для внешней авторизации
external.domain_alias	Str	-	Имя контроллера внешнего домена
external.domain_auth_name	Str	+	Длинная запись домена аутентификации
external.domain_short_name	Str	+	Краткая запись домена аутентификации
external.ldap_attributes_mapping.custom_from_file	Str	+	Имя файла для загрузки маппинга атрибутов
features.is_mail	Bool	+	Если значение true , домен может принимать почтовые сообщения
features.is_authorization	Bool	+	Если значение true , домен можно использовать для авторизации
features.is_service	Bool	+	Если значение true , домен можно использовать для авторизации по умолчанию
external.is_sync_enabled	Bool	+	Включение/отключение синхронизации с внешним доменом. Если значение false , то выключена. Если значение true , то включена
is_prioritized	Bool	+	Приоритетность

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора
admin.password	Str	+	Пароль администратора
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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 маппинг добавится из файла AD.json и сохранится в домене.

8.2.2 Добавление маппинга при настройке делегации домена

Для добавления маппинга при настройке делегированного на внешний LDAP каталог домена необходимо выполнить запрос:

```
nct_ministerium add_domain_delegation
--admin.login <...>
--admin.password <...>
--domain_id <...>
--delegation.default_region_id <...>
--delegation.delegate_id <...>
--delegation.domain_alias <...>
```

```

--delegation.is_sync_enabled=TRUE
--delegation.ldap_attributes_mapping.mapping_type=MAPPING_TYPE_PRESET
--delegation.ldap_attributes_mapping.mapping_preset_name=AD
--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 164.

Таблица 164 – Описание параметров запроса на создание домена

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора
admin.password	Str	+	Пароль администратора
domain_id	Str	+	Идентификатор домена
delegation.default_region_id	Str	+	Идентификатор региона оп умолчанию
delegation.delegate_id	Str	+	Идентификатор делегации (подключения внешнего каталога), берется из секции <code>backends.ldap</code> конфигурации <code>orpheus</code>
delegation.domain_alias	Str	+	Внешний домен для делегации
delegation.is_sync_enabled	Bool	+	Значение true , если внешний домен – AD, в остальных случаях false
delegation.ldap_attributes_mapping.mapping_type	Str	+	Доступные значения: <code>MAPPING_TYPE_PRESET</code> (маппинг с помощью шаблона), <code>MAPPING_TYPE_CUSTOM</code> (маппинг, который необходимо заполнить самостоятельно)
delegation.ldap_attributes_mapping.mapping_preset_name	Str	+	Имя шаблона для маппинга. Доступные значения: AD, FreeIPA, SambaDC

Параметр	Тип	Обязательность	Описание
cox.balancer_endpoint	Str	+	Endpoint балансировщика нагрузки сервиса
cox.compression	Str	+	Метод сжатия данных – без сжатия
cox.endpoint	Str	+	Endpoint 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

8.2.3 Добавление маппинга при обновлении делегации в домене

Для добавления маппинга через обновление делегации в домене, выполните запрос:

```
nct_ministerium update_domain_delegation
--admin.login <...>
--admin.password <...>
--domain_id <...>
--delegation.default_region_id <...>
--delegation.delegate_id <...>
--delegation.domain_alias <...>
--delegation.is_sync_enabled=TRUE <...>
--delegation.ldap_attributes_mapping.mapping_type MAPPING_TYPE_CUSTOM
--delegation.ldap_attributes_mapping.mapping
'avatar=thumbnailPhoto,department=department,first_name=givenName,first_name_alt=extensionAttribute2,group_description=description,group_name=displayName,last_changed=whenChanged,last_name=sn,last_name_alt=extensionAttribute1,locale=localeID,login=sAMAccountName,mail=mail,middle_name=extensionAttribute3,middle_name_alt=extensionAttribute3,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 165.

Таблица 165 – Описание параметров запроса на создание домена

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора
admin.password	Str	+	Пароль администратора
domain_id	Str	+	Идентификатор домена
delegation.default_region_id	Str	+	Идентификатор региона по умолчанию
delegation.delegate_id	Str	+	Идентификатор делегации (подключения внешнего каталога), берется из секции backends.ldap конфигурации orpheus
delegation.domain_alias	Str	+	Внешний домен для делегации

Параметр	Тип	Обязательность	Описание
delegation.is_sync_enabled	Bool	+	Значение true , если внешний домен – AD, в остальных случаях false
delegation.ldap_attributes_mapping.mapping_type	Str	+	Доступные значения: MAPPING_TYPE_PRESET (маппинг с помощью шаблона), MAPPING_TYPE_CUSTOM (маппинг, который необходимо заполнить самостоятельно)

Пример настройки полей приведен в разделе 8.1.

9 НАСТРОЙКА KERBEROS

Сетевой протокол Kerberos предназначен для обеспечения безопасной аутентификации.

9.1 Поддержка kerberos для домена

Чтобы включить поддержку Kerberos для домена необходимо выполнить следующие действия:

1. На контроллере домена через оснастку AD рабочей станции администратора ОС Windows создать служебных пользователей stagehttp (stageimap/stagesmtp/stageldap/stagegrpc) (см. Рисунок 53).

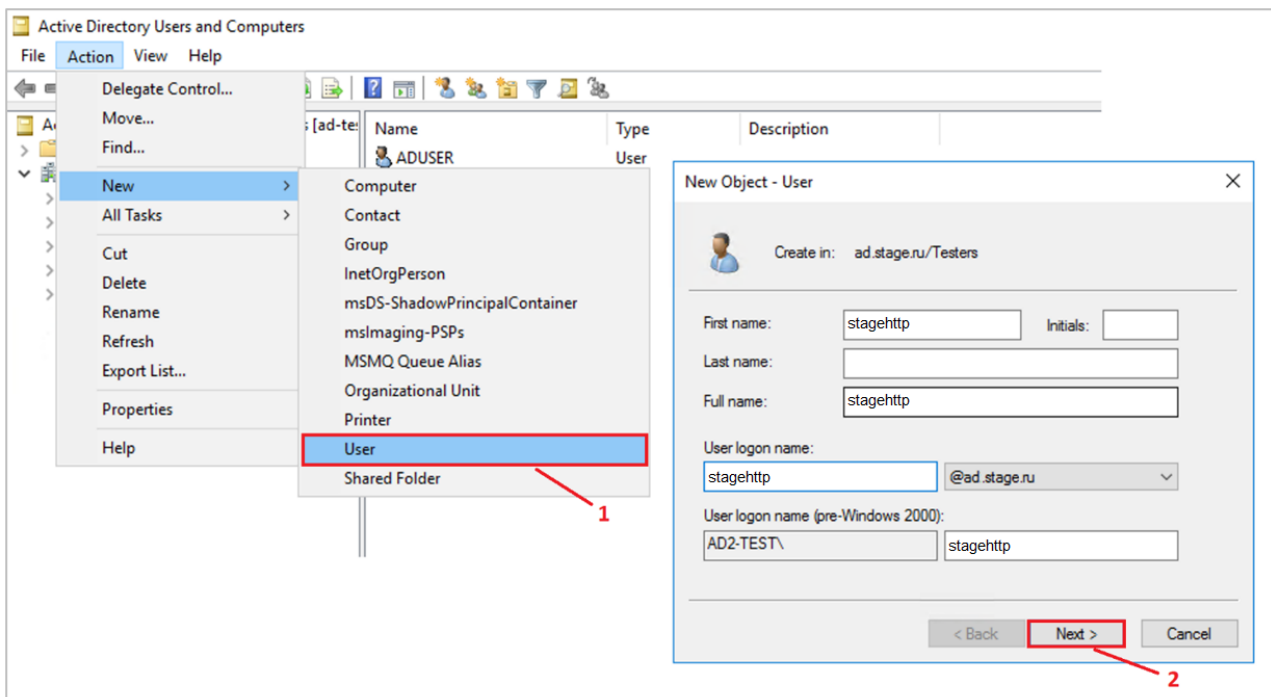


Рисунок 53 – Создание служебных пользователей

2. Запретить изменять пароль и установить пароль бессрочным (см. Рисунок 54).

The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: ad.stage.ru/Testers'. Below that are two password input fields, both filled with dots. Underneath are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (checked), 'Password never expires' (checked), and 'Account is disabled' (unchecked). At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

Рисунок 54 – 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 166 перечислено соответствие системного пользователя и его SPN.

Таблица 166 – Соответствие системного пользователя и его SPN

Системный пользователь	SPN
stagehttp	HTTP/api-testmail.domain.ru
stageimap	imap/imap-testmail.domain.ru
stagesmtp	smtp/smtp-testmail.domain.ru
stageldap	ldap/ldap-testmail.domain.ru
stagegrpc	grpc/grpc-testmail.domain.ru

Затем необходимо выполнить следующие действия (процесс рассмотрен на основе пользователя stagehttp):

1. Открыть командную строку или PowerShell (<https://learn.microsoft.com/ru-ru/powershell/>) от имени администратора ОС. Выполнить команду для регистрации SPN:

```
C:\Temp>setspn -A HTTP/api-testmail.domain.ru stagehttp
Регистрация ServicePrincipalNames для CN=stagehttp,CN=Users,DC=domain,DC=ru
HTTP/api-testmail.domain.ru
Обновленный объект
```

2. Выполнить проверку и убедиться, что SPN создан и принадлежит пользователю stagehttp:

```
C:\Temp>setspn -L stagehttp
Зарегистрирован ServicePrincipalNames для
CN=stagehttp,CN=Users,DC=domain,DC=ru
HTTP/api-testmail.domain.ru
```

3. Выполнить команду, чтобы сгенерировать keytab-файл. Данный файл будет содержать пары Kerberos принципалов и их ключей для зарегистрированного SPN. Необходимо выполнить для каждого системного пользователя:

Важно – 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 ниже:

```
nct-ministerium save_keytab --config config.local.json --domain_id 'fae98b71-29e5-52ba-
ab28-3b4a66643ef1' --principal 'HTTP/api-testmail.domain.ru' --keytab_path
'/tmp/stagehttp.keytab'
```

5. Настроить клиент на авторизацию методом Kerberos/GSSAPI.
6. Для http разрешить Kerberos в конфигурационном файле сервиса **house**. Пример секции в файле:

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

9.2 Настройка для веб-клиента

9.2.1 Настройка браузера для авторизации через Kerberos

Настройка браузера может быть произведена пользователем с ролью:

- локальный пользователь ОС Windows – пользователь с правами администратора;
- доменный пользователь ОС Windows – Пользователь AD, с ролью которого нужно будет авторизовываться в ОС Windows. Для доменных пользователей, авторизованных в ОС Windows, авторизация в ПО «Mailion» будет происходить автоматически. Для переключения в другой аккаунт пользователю необходимо перейти в другую доменную или локальную учетную запись в ОС Windows.

Авторизация доменных пользователей ОС Windows происходит как в Microsoft Outlook Web: потребуется домен, логин и пароль пользователя. Домен и логин пользователя указываются через слеш: AD\ADUSR25.

9.2.2 Проверка конфигурации Kerberos

Перед тем как осуществить настройку необходимо выполнить проверку:

1. Посмотреть в конфигурационном файле наличие Kerberos:

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

2. Посмотреть в консоль браузера, запрос session/check. Вместе со статусом 401 должен отдавать header WWW-Authenticate: Negotiate.

9.2.3 Настройка ОС Windows

Важно – 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 55):

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**.

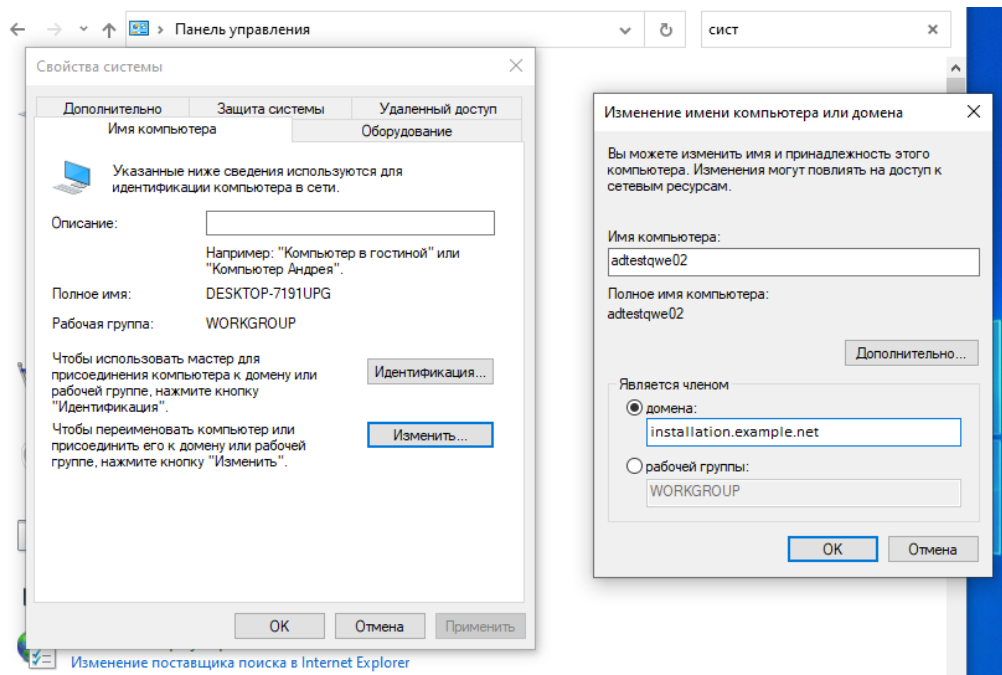


Рисунок 55 – Присоединение ПК к домену

9.2.4 Настройка браузеров в ОС Windows

9.2.4.1 Настройка в Internet Explorer

Важно – 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 56).

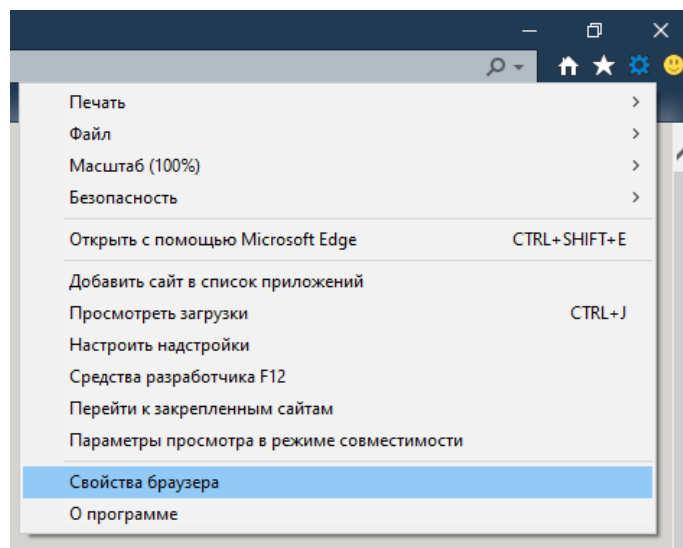


Рисунок 56 – Свойства браузера

2. На вкладке **Безопасность** необходимо выбрать зону **Местная интрасеть** и нажать кнопку **Сайты** (см. Рисунок 57).

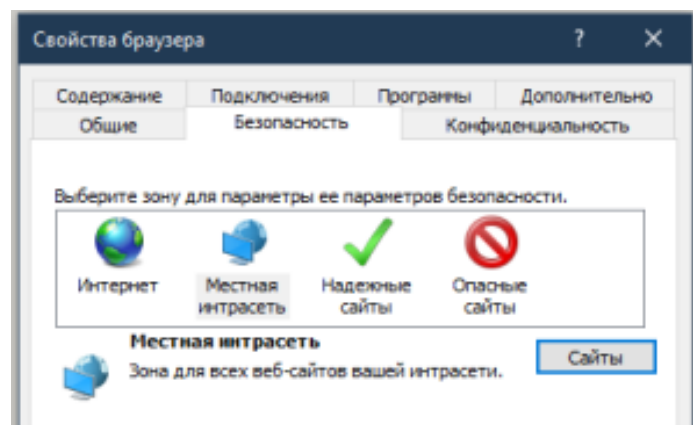


Рисунок 57 – Кнопка Сайты

3. Нажать кнопку **Дополнительно** (см. Рисунок 58).

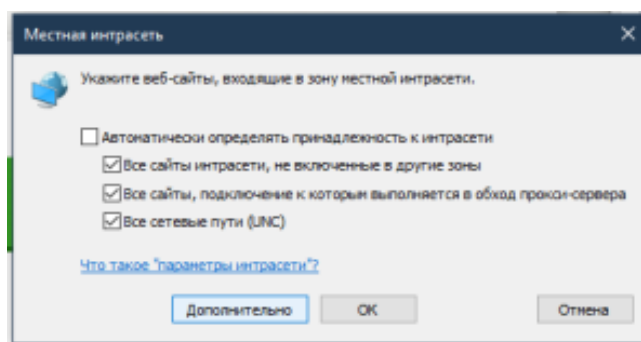


Рисунок 58 – Кнопка **Дополнительно**

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 59).

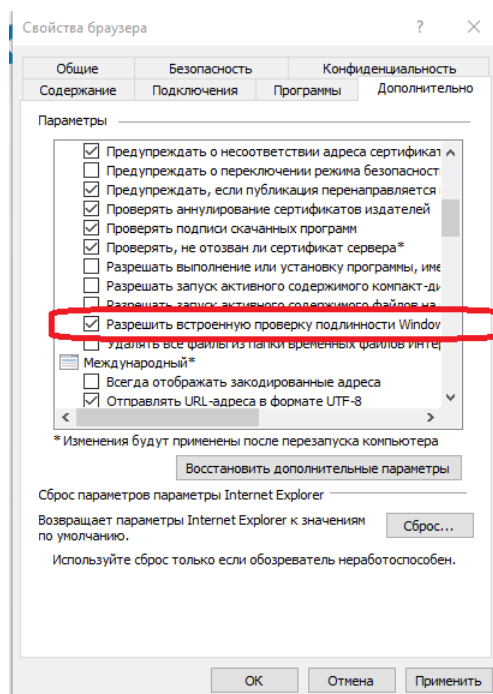


Рисунок 59 – Опция **Разрешить встроенную проверку подлинности Windows**

9.2.4.2 Настройка Google Chrome

В новых версиях Chrome автоматически определяется наличие поддержки Kerberos. Если используется устаревшая версия браузера, то его нужно запустить с дополнительным параметром. Для этого необходимо выполнить следующие действия:

1. Открыть командную строку и указать путь до файла запуска браузера:

```
"C:\Program Files\Google\Chrome\Application\chrome.exe"
```

2. Добавить параметр:

```
--auth-server-whitelist =«*. домен стенда»
```

3. Нажать **Enter**.

После этого откроется браузер Chrome.

9.2.4.3 Настройка Mozilla Firefox

Важно – По умолчанию поддержка Kerberos в Firefox отключена.

Для настройки необходимо выполнить следующие действия:

1. В адресной строке браузера перейти на страницу `about:config`. Нажать кнопку **Принять риск и продолжить**.
2. Найти параметры:
 - `network.negotiate-auth.trusted-uris`;
 - `network.automatic-ntlm-auth.trusted-uris`;
 - `network.negotiate-auth.delegation-uris`.
3. Указать в этих параметрах домен стенда, на котором проходит тестирование.

9.2.4.4 Настройка приложений в ОС Windows

9.2.4.4.1 Thunderbird

Чтобы настроить Kerberos в приложении Thunderbird необходимо выполнить следующие действия:

1. В Thunderbird из меню открыть **Параметры учетной записи** (см. Рисунок 60).

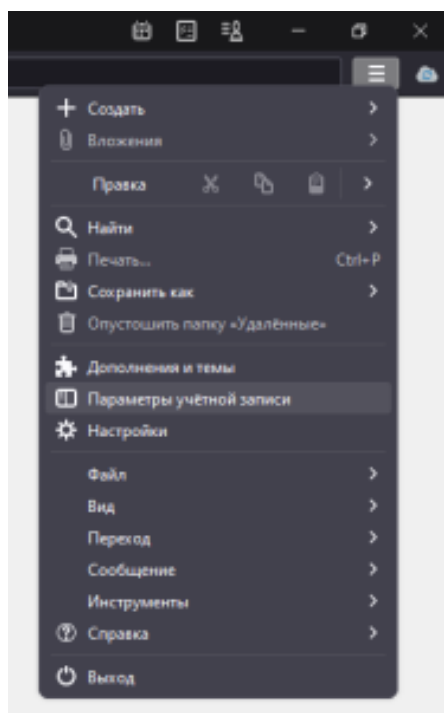


Рисунок 60 – Параметры учетной записи

2. На вкладке **Сервер исходящей почты (SMTP)** нажать кнопку **Добавить/Изменить** (см. Рисунок 61).

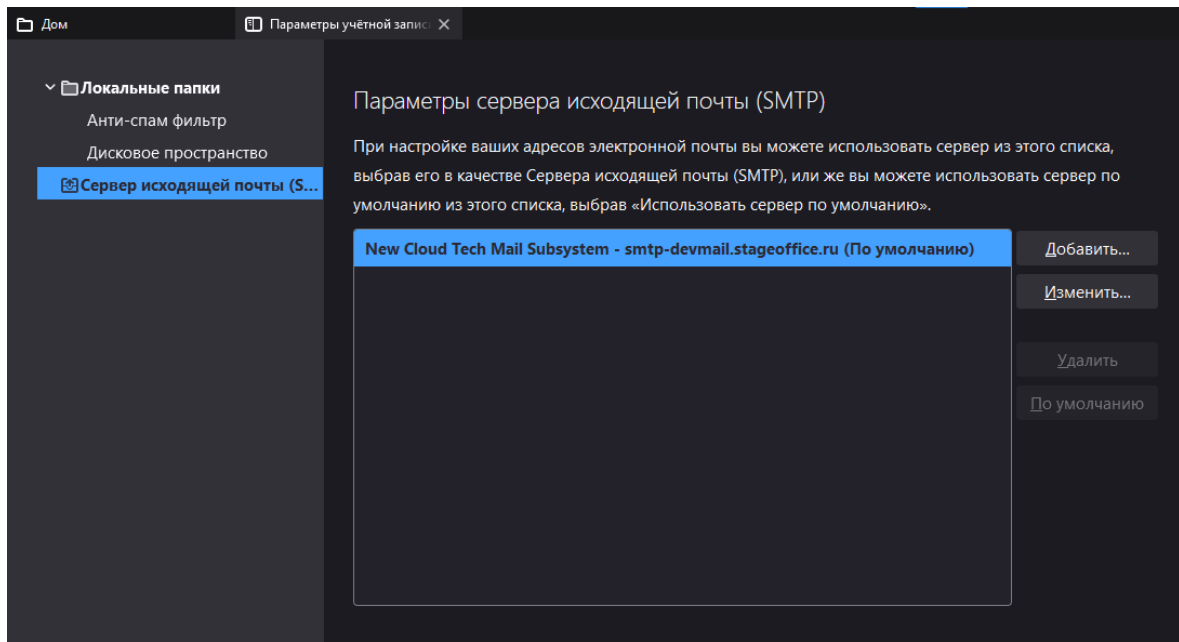


Рисунок 61 – Добавление сервера исходящей почты

3. В **Метод аутентификации** выбрать **Kerberos / GSSAPI**, заполнить оставшиеся необходимые поля и нажать кнопку **ОК** (см. Рисунок 62).

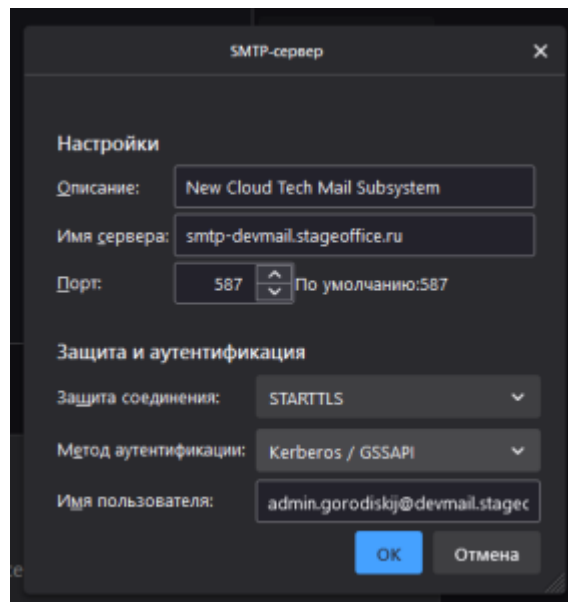


Рисунок 62 – Выбор метода **Kerberos / GSSAPI**

9.2.4.4.2 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 63).

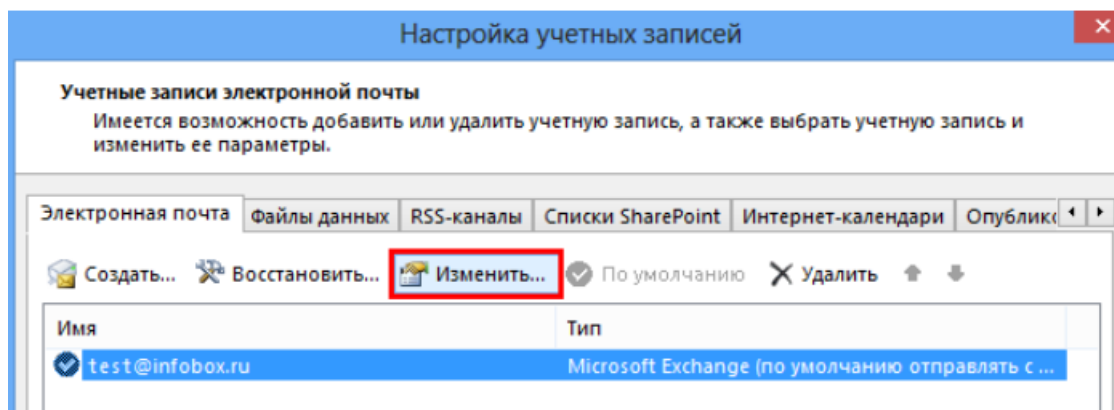


Рисунок 63 – Изменить учетную запись

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

10 УРОВЕНЬ ДОСТУПНОСТИ ПО «MAILION»

ПО «Mailion» имеет уровень доступности 99.9% или “три девятки” при условии обновления системы четыре раза в год.

11 НАСТРОЙКА ОГРАНИЧЕНИЙ ДЛЯ ПОИСКА ПО ВЛОЖЕНИЯМ

Работа в ПО «Mailion» с большим объемом информации, с файлами, нагруженными текстом и вложениями, может привести к высокому потреблению ресурсов оперативной памяти и замедлению выполнения процессов сервисом **viper**.

Для избежания потенциальных проблем с перерасходом памяти и для ускорения процессов (например, миграции пользователей) были введены следующие ограничения:

- ограничение размера вложений для поиска;
- возможность отключения поиска по вложениям;
- ограничение скорости парсинга или ограничение числа потоков одновременного парсинга.

Примечание – Парсинг – автоматизированный сбор и структурирование текстовой информации из документа для поискового индекса.

11.1 Ограничение размера вложений для поиска

Ограничение гарантирует, что сервис **viper** не будет не будет расходовать ресурсы памяти в большом объеме и оставит функцию поиска по вложениям для большинства пользователей. Таким образом, поиск будет осуществляться только по вложениям, размер которых не превышает 1 МБ.

Примечание – Настройка лимита сохраняется только в конфигурационных файлах внутри сервиса.

11.2 Отключение поиска по вложениям

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

При значении **true** сервис **viper** не будет индексировать вложения при сохранении писем, что приведет к снижению затрат на память и CPU.

Пример секции в конфигурационном файле:

```
viper_disable_attachment_indexing: true
```

11.3 Ограничение скорости парсинга

Для ограничения числа потоков, которые одновременно выполняют индексацию вложений, в конфигурационный файл сервиса **viper** ПО «Mailion» добавлен параметр **viper_client.tripoli.attach_parsing_thread_limit**.

Настройка данного параметра влияет на следующие показатели:

- на пик потребляемой памяти (чем меньше потоков, тем меньше одновременных вложений будет в памяти сервиса);
- на процессорное время, потребляемое сервисом **viper** (чем меньше ядер занято парсингом, тем больше времени остается для других сервисов или задач).

Если нагрузка от сервиса **viper** или нагрузка в виде большого количества писем с вложениями в секунду замедляет процессы, то для ограничения потребления ресурсов можно уменьшить этот параметр. При этом общая скорость индексации вложений соответственно уменьшится.

По умолчанию значение равно количеству доступных виртуальных ядер с той виртуальной машины на которой запущен сервис **viper**.

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

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

12 ИНСТРУКЦИЯ ПО ОБНОВЛЕНИЮ СЕРТИФИКАТОВ НА ФРОНТЕНД-СЕРВЕРАХ

Сертификаты для домена установки находятся в папке, где расположен установщик:

- certificates/server.crt – сертификат сервера;
- certificates/server.nopass.key – ключ сертификата сервера;
- certificates/ca.pem – сертификат или цепочка сертификатов УЦ.

Если имена сертификатов изменились, то необходимо изменить значения **group_vars** в файле `group_vars/<installation_name>/main.yml`:

```
setup:
  tls:
    cert_filename: <имя файла с сертификатом>
    key_filename: <имя файла с ключом>
    ca_filename: <файл с сертификатом или цепочкой сертификатов УЦ>
```

После чего запустить переустановку сервисов фронтенд-сервера следующей командой (независимо от изменения имен сертификатов):

```
ansible-playbook playbooks/main.yml [-i hosts_cluster.yml]
--diff
--limit ucs_frontend,ucs_mail,ucs_infrastructure
--tags cox,house,leda,ararat,imap,postfix
--extra-vars '{"reissue_certificates": true}'
--extra-vars '{"postfix_recreate": true}'
```


13 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ

В ПО «Mailion» предусмотрено резервное копирование и восстановление данных.

13.1 Dispersed object store

В конфигурационном файле Dispersed object store (DOS) каждой ноды (нода – виртуальная или физическая машина, на которой разворачиваются и запускаются контейнеры; совокупность нод образует кластер) должны быть заданы параметры резервного копирования (бэкапа):

```
"backup_engine": {  
  "store_count": 1, // не используется для  
  бэкапов с лидером  
  "path": "/srv/docker/dispersed_object_store/backup" // путь для  
  хранения бэкапов  
}
```

В DOS существует два вида резервного копирования:

1. Локальное – бэкап RocksDB на одной ноде, не зависит от типа установки.
2. Кластерное – набор локальных бэкапов всех нод, которые снимаются со всего кластера в одно время. Кластерный бэкап можно снять только с кластерной установки.

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

- Для локальной (Standalone) и кластерной (отказоустойчивой) установки используется одно API (Application Programming Interface – программный интерфейс приложения). При снятии и восстановлении бэкапа необходимо работать с тем идентификатором, который вернул DOS.
- Идентификаторы локальных и кластерных бэкапов имеют один тип и не зависят от типа инсталляции.

Для проведения восстановления необходимо перезапустить ноду в режиме восстановления. Для этого необходимо выполнить следующие действия:

1. Остановить ноду.

2. Поменять поле в файле конфигурации `server.recovery_mode = true`.
3. Запустить ноду.

После этого нода готова для восстановления. После проведения восстановления необходимо вернуть значения поля обратно на **false**.

Важно – Нода в режиме восстановления подключается к кластеру так же, как и в нормальном режиме. Нода в режиме восстановления не обрабатывает клиентские запросы.

13.1.1 Снятие бэкапа

Команды для управления бэкапами необходимо выполнить в любом из Docker-контейнеров DOS.

Примечание – Docker-контейнер (Docker-container) – это автономный исполняемый пакет программного обеспечения, который включает в себя все необходимое для запуска приложения: код, среду выполнения, системные инструменты, системные библиотеки и настройки.

Для этого необходимо перейти в любой из контейнеров с помощью команды:

```
docker exec -it dispersed_object_store bash
```

Следующая команда запустит создание кластерного бэкапа для кластерной инсталляции или локального бэкапа для Standalone инсталляции соответственно.

В кластерной конфигурации команда на создание кластерного бэкапа вызывается только через «лидера» (в терминологии DOS – нода, через которую осуществляется управление кластером) кластера. Необходимо, чтобы все ноды кластера успешно выполнили бэкап. Если хотя бы одна из нод не смогла сделать бэкап, то весь кластерный бэкап не считается выполненным.

Запуск бэкапа метаданных выполняется с помощью команды:

```
ucs_dispersed_object_store leader backup run -H dos.ucs-dos-shard-2.ucs-developers.example.com -p 7400 --token=***** --tls_settings.key_file=/srv/tls/keys/dos.ucs-dos-shard-1.ucs-developers.example.com-main-key.pem --tls_settings.client_cert_file=/srv/tls/certs/dos.ucs-dos-shard-1.ucs-developers.example.com-main-client.pem --tls_settings.ca_file=/srv/tls/certs/ucs-infra-1.ucs-developers.example.com-main-ca.pem
```

Точное расположение SSL сертификатов и ключей можно посмотреть в конфигурационном файле `/etc/ucs/dispersed-object-store/config.json` в секции `tls_settings`.

При этом следует соблюдать следующие правила:

- не останавливать ноды для снятия бэкапа;
- поле **blocking** делает снятие бэкапа блокирующим или асинхронным. Для проверки статуса асинхронного бэкапа необходимо использовать команду проверки статуса бэкапа (см. раздел 13.1.2);
- одновременно может сниматься только один бэкап;
- для кластера снятие бэкапа необходимо выполнять через «лидера»;
- для кластера можно сделать только кластерный бэкап;
- в качестве ответа на операцию снятия бэкапа вернется сообщение, содержащее в себе идентификатор бэкапа (JSON, значение поля «`backup_time`»);
- если операция снятия бэкапа прошла с ошибками, то идентификатор бэкапа в ответном сообщении (JSON, значение поля «`backup_time`») будет «0».

В ответе на успешный запрос снятия бэкапа, поле **backup_time** содержит идентификатор бэкапа. Ответ на выполнение **dos leader backup run**:

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

13.1.2 Проверка статуса бэкапа

Проверка статуса резервного копирования выполняется с помощью команды:

```
ucs-dispersed-object-store-client leader backup status -H dos.ucs-dos-shard-2.ucs-
developers.example.com -p 7400 --token=***** --tls_settings.key_file=/srv/tls/keys/dos.ucs-
dos-shard-1.ucs-developers.example.com-main-key.pem --
tls_settings.client_cert_file=/srv/tls/certs/dos.ucs-dos-shard-1.ucs-developers.example.com-
main-client.pem --tls_settings.ca_file=/srv/tls/certs/ucs-infra-1.ucs-developers.example.com-
main-ca.pem \
```

```
--backup_time 1693763682 \ // идентификатор бэкапа  
--verify=true // флаг верификации бэкапа
```

В случае кластерной инсталляции, команду необходимо запускать через «лидер» кластера.

Данная команда осуществляет проверку:

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

Пример ответа на выполнение команды **dos leader backup status** в кластерной инсталляции:

```
{  
  "error": {  
    "module": 24,  
    "code": 200,  
    "msg": "succeeded",  
    "details": []  
  },  
  "info": {  
    "backup_time": "1693763682",  
    "status": 1,  
    "node_backups": { // для кластерного бэкапа указывает локальные  
                      бэкапы на всех нодах кластера. Для SA инсталляции будет пусто  
      "1": {  
        "status": 1,  
        "rocksdb_info": {  
          "backup_id": 5, // внутренний идентификатор бэкапа RocksDB
```

```
"timestamp": "1693763686", // идентификатор локального бэкапа на
данной ноде
```

```
"size": "223327490",
```

```
"num_files": 15
```

```
},
```

```
"backends": {
```

```
"1627464062": {
```

```
"blob": {
```

```
"blob_path": "/srv/docker/dispersed_object_store/data/disk1/blob",
```

```
"rocksdb_info": {
```

```
"backup_id": 5,
```

```
"timestamp": "1693763689",
```

```
"size": "9459078",
```

```
"num_files": 13
```

```
},
```

```
"blob_backup_id": "5"
```

```
}
```

```
},
```

```
"4180084543": {
```

```
"blob": {
```

```
"blob_path": "/srv/docker/dispersed_object_store/data/disk2/blob",
```

```
"rocksdb_info": {
```

```
"backup_id": 5,
```

```
"timestamp": "1693763690",
```

```
        "size": "5857733",
        "num_files": 14
    },
    "blob_backup_id": "5"
}
}
},
"2": {
    "status": 1,
    "rocksdb_info": {
        "backup_id": 5,
        "timestamp": "1693763690",
        "size": "156609579",
        "num_files": 21
    },
    "backends": {
        "2563458084": {
            "blob": {
                "blob_path": "/srv/docker/dispersed_object_store/data/disk1/blob",
                "rocksdb_info": {
                    "backup_id": 5,
                    "timestamp": "1693763700",
                    "size": "10226794",
```

```
        "num_files": 14
      },
      "blob_backup_id": "5"
    }
  },
  "3800749068": {
    "blob": {
      "blob_path": "/srv/docker/dispersed_object_store/data/disk2/blob",
      "rocksdb_info": {
        "backup_id": 5,
        "timestamp": "1693763705",
        "size": "5939407",
        "num_files": 10
      },
      "blob_backup_id": "5"
    }
  }
},
"3": {
  "status": 1,
  "rocksdb_info": {
    "backup_id": 5,
```

```
"timestamp": "1693763708",  
  
"size": "201223876",  
  
"num_files": 16  
},  
  
"backends": {  
  
  "360601927": {  
  
    "blob": {  
  
      "blob_path": "/srv/docker/dispersed_object_store/data/disk2/blob",  
  
      "rocksdb_info": {  
  
        "backup_id": 5,  
  
        "timestamp": "1693763720",  
  
        "size": "6252619",  
  
        "num_files": 15  
  
      },  
  
      "blob_backup_id": "5"  
  
    }  
  
  },  
  
  "1202462078": {  
  
    "blob": {  
  
      "blob_path": "/srv/docker/dispersed_object_store/data/disk1/blob",  
  
      "rocksdb_info": {  
  
        "backup_id": 5,  
  
        "timestamp": "1693763725",  
  
        "size": "9392734",
```



```
        "num_files": 15
      },
      "blob_backup_id": "5"
    }
  }
},
"4": {
  "status": 1,
  "rocksdb_info": {
    "backup_id": 5,
    "timestamp": "1693763729",
    "size": "223651851",
    "num_files": 15
  },
  "backends": {
    "199161773": {
      "blob": {
        "blob_path": "/srv/docker/dispersed_object_store/data/disk2/blob",
        "rocksdb_info": {
          "backup_id": 5,
          "timestamp": "1693763742",
          "size": "5719444",
```

```
        "num_files": 14
      },
      "blob_backup_id": "5"
    }
  },
  "661017583": {
    "blob": {
      "blob_path": "/srv/docker/dispersed_object_store/data/disk1/blob",
      "rocksdb_info": {
        "backup_id": 5,
        "timestamp": "1693763738",
        "size": "10137511",
        "num_files": 15
      },
      "blob_backup_id": "5"
    }
  }
}
```

13.1.3 Получение списка бэкапов

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

Пример команды получения списка бэкапов:

```
ucs-dispersed-object-store-client leader backup list -H dos.ucs-dos-shard-4.ucs-
developers.example.com -p 7400 --token=***** --
tls_settings.key_file=/srv/tls/keys/dos.ucs-dos-shard-1.ucs-developers.example.com-main-
key.pem --tls_settings.client_cert_file=/srv/tls/certs/dos.ucs-dos-shard-1.ucs-
developers.example.com-main-client.pem --tls_settings.ca_file=/srv/tls/certs/ucs-infra-1.ucs-
developers.example.com-main-ca.pem
```

13.1.4 Восстановление из бэкапа

При потере или повреждении данных можно восстановить их из резервного копирования. Присутствуют следующие ограничения:

- Если данные были повреждены, то для их восстановления из бэкапа необходимо сначала удалить данные в основном хранилище.
- В данном релизе восстанавливаются все данные, кроме backend-данных.

Для восстановления данных в режиме Standalone необходимо выполнить следующие действия:

1. Остановить ноду.
2. Поменять поле в конфигурационном файле **server.recovery_mode = true**.
3. Запустить ноду.
4. Если не известен идентификатор (ID) backup, то его можно найти в списке backup.
5. Запустить команду по **restore** из backup.
6. Остановить ноду.
7. Поменять поле в конфиге.
8. Запустить ноду **server.recovery_mode = false**.

Пример команды **restore**:

```
ucs-dispersed-object-store-client leader backup restore \
-H 127.0.0.1 -p 20300 --token **** --servus_token **** \
--backup_time 1212121212 // идентификатор backup
```

Для восстановления данных в режиме отказоустойчивости необходимо выполнить следующие действия:

1. На машине оператора запустить установку DOS на новую ноду через Ansible с помощью команды:

```
ansible-playbook -i hosts.yml playbooks/mailion/core.yml --tags=dos
```

2. Остановить все ноды командой:

```
docker stop dispersed_object_store
```

3. Монтировать сетевые диски с бэкапом DOS в `/srv/docker/dispersed_object_store/backup/` или копировать данные этой папки с сервера резервного копирования.
4. Копировать `raft json /srv/docker/dispersed_object_store/backup/rsm_dump.1693763682.json` с ноды лидера в бэкап-директории остальных нод.
5. На всех нодах DOS в конфигурационный файл `/srv/docker/dispersed_object_store/conf/config.json` в секцию `server` добавить параметр `recovery_mode = true`.

6. Запустить DOS на всех нодах с помощью команды:

```
docker start dispersed_object_store
```

7. Запустить команду `restore` из бэкапа на «лидере».
8. Остановить все ноды.
9. Изменить поле в конфигурационном файле `server.recovery_mode = false` на всех нодах.
10. Запустить DOS на всех нодах с помощью команды:

```
docker start dispersed_object_store
```

Пример команды для восстановления из бэкапа при установке в режиме отказоустойчивости:

```
ucs-dispersed-object-store-client leader backup restore --token=***** --servus_token
***** -H dos.ucs-dos-shard-1.ucs-developers.example.net -p 7400
--token=RhtgjcmmLe[f          --tls_settings.key_file=/srv/tls/keys/dos.ucs-dos-shard-1.ucs-
developers.example.net-main-key.pem --tls_settings.client_cert_file=/srv/tls/certs/dos.ucs-dos-
shard-1.ucs-developers.example.net-main-client.pem --tls_settings.ca_file=/srv/tls/certs/ucs-
infra-1.ucs-developers.example.net-main-ca.pem --backup_time 1693767209 \      //
идентификатор бэкапа
--local=false \                // восстановление из кластерного бэкапа
(запускается на лидере кластера)
--remote_endpoints="dos.ucs-dos-shard-2.ucs-developers.example.net:7400,dos.ucs-dos-
shard-3.ucs-developers.example.net:7400,dos.ucs-dos-shard-4.ucs-
developers.example.net:7400" // восстанавливаем кластер из 3 нод [1,2,3]; команда
запускалась с ноды [1]; перечисляем эндпойнты
```

13.1.5 Частичное восстановление из бэкапа для кластера

Для кластера существует возможность восстановить часть нод из бэкапа. Для этого необходимо выполнить следующие действия:

1. Получить статус бэкапа (см. раздел 13.1.2).
2. В структуре **node_backups** для всех нод, которые необходимо восстановить, определить идентификаторы локальных бэкапов (поле **timestamp**).
3. Перезапустить все требующие восстановления ноды в режиме восстановления.
4. На каждой ноде, которую необходимо восстановить, провести локальное восстановление. Необходимо использовать команду восстановления с флагом **--local=true**, а в качестве идентификатора бэкапа указать **локальный идентификатор бэкапа** из структуры **node_backups**.

Пример сообщения в ответе:

```
{
  "error": {
    "module": 24,
```

```
"code": 200,
"msg": "succeeded",
"details": []
},
"backups": [
  {
    "backup_time": "1634895238",
    "status": 1,
    "node_backups": {
      "1": {
        "status": 1,
        "rocksdb_info": {
          "backup_id": 1,
          "timestamp": "1634895238",
          "size": "23785",
          "num_files": 5
        }
      },
      "2": {
        "status": 1,
        "rocksdb_info": {
          "backup_id": 1,
          "timestamp": "1634895238",
          "size": "23785",
          "num_files": 5
        }
      },
      "3": {
        "status": 1,
        "rocksdb_info": {
          "backup_id": 1,
          "timestamp": "1634895239",
          "size": "23785",
          "num_files": 5
        }
      }
    }
  }
]
}
```

Задание на автоматическое резервное копирование в планировщик задач может быть включено через конфигурирование инсталлятора с помощью переменной:

```
dispersed_object_store_backup_full_job_cron_enabled
```

Переменная принимает булевы значения: true (включено) или false (выключено).

13.2 ArangoDB

13.2.1 Резервное копирование

Для резервного копирования ArangoDB необходимо выполнить следующие действия:

1. Запустить скрипт для бэкапов, который находится на машине инфраструктуры по пути `/srv/docker/arangodb_backup/cron_scripts/arangodb_backup.sh`.
2. Бэкап запускается по расписанию через **crontab root** пользователя:

```
0 0 * * * /srv/docker/arangodb_backup/cron_scripts/arangodb_backup.sh
```

3. Дампы создаются в каталоге `/srv/backups/arangodb`.

Примечание – Задание на автоматическое резервное копирование в планировщик задач включается с помощью переменной:

```
arangodb_backup_enabled: true
```

По умолчанию включено.

13.2.2 Восстановление

Для восстановления необходимо выполнить следующие действия:

1. Разархивировать архив. Структура из архива с дампом:

```
root@ucs-infra-1:/srv/backups/arangodb/arangodb_2023_01_27_0000# ll
total 12
drwxr-xr-x. 2 root root 4096 Jan 27 00:00 ektor
-rw-r-----. 1 root root  4 Jan 27 00:00 ENCRYPTION
drwxr-xr-x. 2 root root 4096 Jan 27 00:00 euripides
drwxr-xr-x. 2 root root 41 Jan 27 00:00 _syste
```

2. Выполнить скрипт (восстановление баз ArangoDB):

```
#!/bin/bash
set -e

BACKUP_DIR="/srv/backups/arangodb"

docker run \
  -e TZ="Europe/Moscow" \
  --log-driver syslog \
  --log-opt syslog-address=udp://ucs-infra-1.installation.example.net:514 \
  --log-opt tag=arangodb \
  --name arangodb_restore \
  --rm \
  -v "${BACKUP_DIR}":"${BACKUP_DIR}" \
  192.168.113.164:5000/arangodb:3.8.4-2-35 \
  arangorestore \
  --all-databases true \
  --create-database true \
  --input-directory "${BACKUP_DIR}/arangodb_2023_01_27_0000" \
  --server.authentication true \
  --server.endpoint 'http+ssl://arangodb.ucs-catalog-1.installation.example.net:8529' \
  --server.password 'password' \
  --server.username 'root'
```

Примечание – Утилиты `arangodump` и `arangorestore` вызываются из образа с `arangodb`.
 Инструкции по использованию команд:
<https://www.arangodb.com/docs/stable/programs-arangodump.html>,
<https://www.arangodb.com/docs/stable/programs-arangorestore.html>

13.3 Redis

Резервное копирование Redis не требуется, т.к. в большей части экземпляров redis, используемых в ПО «Mailion», хранится кэш. Исключением является Redis для сервиса **dafnis** – в нем хранятся данные о квотах пользователей. Если резервная копия была сделана ранее, при восстановлении хранилища с квотами из бэкапа, будут получены некорректные данные факта используемой квоты и ее расчета в системе. Поэтому, в случае потери данных этого хранилища лучше использовать механизм пересчета квот через команду **recount_quotas** с помощью интерфейса командной строки.

13.3.1 Резервное копирование

Данные Redis находятся в каталоге **/srv/docker/redis/data/dump.rdb**. Необходимо выполнить следующие действия:

1. Для актуального состояния дампа необходимо сохранить состояние базы через **redis-cli**. Указать порт и пароль в следующей команде:

```
docker exec -ti redis redis-cli -p port -a password save
```

2. Остановить сервис redis, выполнив команду:

```
docker stop redis
```

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

13.3.2 Восстановление

Для восстановления необходимо выполнить следующие действия:

1. Остановить образ Redis с помощью команды:

```
# docker stop redis
```

2. Убрать текущие файлы баз в рабочей директории:

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

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

4. Отключить AOF **appendonly no** в `/srv/docker/redis/conf/redis.conf`.

Примечание – AOF – аббревиатура от Append Only File. Свойство компьютерного хранилища данных, позволяющее добавлять новые данные в хранилище, но при этом существующие данные остаются неизменными.

5. Запустить сервис Redis с помощью команды:

```
# docker start redis
```

6. Включить AOF, новый файл появится в каталоге `/srv/docker/redis/data/appendonly.aof`

```
# docker exec -ti redis redis-cli -a password
127.0.0.1:6379> BGREWRITEAOF
Background append only file rewriting started
```

7. Остановить сервис Redis с помощью команды:

```
# docker stop redis
```

8. Включить AOF в конфиге redis **appendonly yes** в `/srv/docker/redis/conf/redis.conf`

9. Запустить Redis с помощью команды:

```
# docker start redis
```

Примечание – Официальные инструкции по ссылке <https://redis.io/topics/persistence>.

13.4 MongoDB

13.4.1 Резервное копирование

Для резервного копирования MongoDB необходимо выполнить следующие действия:

1. Запустить скрипт для бэкапов, который находится на машине инфраструктуры по пути `/srv/docker/mongodb/backup_scripts/mongodb_backup.sh`.

2. Бэкап запускается по расписанию через файл `/etc/cron.d/ansible_mongodb_backup`:

```
#Ansible: mongodb-backup
0 1 * * * root /srv/docker/mongodb/backup_scripts/mongodb_backup.sh
```

3. Дампы создаются в каталоге `/srv/backups/mongodb/`.

Примечание – Задание на автоматическое резервное копирование в планировщик задач включается с помощью переменной:

```
mongodb_backup_cron_enabled: true
```

По умолчанию включено.

Mongodump и mongorestore не могут быть частью стратегии резервного копирования для сегментированных кластеров 4.2+, в которых выполняются сегментированные транзакции, поскольку резервные копии, созданные с помощью mongodump, не поддерживают гарантии атомарности транзакций между сегментами.

Примечание – Инструкции по командам: <https://docs.mongodb.com/manual/tutorial/backup-and-restore-tools/#basic-mongodump-operations>, <https://docs.mongodb.com/manual/tutorial/backup-and-restore-tools/#restore-a-database-with-mongorestore>, <https://docs.mongodb.com/database-tools/mongorestore/#mongodb-binary-bin.mongorestore>.

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

13.4.2 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/backups/mongodb/data/backups" \
  192.168.113.164:5000/mongo:4.4.10-12 \
  mongorestore \
  --uri=mongodb://mongodb.ucs-infra-1.installation.example.net \
  --port=27017 \
  --username="username" \
  --password="password" \
```

```
--drop \  
/data/backups/mongodb_dump_2023_01_27_0100.gz
```

Примечание – При восстановлении на существующую базу нужно использовать ключ **--drop**, чтобы избежать ошибок с **duplicate key**. При восстановлении на чистый экземпляр запущенного сервиса **mongodb** ключ **--drop** не требуется. Если требуется восстановить коллекцию с текущим **UUID**, нужно использовать ключ **--drop** с **--preserveUUID**, иначе новой коллекции будет присвоен новый **UUID** (подробнее: <https://docs.mongodb.com/database-tools/mongorestore/#std-option-mongorestore.--preserveUUID>).

13.5 Search

Для резервного копирования необходимо выполнить следующие действия:

1. Остановить сервис, дампы которого нужно сделать, – **dirbek** или **mailbek_search**.
2. Заархивировать каталог с данными: **tar -czpf имя_сервис_data.tar.gz /srv/docker/имя_сервиса/data**.
3. Скопировать архив на тестовый сервер поиска: **rsync -ax имя_сервиса_data.tar.gz root@searchstage.example.net:/tmp**.

Все данные поисковых подсистем могут быть восстановлены через полный проход по всем объектам.

Данные кэша поиска по пользователям, письмам, событиям и пр. можно полностью пересоздать. Подробная информация приведена в разделах 13.5.1 и 13.5.2.

13.5.1 Ручная синхронизация данных в **dirbek** – поиске по пользователям

В состав поставки входит вспомогательный скрипт, с помощью которого можно провести переиндексацию пользователей в индексе поискового движка.

Вспомогательная утилита поставляется внутри контейнера **perseus**, соответственно, на любой машине с ролью **ucs_catalog**.

Для вызова команды на переиндексацию выполнить:

```
docker exec -it perseus ucs-perseus-dirmole-upsync -c /etc/ucs/perseus/config.json
```

13.5.2 Ручная переиндексация почтовых ящиков или календарных событий в поиске

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

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

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

При запуске скрипта можно вызвать справку использования с помощью команды:

```
[root@ucs-infra-1 ~]# /bin/ucs-sreindexer -h  
Usage: ucs-sreindexer <scope> <your_tenant_id>  
scopes:  
mail - index all users mails  
cal - index all users calendar events
```

Команда на реиндексацию всех почтовых ящиков:

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

Команда на реиндексацию всех календарных событий:

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

13.6 Настройка роли `ApplicationImpersonation` (Олицетворение)

Важно – Для настройки потребуется доступ к `Microsoft Exchange Management Shell`, который будет подключен к настраиваемому серверу `Microsoft Exchange`.

Роль **ApplicationImpersonation** позволяет приложениям олицетворять пользователей в организации для выполнения задач от имени пользователя.

Олицетворение – это стандартная техника, которую службы используют для ограничения клиентского доступа к ресурсам домена службы. В Microsoft Exchange используется управление доступом на основе ролей (RBAC). Поэтому для возможности олицетворения приложения потребуется присвоить аккаунту приложения роль **ApplicationImpersonation** (предварительно приложению нужно создать аккаунт, если его нет). Помимо присвоения роли, возможно, потребуется ограничить область видимости для присвоенной аккаунту приложения роли (**ManagementScope**).

Для этого необходимо выполнить следующие действия:

1. Создать ограничения области видимости:

```
New-ManagementScope -Name:<scopeName> -RecipientRestrictionFilter:"<Filter>"
```

2. Присвоить роль **ApplicationImpersonation** и ограничение области видимости для этого присвоения:

```
New-ManagementRoleAssignment -Name:<Assignment name> -  
Role:ApplicationImpersonation -User:<impersonationuser>  
CustomRecipientWriteScope:<ManagementScope>
```

3. Проверить, какой фильтр указан в **ManagementScope**:

```
Get-ManagementScope | Format-list RecipientFilter,Identity
```

4. Проверить, какой **ManagementScope** указан для присвоенных ролей и каким аккаунтам присвоены роли:

```
Get-ManagementRoleAssignment -RoleAssigneeType User -Role ApplicationImpersonation |  
Format-list User,Role,EffectiveUserName,CustomRecipientWriteScope,DataObject,Identity
```

5. Изменить **ManagementScope** для присвоенной роли:

```
Set-ManagementRoleAssignment -Identity <identity> -CustomRecipientWriteScope  
<scopeIdentity>
```

6. Изменить фильтр **ManagementScope**:

```
Set-ManagementScope -Identity <scopeIdentity> -RecipientRestrictionFilter:"<Filter>"
```

7. **Пример** – Создать скоуп для управления почтовыми аккаунтами в OU "ad.installation.example.net/FS":

```
New-ManagementScope -Name "FS_Mailboxes" -RecipientRoot  
"ad.installation.example.net/FS" -RecipientRestrictionFilter "RecipientType -eq 'UserMailbox'"
```

8. Создать роль и привязать ее к пользователю и скоупу:

```
New-ManagementRoleAssignment -Name "NMRassignment" -Role  
"ApplicationImpersonation" -User "ADUSR01" -CustomRecipientWriteScope  
"FS_Mailboxes"
```

14 АВТОМАТИЧЕСКОЕ КОНФИГУРИРОВАНИЕ КЛИЕНТА «МОЙОФИС ПОЧТА»

Автоконфигурация клиента включает следующие шаги:

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

14.1 Адресные книги CardDAV

Пример секции файла, содержащей адресные книги:

```
"addressbooks": {
  "login": "user@example.net",
  "addressbookPasswordUri": "https://test.example.net",
  "addressbookUri": "https://test.example.net /dav.php/addressbooks/user@example.net"
},
```

Описание полей приведено в таблице 64.

Таблица 64 – Описание полей секции файла, содержащей адресные книги

Параметр	Тип	Описание
addressbookPasswordUri	Str	Специфическое поле для настольного клиента. URI домена.
login	Str	Логин для доступа к CardDAV
addressbookUri	Str	URI DAV-коллекции книг

14.2 Календари CalDAV

Пример секции файла, содержащей календари:

```
"calendars": {
  "eventAttachSizeLimit": 2000000,
  "login "user@example.net",
  "calendarPasswordUri": "https://test.example.net",
  "calendarUri": "https://test.example.net /dav.php/calendars/user@example.net"
},
```

Описание полей приведено в таблице 65.

Таблица 65 – Описание полей файла секции файла, содержащей календари

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

14.3 Глобальная адресная книга LDAP

Пример секции файла, содержащей глобальную адресную книгу:

```
"ldap": {
  "exists": true,
  "binddn": "mail=user@example.net,ou=People,dc=test.example.net,dc=ru",
  "description": "Глобальная адресная книга",
  "basedn": "ou=IT,dc=test.example.net,dc=ru",
  "uri": "ldaps://test.example.net:636/",
  "searchFilter": "(objectclass=*)",
  "autocompleteFilter": "(!((displayName=%v*)(mail=%v*)))",
  "fullname": "Test User"
},
```

Описание полей приведено в таблице 66.

Таблица 66 – Описание полей секции файла, содержащей календари

Параметр	Тип	Описание
exists	Str	Используется ли наш LDAP сервер как глобальная адресная книга
binddn	Str	DN подключения (Bind DN)

Параметр	Тип	Описание
description	Str	Специфическое поле для настольного клиента. Описание книги.
basedn	Str	База поиска
uri	Str	Uri LDAP сервера (включает протокол и порт)
searchFilter	Str	Фильтр поиска по книге
autocompleteFilter	Str	Фильтр для поиска в клиентском автокомплите
fullname	Str	Имя и фамилия пользователя из адресной книги, если есть, если нет, то false

Важно – Score для LDAP поиска будет subtree. Паролем будет являться пароль пользователя.

14.4 Настройки FCM

Пример секции файла, содержащей клиентские настройки FCM:

```
"fcm":
{
  "exists": true,
  "ios":
  {
    "api_key": "AIzaSyAFmtvX4xZB3SUSHIWn9Nsvl02yI4ulKK8",
    "app_id": "1:799400580219:ios:bf6f80e6feb4d4b29dfede",
    "messaging_sender_id": "799400580219",
    "project_id": "aamil-push"
  },
  "android":
  {
    "api_key": "AIzaSyA4q_SeJKESXGEEFwM_wylha-Zy_fidATQ",
    "app_id": "1:799400580219:android:96051b1c3139ef31",
    "messaging_sender_id": "799400580219",
    "project_id": "aamil-push"
  },
  "huawei": {},
}
```

Описание полей приведено в таблице 67.

Таблица 68 – Описание полей секции файла, содержащей клиентские настройки FCM

Параметр	Тип	Описание
exists	Str	Используется ли FCM

Важно – Остальные поля используются мобильными клиентами, пояснения по их значениям необходимо уточнять у разработчиков мобильных клиентов.

14.5 Другие ответы сервера

Описание примеров сообщений об ошибке приведены в таблице 69.

Таблица 69 – Описание примеров сообщений об ошибке

Пример	Тело сообщения
Неправильный логин или пароль, код ответа 403	{ "message": "You don't have the permission to access the requested resource. It is either read-protected or not readable by the server." }
Не передан обязательный параметр, код ответа 400	{"message": {"password": "password required"}}
Ошибка сервера, код ответа 500	{"message": "Internal Server Error"}

15 УДАЛЕНИЕ КЛИЕНТА «МОЙОФИС ПОЧТА»

15.1 Удаление приложения на ОС Windows

Удаление приложения «МойОфис Почта» можно выполнить с помощью Панели управления ОС Windows. Рассмотрим удаление на примере ОС Windows 10.

Чтобы удалить приложение, откройте меню «Пуск» Windows и выберите Панель управления.

В окне **Панель управления** выберите **Программы и компоненты**.

В списке программ (см. Рисунок 70) выберите приложение «МойОфис Почта» и нажмите кнопку **Удалить**.

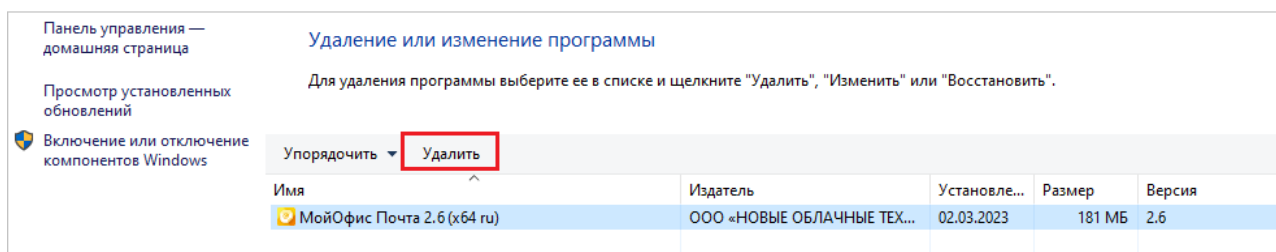


Рисунок 70 – Окно **Удаление или изменение программы**

В мастере удаления, представленном на рисунке 71, нажмите кнопку **Далее**.

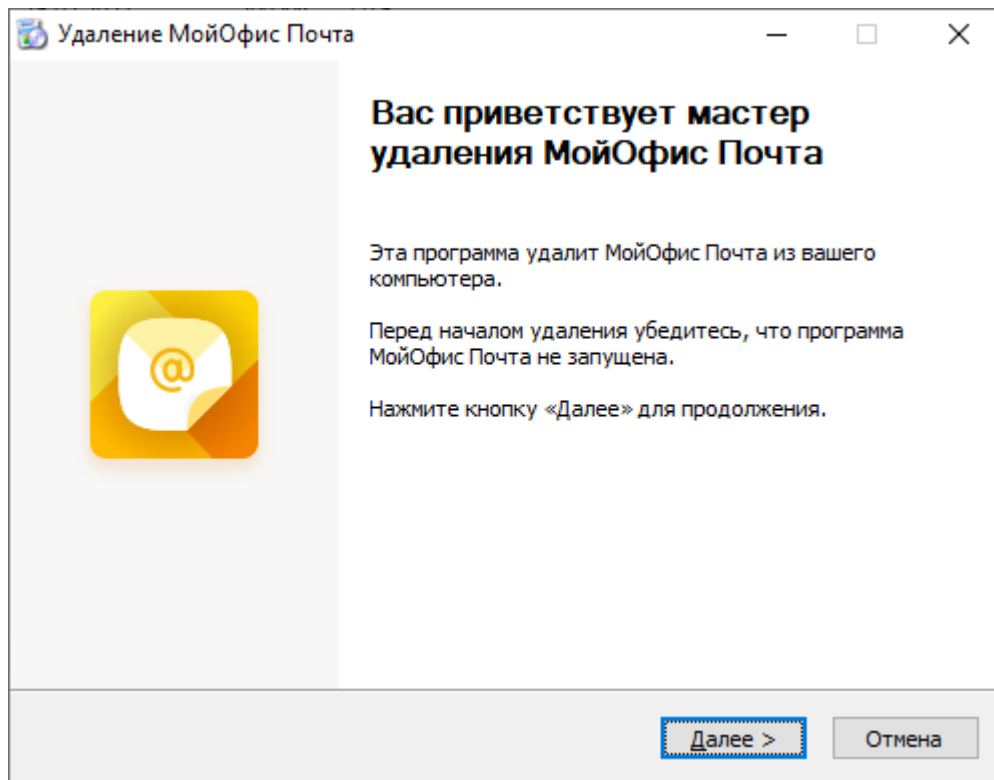


Рисунок 71 – Запрос на подтверждение удаления приложения

Дождитесь подготовки к удалению, нажмите кнопку **Удалить** (см. Рисунок 72).

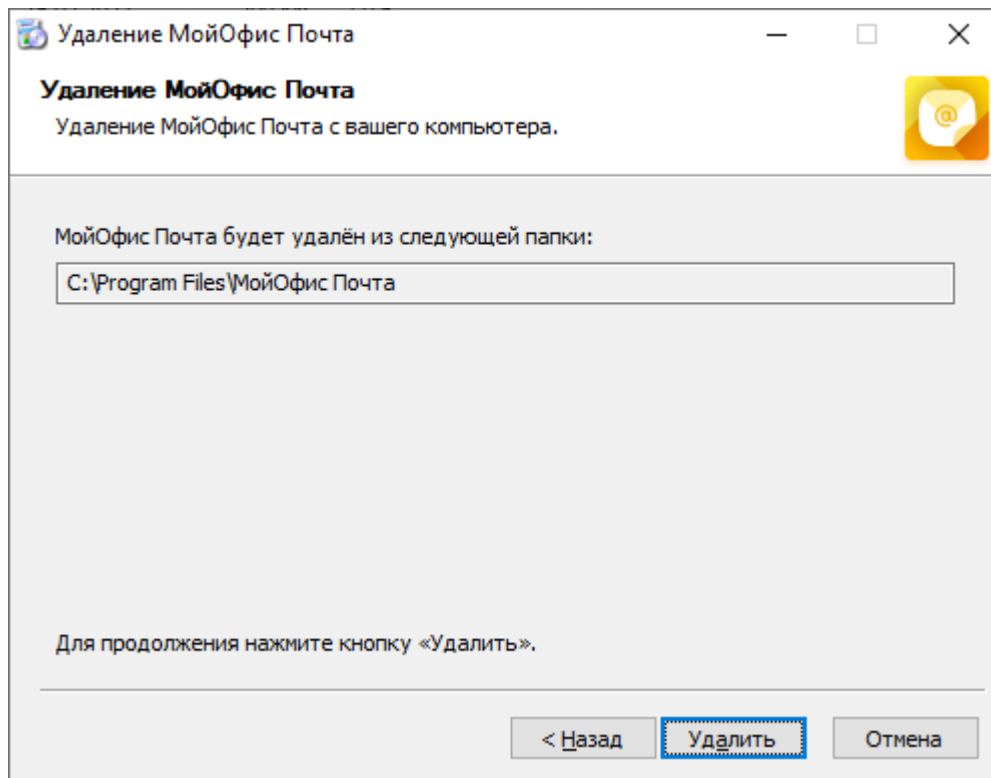


Рисунок 72 – Удаление компонентов приложения

На окончательном экране мастера удаления МойОфис Почта нажмите **Готово** (см. Рисунок 73).

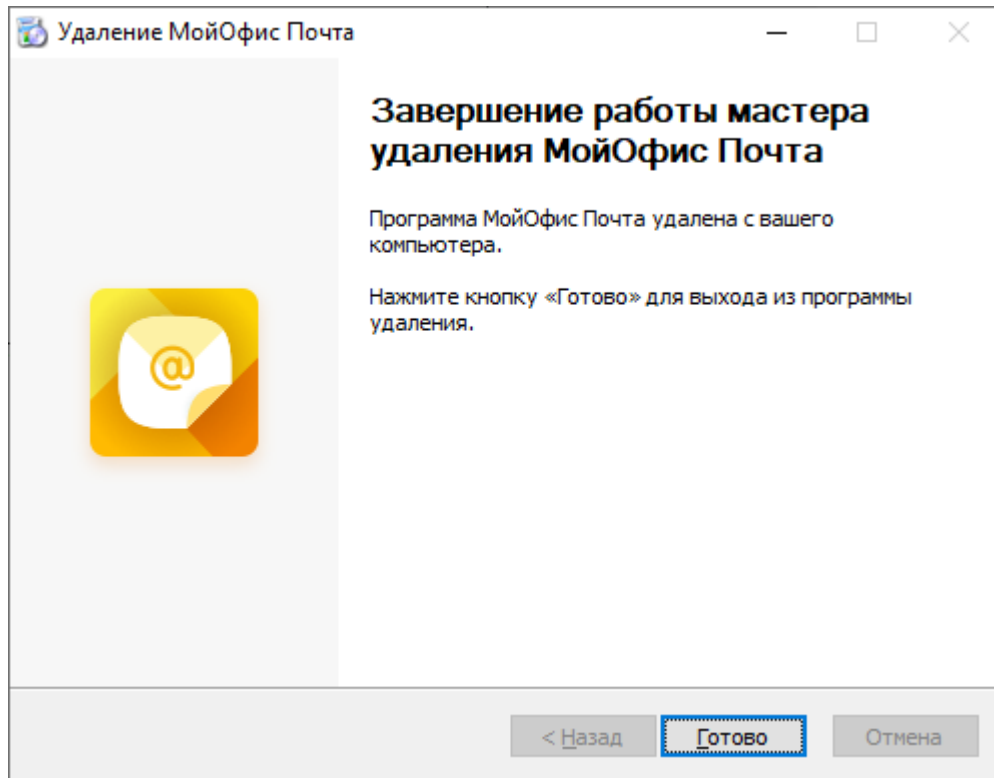


Рисунок 73 – Завершение работы мастера удаления

Если удаление приложения «МойОфис Почта» завершается успешно, строка приложения автоматически удаляется из списка программ.

15.2 Удаление приложения на ОС Linux

Для удаления приложения «МойОфис Почта» на ОС Linux выполните следующие действия:

1. Откройте терминал в папке, в которой находится файл дистрибутива «МойОфис Почта» `MyOffice_Mail_PSN_clean_Linux_x64_2.6.1.sh`.
2. При необходимости добавьте необходимые права исполняемому файлу дистрибутива, если вы не делали этого ранее:

```
chmod +x ./MyOffice_Mail_PSN_clean_Linux_x64_2.6.1.sh
```

3. Запустите выполнение файла дистрибутива:

```
./MyOffice_Mail_PSN_clean_Linux_x64_2.6.1.sh
```

4. Укажите **2**, чтобы начать процесс удаления приложения (см. Рисунок 74).

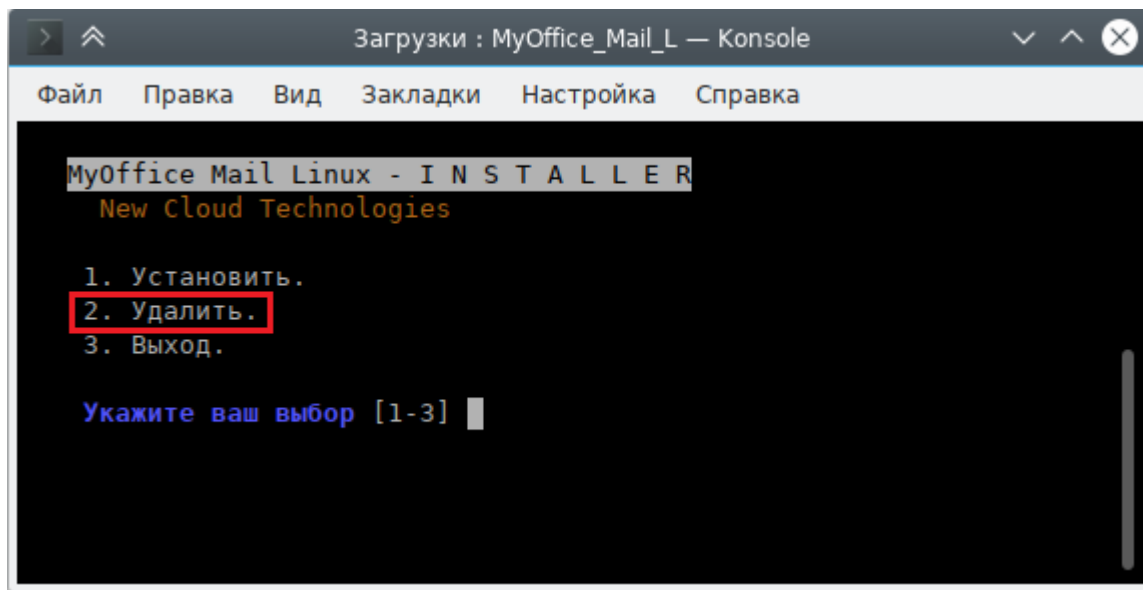


Рисунок 74 – Выбор основного сценария действий

5. Введите **yes**, чтобы согласиться с удалением приложения (см. Рисунок 75).

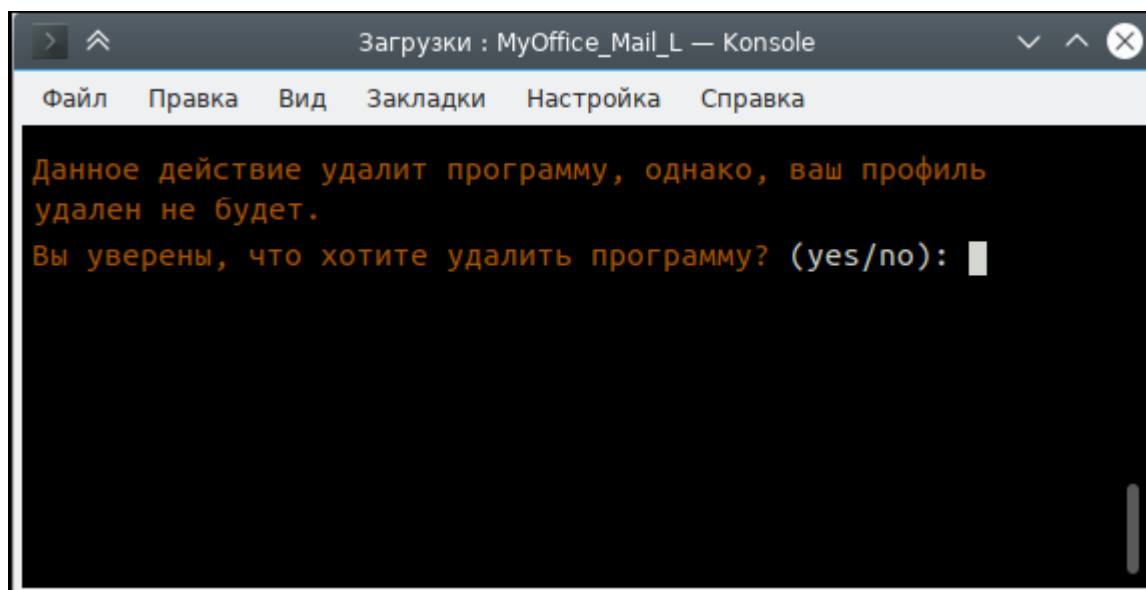


Рисунок 75 – Подтверждение удаления приложения

6. При необходимости укажите папку приложения (см. Рисунок 76).

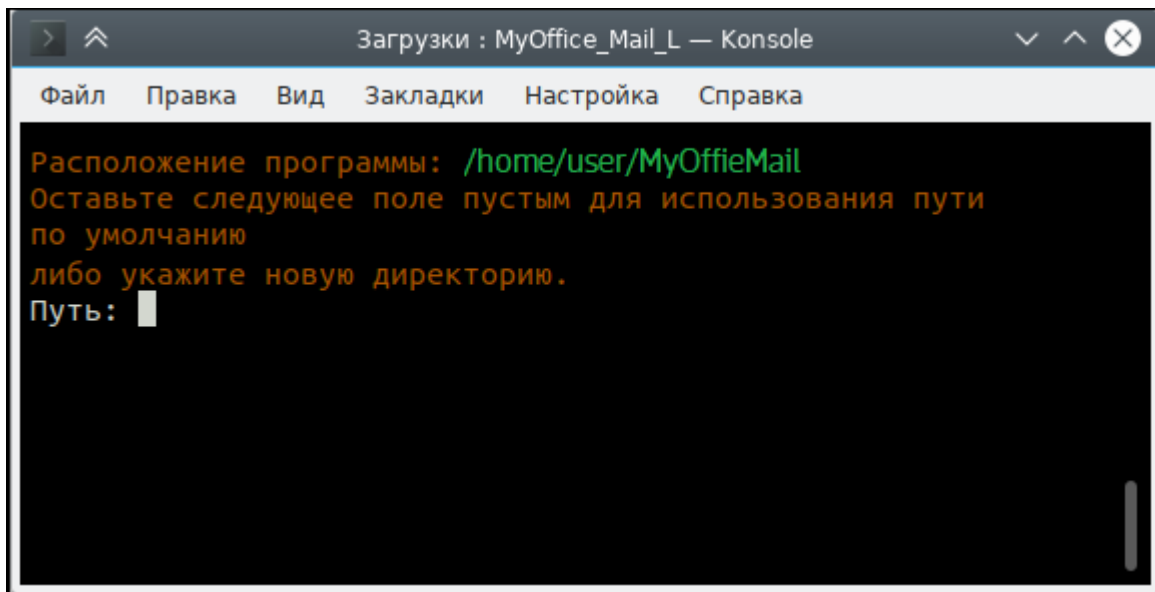


Рисунок 76 – Указание пути приложения

7. Приложение удалено.

16 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

16.1 Сбор и анализ логов

Syslog-ng – сервис централизованного сбора журналов работы системы, включающий в себя **Syslog-ng tier** и **Syslog-ng collector**. Более подробная информация о них приведена ниже.

16.1.1 Syslog-ng tier

На каждый сервер в поставке устанавливается экземпляр **syslog-ng**, который именуется как **tier syslog-ng**.

Данный экземпляр имеет следующие задачи:

- сбор всех данных, поступающих к нему по имени сервера или внутренним адресам через порт 514/udp;
- переопределение заголовка `hostname` на имя сервера.

Журналы собираются по протоколу без гарантии доставки, так как предполагается, что внутри машины возникновение проблем с сетью достаточно мала.

Локальный **syslog-ng** в поставке имеет дополнительные настройки для того, чтобы:

- сохранять копии журналов локально;
- отправлять данные на единый коллектор **syslog-ng**;
- использовать буфер на диске для отправляемых данных (подробнее см. на официальном сайте разработчика);
- настраивать параметры гарантии доставки (по умолчанию гарантия доставки отключена, подробнее см. на официальном сайте разработчика).

16.1.2 Syslog-ng collector

Коллектор **syslog-ng** устанавливается на инфраструктурную машину.

Данный коллектор имеет следующие задачи:

- сбор всех журналов с сервисов, которые используются на инфраструктурной машине;
- прием и агрегирование журналов с других серверов системы, раскладывая их по отдельным директориям.

Журналы на коллектор отправляются по протоколу гарантирующему доставку на порт 601/tcp.

Коллектор имеет дополнительные параметры:

- настройки количества соединений tcp (по умолчанию вычисляется по формуле);
- фильтрации для соединений с других серверов на базе имени сервера (опционально).

16.1.3 Доставка журналов до сервера логирования

Практически каждый сервис в поставке самостоятельно устанавливает соединение с сервером логирования и отправляет на него свои журналы. Дополнительно на сами контейнеры установлены правила отправки журналов на сервер логирования через **docker log-driver**.

Такое разделение вызвано следующими идеями:

- **log-driver** системы контейнеризации работает медленнее встроенного механизма за счет нескольких слоев перенаправления данных;
- **log-driver** системы контейнеризации используется для ПО с открытым исходным кодом, которые не умеют самостоятельно отправлять журналы на серверы логирования, устанавливая удаленное соединение по протоколу **syslog**;
- **log-driver** системы контейнеризации дополняет сборку журналов на случай, если сервис не может быть запущен и не успевает инициализировать соединение с серверов логирования.

16.1.4 Настройка параметров Syslog-ng

Описание настройки параметров **Syslog-ng** приведено в таблице 167.

Таблица 167 – Настройка параметров Syslog-ng

Параметр	Тип данных	Описание
syslog_ng:		Словарь параметров syslog_ng
disk_buffer:		Эта опция позволяет помещать исходящие сообщения в дисковый буфер места назначения, чтобы избежать потери сообщения в случае сбоя системы на стороне назначения
disk_buf_size:	int	Максимальный размер дискового буфера в байтах. Минимальное значение – 1048576 байт. Если установить меньшее значение, минимальное значение будет использоваться автоматически (По умолчанию: 335544320)
enabled:	bool	Включить/Отключить дисковый буфер (По умолчанию: False)
mem_buf_size:	int	Этот параметр содержит размер сообщений в байтах, который используется в части памяти дискового буфера. Используется только вместе с параметром reliable: True , параметр будет проигнорирован, если указано reliable: False (По умолчанию: 201326592)
reliable:	bool	Если значение этого параметра установлено в True , syslog-ng не может потерять журналы в случае перезагрузки/перезапуска, недоступности места назначения или сбоя syslog-ng . Это решение обеспечивает более медленный, но надежный вариант дискового буфера. Он создается и инициализируется при запуске и постепенно увеличивается по мере поступления новых сообщений. Если установлено значение False , будет использоваться обычный дисковый буфер. Это обеспечивает более быстрый, но менее надежный вариант дискового буфера (По умолчанию: False)
collector:		Эта опция определяет параметры настройки коллектора syslog-ng
service_ports:	list	Порты TCP/UDP для коллектора
hostname:	Str	Имя хоста для установки коллектора syslog-ng
image:		Эта опция определяет параметры настройки используемого образа
registry:	Str	Путь к образу в хранилище docker-registry
tag:	Str	Имя тега образа
services:	dict	Список сервисов для правил фильтрации логов

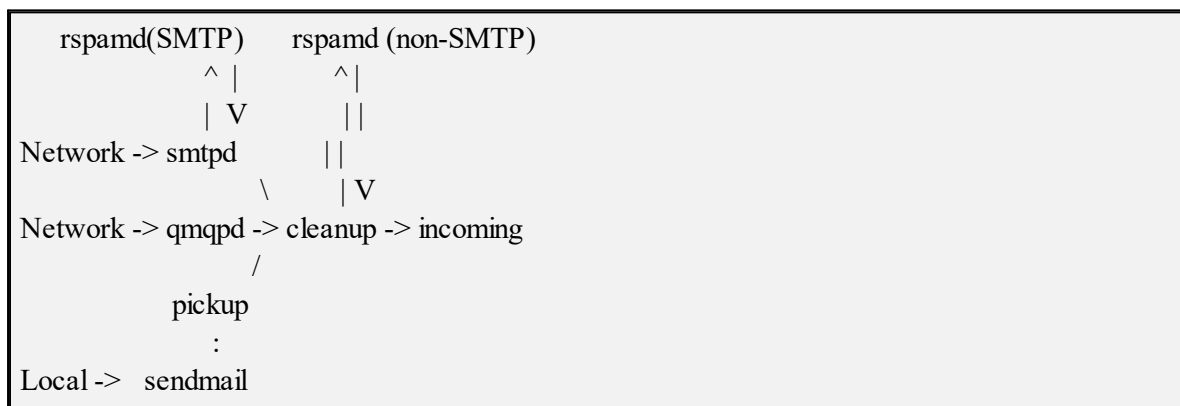
Параметр	Тип данных	Описание
tier:		Эта опция определяет параметры хранения и отправки для локального syslog-ng
send_remote	bool	Отправка журналов работы системы на коллектор
local_store:	bool	Хранение логов на локальном сервере
service_ports:	list	Порт для отправки сообщений для локального syslog-ng

16.2 Антиспам

Rspamd – это продвинутая система фильтрации нежелательной почты, которая позволяет оценивать сообщения по ряду правил, включая регулярные выражения, статистический анализ и пользовательские сервисы, такие как черные списки URL. Каждое сообщение анализируется **Rspamd** и получает оценку вероятности нежелательной почты. В соответствии с этим показателем и настройками пользователя **Rspamd** рекомендует 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:



Типы Milter:

- SMTP-only – обрабатывают почту, приходящую через **smtpd**. Обычно используется для отсеивания нежелательной почты и подписи почты от авторизованных клиентов;
- Non-SMTP – обрабатывает почту, поступающую через командную строку, **qmqpd**-сервер. Обычно используется для цифровой подписи почты.

Rspamd в ПО «Mailion» используется и как SMTP-only, и как non-SMTP milter.

Более подробную информацию про **Rspamd** можно найти на официальном сайте разработчика, про архитектуру postfix и работу milter в postfix – на официальном сайте **postfix**.

Для настройки **Rspamd** в ПО «Mailion» следует использовать переменные роли **Rspamd**. Подробная информация о них описана в таблице 168.

Таблица 168 – 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>
dkim_key: Примечание – При наличии дополнительного внешнего домена добавляется еще один параметр dkim_key .	 -----BEGIN PRIVATE KEY----- ... -----END PRIVATE KEY-----	
dkim_selector:	“mail”	Переключатель функции DKIM ключа
plugins:		Настройка исключений плагина антиспам системы, реализующего технологию серых списков: https://rspamd.com/doc/modules/greymailing.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	

Параметр	Пример заполнения	Описание
rate:	0.5	
to_ip:		Лимит на всю почту, получаемую с одного адреса-источника (на получателя)
burst:	100	
rate:	0.5	
bounce_to:		Общий лимит на bounce (на получателя)
burst:	5	
rate:	0.5	
bounce_to_ip:		Лимит на bounce из одного адреса-источника (на получателя)
burst:	5	
rate:	0.5	
user:		Лимит на всю почту (на пользователя)
burst:	0	
rate:	0.01666666667	
proxy_port:	11332	Прослушиваемый прокси-порт
service_port:	11333	Порт, прослушиваемый сервисом
use_tls:	false	Использование TLS для сетевых соединений
web_port:	11334	Порт, прослушиваемый веб-интерфейсом сервиса
web_password:	"passwd"	Пароль для доступа к веб-интерфейсу
configuration:		
composites:		composites используются для сложения (конкатенации) существующих правил и создания более комплексных правил: https://rspamd.com/doc/configuration/composites.html
test_composite_1:		
expression:	"SYMBOL1 and SYMBOL2 and (not SYMBOL3 not SYMBOL4 not SYMBOL5)"	
score:	1.0	
group:	"some group"	

Параметр	Пример заполнения	Описание
description:	"description 1"	
policy:	"leave"	
test_composite_2:		
expression:	"SYMBOL3 and SYMBOL4 and (not SYMBOL5 not SYMBOL6 not SYMBOL7)"	
score:	2.0	
group:	"some group"	
description:	"description 2"	
policy:	"remove_symbol"	

Для настройки, сбора статистики, журнала обработки писем и обучения **Rspamd** доступен веб-интерфейс, который будет доступен по адресам VM-группы **ucs_mail_mx**.

Например: `ucs-mail-1.example.net:{{ rspamd.web_port }}`.

В интерфейсе будут доступны вкладки **Status**, **Throughput**, **Configuration**, **Symbols**, **Scan/Learn**, **Test selectors**, **History**:

- **Status** отображает общую статистику работы **Rspamd**;
- **Throughput** предоставляет графики действий;
- **Configuration** предоставляет интерфейс работы с конфигурацией;
- **Symbols** предоставляет интерфейс работы с правилами;
- **Scan/Learn** предоставляет интерфейс сканирования и обучения **Rspamd**;
- **Test selectors** предоставляет интерфейс проверки и работы с селекторами **Rspamd**;
- **History** предоставляет интерфейс просмотра истории действий **Rspamd**.

16.3 Подключение антивирусного модуля KSE (Kaspersky)

Rspamd поддерживает несколько сторонних антивирусных модулей, в том числе Kaspersky. Настройка данного модуля осуществляется через переменные роли **Rspamd**, приведенные в таблице 169.

Таблица 169 – Настройка переменных ролей Rspamd

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

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

Подробное описание этих ролей приведено в таблице 170.

Таблица 170 – Настройка переменных ролей Rspamd

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

Важно – Продукт Kaspersky Scan Engine не является частью поставки ПО «Mailion».

16.4 Аудит действий

Для получения событий из аудита выполнить запрос:

```
nct-ministerium --config juliett.json --c --
-v get_audit_events_by_app_name
--timestamp_from "2012-11-01T22:08:41+00:00"
--timestamp_to "2022-11-01T22:08:41+00:00"
```

```

--limit 10
--tenant_id c4972e94-2aff-49ce-4e40-f3c3268bea45
--actors_ids dfe7d654-96ef-454a-a41c-2e83385460b5
--app_name APP_NAME_CATALOG

```

Описание параметров запроса приведено в таблице 171.

Таблица 171 – Описание параметров запроса на получение аудита

Параметр	Тип	Обязательность	Описание
time	Str	+	Время регистрации события
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
app_name	Str	+	Имя приложения

16.4.1 Поиск событий безопасности пользователя

16.4.1.1 Вход в систему

Для входа в систему и создания сессии 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 172.

Таблица 172 – Описание параметров запроса на вход в систему и создания сессии

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта

Параметр	Тип	Обязательность	Описание
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "5a40de50-ac11-0009-0301-000000000000",
      "actor_id": "53c6173f-3e64-4112-93b0-c0c380b33a51",
      "method": {
        "code": "METHOD_MINOS_CREATE_SESSION",
        "name": "METHOD_MINOS_CREATE_SESSION"
      },
      "time": {
        "unixmicro": "1663337892000000",
        "zone": 10800,
        "zone_name": ""
      },
      "touches": null,
      "client_ip": "\u003cnil\u003e",
      "streamseq": "0"
    },
    {
      "request_id": "5a40de50-ac11-0009-0301-000000000000",
      "actor_id": "53c6173f-3e64-4112-93b0-c0c380b33a51",
      "method": {
        "code": "METHOD_MINOS_CREATE_SESSION",
        "name": "METHOD_MINOS_CREATE_SESSION"
      },
      "time": {
        "unixmicro": "1663337892000000",
        "zone": 10800,
        "zone_name": ""
      },
      "response": {
        "@type": "catalog.minos.v1.CreateSessionResponse",
        "error": {
          "module": "INTERNAL",
          "code": 200,
          "msg": ""
        }
      }
    }
  ]
}
```

```
    "details": []
  },
  "access_token": "",
  "expire_at": null,
  "user_id": "",
  "duration": null,
  "need_change_credential": false,
  "quotas_state": [],
  "refresh_token": "",
  "auth_type": "RESERVED",
  "awaiting_second_factor": false,
  "secret_key": "",
  "blocked_for": "0"
},
"touches": null,
"client_ip": "\u003cnil\u003e",
"streamseq": "0"
}
],
"next": {
  "time": {
    "unixmicro": "1663337892000000",
    "zone": "10800"
  },
  "requestId": "5a40de50-ac11-0009-0301-000000000000",
  "actorId": "53c6173f-3e64-4112-93b0-c0c380b33a51",
  "methodCode": "METHOD_MINOS_CREATE_SESSION"
},
"is_final": false
}
```

16.4.1.2 Смена пароля пользователя

Для смены пароля пользователя 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 173.

Таблица 173 – Описание параметров запроса на смену пароля пользователя

Параметр	Тип	Обязательность	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
}
```

16.4.2 Поиск событий безопасности администратора

16.4.2.1 Операции над пользователем

16.4.2.1.1 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 174.

Таблица 174 – Описание параметров запроса на создание пользователя

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "d2770df7-a32f-4542-a3e0-28ea4829bf94",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_CREATE_USER",
        "name": "METHOD_MINISTERIUM_CREATE_USER"
      },
      "time": {
        "unixmicro": "1663304717000000",
        "zone": "10800",
        "zone_name": ""
      },
      "request": {
        "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
        "name": "create_user",
        "input": "{\n  \"tls_settings\": {\n    \"ca_file\": \"../builds/0/mail-back-tests/certs/ca.pem\",\n    \"client_cert_file\": \"../builds/0/mail-back-tests/certs/client.crt.pem\",\n    \"server_cert_file\": \"../builds/0/mail-back-tests/certs/client_key.pem\",\n    \"key_file\": \"../builds/0/mail-back-tests/certs/client_key.pem\",\n    \"server_name_override\": \"\",\n    \"client_auth_type\": \"\",\n    \"tls_min_version\": \"\"",
```

```

{"prefer_server_cipher_suites":false,"use_tls_bundle":false},"cox":{"endpoint":"grpc-
install.example.net:3142","balancer_endpoint":"hydra.ucs-apps-
1.install.example.net:50053","balancer_endpoints":null,"service_name":"cox",
"load_balanced":false,"use_tls":true,"use_tls_balancer":false,"request_timeout":
"10s","max_send_size":"0B","max_recv_size":"0B","compression":"none",
"is_external":false},"token-name":"ucs-access-token","admin":{"login":
"admin_tenant@install.example.net","password":"bKv9jqZ9PSwqKD7s"},
"tenant_id":"01068ade-1cce-4125-ab6b-91d977ecf85b","region_id":"2dbacea3-
5889-4021-8f38-bc2214dd7423","login":
"autotest_1663293917.343707@install.example.net","password":
"4TXoWASIMGD$EY3*.ij","email":
"autotest_1663293917.343707@install.example.net","profile":{"first_name":
"Герасим","last_name":"Одинцов","middle_name":"","locale":"","addresses":
[],"department":"","title":"","phones":[],"preferable_phone":"","gender":"","
"birthday":"","roles":[],"gal_tags":["0c22be2e-1e2f-5f6d-bec5-842c5d48e9d3"],
"quotas":{}}
},
"touches": null,
"client_ip": "172.17.0.2",
"streamseq": "0"
},
{
"request_id": "57b87da0-62f9-4c38-a180-ebe8add7421b",
"actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
"method": {
"code": "METHOD_MINISTERIUM_CREATE_USER",
"name": "METHOD_MINISTERIUM_CREATE_USER"
},
"time": {
"unixmicro": "1663304718000000",
"zone": "10800",
"zone_name": ""
},
"request": {
"@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
"name": "create_user",
"input": {"tls_settings":{"ca_file":"/builds/0/mail-back-tests/certs/ca.pem",
"client_cert_file":"/builds/0/mail-back-tests/certs/client.crt.pem","server_cert_file":
"", "key_file":"/builds/0/mail-back-tests/certs/client_key.pem",
"server_name_override":"","client_auth_type":"","tls_min_version":"","
"prefer_server_cipher_suites":false,"use_tls_bundle":false},"cox":{"endpoint":"grpc-
install.example.net:3142","balancer_endpoint":"hydra.ucs-apps-
1.install.example.net:50053","balancer_endpoints":null,"service_name":"cox",
"load_balanced":false,"use_tls":true,"use_tls_balancer":false,"request_timeout":
"10s","max_send_size":"0B","max_recv_size":"0B","compression":"none",
"is_external":false},"token-name":"ucs-access-token","admin":{"login":
"admin_tenant@install.example.net","password":"bKv9jqZ9PSwqKD7s"},

```



```

\"tenant_id\": \"01068ade-1cce-4125-ab6b-91d977ecf85b\", \"region_id\": \"2dbacea3-5889-4021-8f38-bc2214dd7423\", \"login\":
\"autotest_1663293917.881039@install.example.net\", \"password\":
\"pJuPaw(lmbC2zAhOG3MS\", \"email\":
\"autotest_1663293917.881039@install.example.net\", \"profile\": { \"first_name\":
\"Нифонт\", \"last_name\": \"Медведев\", \"middle_name\": \"\", \"locale\": \"\", \"addresses\":
\"\", \"department\": \"\", \"title\": \"\", \"phones\": [], \"preferable_phone\": \"\", \"gender\": \"\",
\"birthday\": \"\", \"roles\": [], \"gal_tags\": [\"0c22be2e-1e2f-5f6d-bec5-842c5d48e9d3\"],
\"quotas\": {} }
  },
  \"touches\": null,
  \"client_ip\": \"172.17.0.2\",
  \"streamseq\": \"0\"
}
],
\"next\": {
  \"time\": {
    \"unixmicro\": \"1663304718000000\",
    \"zone\": 10800
  },
  \"requestId\": \"57b87da0-62f9-4c38-a180-ebe8add7421b\",
  \"actorId\": \"59ed9c03-0c75-47e2-ac12-eacf6f775431\",
  \"methodCode\": \"METHOD_MINISTERIUM_CREATE_USER\"
},
\"is_final\": false
}

```

16.4.2.1.2 Обновление профиля пользователя

Для обновления профиля пользователя 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 175.

Таблица 175 – Описание параметров запроса на обновление профиля пользователя

Параметр	Тип	Обязательность	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": "{\n  \"tls_settings\": {\n    \"ca_file\": \"../builds/0/mail-back-tests/certs/ca.pem\",\n    \"client_cert_file\": \"../builds/0/mail-back-tests/certs/client.crt.pem\",\n    \"server_cert_file\": \"\",\n    \"key_file\": \"../builds/0/mail-back-tests/certs/client_key.pem\",\n    \"server_name_override\": \"\",\n    \"client_auth_type\": \"\",\n    \"tls_min_version\": \"\",\n    \"prefer_server_cipher_suites\": false,\n    \"use_tls_bundle\": false\n  },\n  \"cox\": {\n    \"endpoint\": \"grpc-install.example.net:3142\",\n    \"balancer_endpoint\": \"hydra.ucs-apps-1.install.example.net:50053\",\n    \"balancer_endpoints\": null,\n    \"service_name\": \"cox\",\n    \"load_balanced\": false,\n    \"use_tls\": true,\n    \"use_tls_balancer\": false,\n    \"request_timeout\": \"10s\",\n    \"max_send_size\": \"0B\",\n    \"max_recv_size\": \"0B\",\n    \"compression\": \"none\",\n    \"is_external\": false\n  },\n  \"token-name\": \"ucs-
```

```

access-token\", \"admin\": { \"login\": \"admin_tenant@install.example.net\", \"password\":
\\\"bKv9jqZ9PSwqKD7s\\\", \"entity_id\": \"ca6d8fca-f2bf-4ff4-a08e-987e23b99f4c\", \"profile\":
{ \"first_name\": \"Адриан\", \"last_name\": \"Новиков\", \"middle_name\": \"Викторович\",
\\\"locale\": \"en_US\", \"addresses\": [ { \\\"name\\\": \\\"Один заложить.\\\", \\\"country\\\": \\
\\\"Ямайка\\\", \\\"region\\\": \\\"Тульская обл.\\\", \\\"city\\\": \\\"п. Токма\\\", \\\"zip_code\\\": \\
\\\"132543\\\", \\\"address\\\": \\\"пр. Тенистый, д. 682 стр. 62\\\", \\\"floor\\\": \\\"59\\\", \\
\\\"room\\\": \\\"72\\\", \\\"workplace\\\": \\\"760\\\", \\\"coordinates\\\": { \\\"latitude\\\": 33.09753, \\
\\\"longitude\\\": 15.37725}, \\\"preference\\\": 28, \\\"type\\\": \\\"work\\\"} ] }, \"department\":
\\\"department_1663296204\\\", \"title\": \"title_1663296204\\\", \"phones\": [ \\\"WORK:
+72939806278\\\", \\\"HOME:8 658 438 44 22\\\" ], \"preferable_phone\": \"+72939806278\\\",
\\\"gender\": \"FEMALE\", \"birthday\": \"1979-02-10\\\", \"create\": false, \"gal_tags\": [],
\\\"gal_region_id\": \"\" }
    },
    \"touches\": null,
    \"client_ip\": \"172.17.0.2\",
    \"streamseq\": \"0\"
  },
  {
    \"request_id\": \"873a1c4b-ef29-44af-8fba-cd4d005da0bc\",
    \"actor_id\": \"59ed9c03-0c75-47e2-ac12-eacf6f775431\",
    \"method\": {
      \"code\": \"METHOD_MINISTERIUM_UPDATE_USER_PROFILE\",
      \"name\": \"METHOD_MINISTERIUM_UPDATE_USER_PROFILE\"
    },
    \"time\": {
      \"unixmicro\": \"1663307007000000\",
      \"zone\": 10800,
      \"zone_name\": \"\"
    },
    \"response\": {
      \"@type\": \"type.googleapis.com/ministerium.v1.MinisteriumCommand\",
      \"name\": \"update_user_profile\",
      \"output\": \"{ \\\"changed\\\": true, \\\"failed\\\": false, \\\"msg\\\": \\\"ok\\\" } \"
    },
    \"touches\": null,
    \"client_ip\": \"172.17.0.2\",
    \"streamseq\": \"0\"
  }
],
\"next\": {
  \"time\": {
    \"unixmicro\": \"1663307007000000\",
    \"zone\": 10800
  },
  \"requestId\": \"873a1c4b-ef29-44af-8fba-cd4d005da0bc\",
  \"actorId\": \"59ed9c03-0c75-47e2-ac12-eacf6f775431\",
  \"methodCode\": \"METHOD_MINISTERIUM_UPDATE_USER_PROFILE\"
}

```

```

},
"is_final": false
}

```

16.4.2.1.3 Удаление пользователя

Для удаления пользователя 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 176.

Таблица 176 – Описание параметров запроса на удаление пользователя

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:

```

{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "60e48e50-ac11-0009-3500-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",

```

```
"method": {
  "code": "METHOD_ERAKLES_CHANGE_STATUS",
  "name": "METHOD_ERAKLES_CHANGE_STATUS"
},
"time": {
  "unixmicro": "1663331652000000",
  "zone": 10800,
  "zone_name": ""
},
"touches": null,
"client_ip": "10.7.98.71",
"streamseq": "0"
},
{
  "request_id": "60e48e50-ac11-0009-3700-000000000000",
  "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "method": {
    "code": "METHOD_ERAKLES_CHANGE_STATUS",
    "name": "METHOD_ERAKLES_CHANGE_STATUS"
  },
  "time": {
    "unixmicro": "1663331652000000",
    "zone": 10800,
    "zone_name": ""
  },
  "touches": null,
  "client_ip": "10.7.98.71",
  "streamseq": "0"
}
],
"next": {
  "time": {
    "unixmicro": "1663331652000000",
    "zone": 10800
  },
  "requestId": "60e48e50-ac11-0009-3700-000000000000",
  "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "methodCode": "METHOD_ERAKLES_CHANGE_STATUS"
},
"is_final": false
}
```

16.4.2.2 Операции над доменом

16.4.2.2.1 Создание домена

Для создания 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 177.

Таблица 177 – Описание параметров запроса на создание домена

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "3bb37f4c-ac11-0009-ad2c-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_DAIDAL_CREATE_DOMAIN",
        "name": "METHOD_DAIDAL_CREATE_DOMAIN"
      },
      "time": {
        "unixmicro": "1663306692000000",
        "zone": 10800,

```

```
    "zone_name": ""
  },
  "touches": null,
  "client_ip": "10.7.98.54",
  "streamseq": "0"
},
{
  "request_id": "3bb37f4c-ac11-0009-ad2c-000000000000",
  "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "method": {
    "code": "METHOD_DAIDAL_CREATE_DOMAIN",
    "name": "METHOD_DAIDAL_CREATE_DOMAIN"
  },
  "time": {
    "unixmicro": "1663306692000000",
    "zone": 10800,
    "zone_name": ""
  },
  "response": {
    "@type": "catalog.daidal.v1.CreateDomainResponse",
    "error": {
      "module": "INTERNAL",
      "code": 2001,
      "msg": "",
      "details": []
    },
    "id": ""
  },
  "touches": null,
  "client_ip": "10.7.98.54",
  "streamseq": "0"
}
],
"next": {
  "time": {
    "unixmicro": "1663306692000000",
    "zone": 10800
  },
  "requestId": "3bb37f4c-ac11-0009-ad2c-000000000000",
  "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "methodCode": "METHOD_DAIDAL_CREATE_DOMAIN"
},
"is_final": false
}
```

16.4.2.2.2 Обновление домена

Для обновления домена 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 178.

Таблица 178 – Описание параметров запроса на обновление домена

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "3bb37f4c-ac11-0009-b22c-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_DAIDAL_UPDATE_DOMAIN",
        "name": "METHOD_DAIDAL_UPDATE_DOMAIN"
      },
      "time": {
        "unixmicro": "1663306704000000",
```



```
"zone": 10800,
"zone_name": ""
},
"touches": null,
"client_ip": "10.7.98.54",
"streamseq": "0"
},
{
"request_id": "3bb37f4c-ac11-0009-b22c-000000000000",
"actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
"method": {
"code": "METHOD_DAIDAL_UPDATE_DOMAIN",
"name": "METHOD_DAIDAL_UPDATE_DOMAIN"
},
"time": {
"unixmicro": "1663306704000000",
"zone": 10800,
"zone_name": ""
},
"response": {
"@type": "catalog.daidal.v1.UpdateDomainResponse",
"error": {
"module": "INTERNAL",
"code": 2001,
"msg": "",
"details": []
}
},
"touches": null,
"client_ip": "10.7.98.54",
"streamseq": "0"
}
],
"next": {
"time": {
"unixmicro": "1663306704000000",
"zone": 10800
},
"requestId": "3bb37f4c-ac11-0009-b22c-000000000000",
"actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
"methodCode": "METHOD_DAIDAL_UPDATE_DOMAIN"
},
"is_final": false
}
```

16.4.2.2.3 Удаление домена

Для удаления домена 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 179.

Таблица 179 – Описание параметров запроса на удаление домена

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "3bb37f4c-ac11-0009-bc2c-000000000000",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_DAIDAL_DELETE_BY_IDS",
        "name": "METHOD_DAIDAL_DELETE_BY_IDS"
      },
      "time": {
        "unixmicro": "1663306714000000",
```

```
"zone": 10800,
"zone_name": ""
},
"touches": null,
"client_ip": "10.7.98.54",
"streamseq": "0"
},
{
  "request_id": "3bb37f4c-ac11-0009-bc2c-000000000000",
  "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "method": {
    "code": "METHOD_DAIDAL_DELETE_BY_IDS",
    "name": "METHOD_DAIDAL_DELETE_BY_IDS"
  },
  "time": {
    "unixmicro": "1663306714000000",
    "zone": 10800,
    "zone_name": ""
  },
  "response": {
    "@type": "catalog.daidal.v1.DeleteByIDsResponse",
    "error": {
      "module": "INTERNAL",
      "code": 200,
      "msg": "",
      "details": []
    },
    "deleted_ids": [],
    "not_deleted": []
  },
  "touches": null,
  "client_ip": "10.7.98.54",
  "streamseq": "0"
}
],
"next": {
  "time": {
    "unixmicro": "1663306714000000",
    "zone": 10800
  },
  "requestId": "3bb37f4c-ac11-0009-bc2c-000000000000",
  "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "methodCode": "METHOD_DAIDAL_DELETE_BY_IDS"
},
"is_final": false
}
```

16.4.2.3 Операции над ресурсом

16.4.2.3.1 Создание ресурса

Для создания ресурса 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 180.

Таблица 180 – Описание параметров запроса на создание ресурса

Параметр	Тип	Обязательность	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": "{\"tls_settings\":{\"ca_file\":\"/builds/0/mail-back-tests/certs/ca.pem\",
  \\client_cert_file\":\"/builds/0/mail-back-tests/certs/client.crt.pem\",\\server_cert_file\":\"\",
  \\key_file\":\"/builds/0/mail-back-tests/certs/client_key.pem\",\\server_name_override\":\"\",
  \\client_auth_type\":\"\",\\tls_min_version\":\"\",\\prefer_server_cipher_suites\":false,
  \\use_tls_bundle\":false},\\cox\":{\"endpoint\":\"grpc-install.example.net:3142\",
  \\balancer_endpoint\":\"hydra.ucs-apps-1.install.example.net:50053\",
  \\balancer_endpoints\":null,\\service_name\":\"cox\",\\load_balanced\":false,\\use_tls\":true,
  \\use_tls_balancer\":false,\\request_timeout\":\"10s\",\\max_send_size\":\"0B\",
  \\max_recv_size\":\"0B\",\\compression\":\"none\",\\is_external\":false},\\token-name\":\"ucs-
  access-token\",\\admin\":{\"login\":\"admin_tenant@install.example.net\",\\password\":
  \\bKv9jqZ9PSwqKD7s\"},\\tenant_id\":\"01068ade-1cce-4125-ab6b-91d977ecf85b\",
  \\region_id\":\"2dbacea3-5889-4021-8f38-bc2214dd7423\",\\email\":
  \\resource_atankcvob@install.example.net\",\\login\":\"\",\\password\":\"\",\\type\":
  \\MEETING_ROOM\",\\profile\":{\"name\":\"autotest_resource_1663294241\",\\description\":
  \\Пропаганда четко_1663294241\",\\location\":\"г. Казань_0.2871,0.4561\",
  \\geolocation\":\"0.2471,0.5491\",\\company\":\"organization_1663294241\",\\department\":
  \\department_1663294241\",\\capacity\":8},\\gal_tags\":[\\0c22be2e-1e2f-5f6d-bec5-
  842c5d48e9d3\\],\\autobook\":true,\\work_status\":true,\\locale\":\"en_US\"}"}
  },
  "touches": null,
  "client_ip": "172.17.0.2",
  "streamseq": "0"
},
{
  "request_id": "f7def38d-f6ec-41c2-838b-e0459bf2b854",
  "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "method": {
    "code": "METHOD_MINISTERIUM_CREATE_RESOURCE",
    "name": "METHOD_MINISTERIUM_CREATE_RESOURCE"
  },
  "time": {
    "unixmicro": "1663305049000000",
    "zone": "10800",
    "zone_name": ""
  },
  "response": {
    "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
    "name": "create_resource",

```

```

      "output": "{ \"Response\": { \"changed\": true, \"failed\": false, \"msg\": \"ok\" }, \"id\": \"3e5bb5f6-841b-4119-a9bb-480101759253\" }",
    },
    "touches": null,
    "client_ip": "172.17.0.2",
    "streamseq": "0"
  }
],
"next": {
  "time": {
    "unixmicro": "1663305049000000",
    "zone": "10800"
  },
  "requestId": "f7def38d-f6ec-41c2-838b-e0459bf2b854",
  "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "methodCode": "METHOD_MINISTERIUM_CREATE_RESOURCE"
},
"is_final": false
}

```

16.4.2.3.2 Обновление ресурса

Для обновления ресурса 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 181.

Таблица 181 – Описание параметров запроса на обновление ресурса

Параметр	Тип	Обязательность	Описание
admin.login	Str	+	Логин администратора тенанта
admin.password	Str	+	Пароль администратора тенанта
method	Str	+	Метод API
tenant_id	Str	+	Идентификатор тенанта

Параметр	Тип	Обязательность	Описание
actors_ids	Str	+	Идентификаторы учетных записей
time	Str	+	Время регистрации события

Пример ответа:

```
{
  "Response": {
    "changed": false,
    "failed": false,
    "msg": "ok"
  },
  "events": [
    {
      "request_id": "68cfl d91-addc-4c9b-beb1-f40ba61ad385",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacff775431",
      "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": "{\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  },\n  \"cox\": {\n    \"endpoint\": \"grpc-install.example.net:3142\",\n    \"balancer_endpoint\": \"hydra.ucs-apps-1.install.example.net:50053\",\n    \"balancer_endpoints\": null,\n    \"service_name\": \"cox\",\n    \"load_balanced\": false,\n    \"use_tls\": true,\n    \"use_tls_balancer\": false,\n    \"request_timeout\": \"10s\",\n    \"max_send_size\": \"0B\",\n    \"max_recv_size\": \"0B\",\n    \"compression\": \"none\",\n    \"is_external\": false\n  },\n  \"token-name\": \"ucs-access-token\",\n  \"admin\": {\n    \"login\": \"admin_tenant@install.example.net\",\n    \"password\": \"bKv9jqZ9PSwqKD7s\",\n    \"entity_id\": \"b012ff77-7555-4c39-9797-478a52bec6b5\",\n    \"profile\": {\n      \"name\": \"autotest_resource_1663296085\",\n      \"description\": \"Скрытый решение. 1663296085\",\n      \"location\": \"ст. Бийск_0.5581,0.6351\",\n      \"geolocation\": \"0.3011,0.1181\",\n      \"company\": \"organization_1663296085\",\n      \"department\": \"department_1663296085\",\n      \"capacity\": 29,\n      \"create\": false,\n      \"gal_tags\": [\"0c22be2e-1e2f-5f6d-bec5-842c5d48e9d3\"],\n      \"gal_region_id\": \"2dbacea3-5889-4021-8f38-bc2214dd7423\"\n    }\n  }\n}"
      },
    }
  ]
}
```

```
"touches": null,
"client_ip": "172.17.0.2",
"streamseq": "0"
},
{
  "request_id": "68cfl d91-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": "68cfl d91-addc-4c9b-beb1-f40ba61ad385",
  "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "methodCode": "METHOD_MINISTERIUM_UPDATE_RESOURCE_PROFILE"
},
"is_final": false
}
```

16.4.2.4 Операции над группами

16.4.2.4.1 Удаление группы

Для удаления группы 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 182.

Таблица 182 – Описание параметров запроса на удаление группы

Параметр	Тип	Обязательность	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\":\"/builds/0/mail-back-tests/certs/ca.pem\",\n    \"client_cert_file\":\"/builds/0/mail-back-tests/certs/client.crt.pem\",\n    \"server_cert_file\":\"\",\n    \"key_file\":\"/builds/0/mail-back-tests/certs/client_key.pem\",\n    \"server_name_override\":\"\",\n    \"client_auth_type\":\"\",\n    \"tls_min_version\":\"\",\n    \"prefer_server_cipher_suites\":false,\n    \"use_tls_bundle\":false,\n    \"cox\":{\n      \"endpoint\":\"grpc-install.example.net:3142\",\n      \"balancer_endpoint\":\"hydra.ucs-apps-1.install.example.net:50053\",\n      \"balancer_endpoints\":null,\n      \"service_name\":\"cox\",\n      \"load_balanced\":false,\n      \"use_tls\":true,\n      \"use_tls_balancer\":false,\n      \"request_timeout\":\"10s\",\n      \"max_send_size\":\"0B\",\n      \"max_recv_size\":\"0B\",\n      \"compression\":\"none\",\n      \"is_external\":false,\n      \"token-name\":\"ucs-access-token\",\n      \"admin\":{\n        \"login\":\"admin_tenant@install.example.net\",\n        \"password\":\"bKv9jqZ9PSwqKD7s\",\n        \"group_id\":\"4779ebcb-0eb9-4b21-82c3-53afc79278f3\"\n      }\n    }\n  }",
    "touches": null,
    "client_ip": "172.17.0.2",
    "streamseq": "0"
  },
  {
    "request_id": "9f39cb5d-8dde-4b62-9921-dcf72eb238cc",
    "actor_id": "59ed9c03-0c75-47e2-ac12-eacff6f775431",
    "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\":\"ok\"\n}"
    },
    "touches": null,
    "client_ip": "172.17.0.2",
    "streamseq": "0"
  }
],
"next": {
  "time": {
    "unixmicro": "1663306830000000",

```

```

    "zone": 10800
  },
  "requestId": "9f39cb5d-8dde-4b62-9921-dcf72eb238cc",
  "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "methodCode": "METHOD_MINISTERIUM_DELETE_GROUP"
},
"is_final": false
}

```

16.4.2.4.2 Обновление профиля группы

Для обновления профиля группы 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 183.

Таблица 183 – Описание параметров запроса на обновление профиля группы

Параметр	Тип	Обязательность	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": "{\n  \"tls_settings\": {\n    \"ca_file\": \"../builds/0/mail-back-tests/certs/ca.pem\",\n    \"client_cert_file\": \"../builds/0/mail-back-tests/certs/client.crt.pem\",\n    \"server_cert_file\": \"\",\n    \"key_file\": \"../builds/0/mail-back-tests/certs/client_key.pem\",\n    \"server_name_override\": \"\",\n    \"client_auth_type\": \"\",\n    \"tls_min_version\": \"\",\n    \"prefer_server_cipher_suites\": false,\n    \"use_tls_bundle\": false,\n    \"cox\": {\n      \"endpoint\": \"grpc-install.example.net:3142\",\n      \"balancer_endpoint\": \"hydra.ucs-apps-1.install.example.net:50053\",\n      \"balancer_endpoints\": null,\n      \"service_name\": \"cox\",\n      \"load_balanced\": false,\n      \"use_tls\": true,\n      \"use_tls_balancer\": false,\n      \"request_timeout\": \"10s\",\n      \"max_send_size\": \"0B\",\n      \"max_recv_size\": \"0B\",\n      \"compression\": \"none\",\n      \"is_external\": false,\n      \"token-name\": \"ucs-access-token\",\n      \"admin\": {\n        \"login\": \"admin_tenant@install.example.net\",\n        \"password\": \"bKv9jqZ9PSwqKD7s\",\n      },\n      \"entity_id\": \"4779ebcb-0eb9-4b21-82c3-53afc79278f3\",\n      \"profile\": {\n        \"name\": \"group_1663296024_jftakbfbov\",\n        \"description\": \"Торговля помолчать предоставить исполнять сопровождаться горький кузнец.\",\n      },\n      \"create\": false,\n      \"gal_tags\": [],\n      \"gal_region_id\": \"\"\n    }\n  },\n  \"touches\": null,\n  \"client_ip\": \"172.17.0.2\",\n  \"streamseq\": \"0\"\n}",
      "touches": null,
      "client_ip": "172.17.0.2",
      "streamseq": "0"
    },
    {
      "request_id": "e321df1d-61b3-4237-a7e3-a7964674d36a",
      "actor_id": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
      "method": {
        "code": "METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE",
        "name": "METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE"
      },
      "time": {
        "unixmicro": "1663306827000000",
        "zone": "10800",
        "zone_name": ""
      },
    }
  ]

```

```

"response": {
  "@type": "type.googleapis.com/ministerium.v1.MinisteriumCommand",
  "name": "update_group_profile",
  "output": "{\"changed\":true,\"failed\":false,\"msg\":\"ok\"}"
},
"touches": null,
"client_ip": "172.17.0.2",
"streamseq": "0"
}
],
"next": {
  "time": {
    "unixmicro": "1663306827000000",
    "zone": 10800
  },
  "requestId": "e321df1d-61b3-4237-a7e3-a7964674d36a",
  "actorId": "59ed9c03-0c75-47e2-ac12-eacf6f775431",
  "methodCode": "METHOD_MINISTERIUM_UPDATE_GROUP_PROFILE"
},
"is_final": false
}

```

16.5 Перечень регистрируемых методов API

В таблицах 184 и 185 представлено соответствие реализованных бизнес-функций отправляемым API-запросам в рамках ПО «Mailion».

Таблица 184 – 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
Удаление пользователя/User Delete	/v1/erakles/change_status
Создание локальной адресной книги	v1/marker/create_usertag
Переименование локальной адресной книги	v1/marker/rename_tag

Название события	Список запросов
Перемещение локальной адресной книги	v1/marker/rename_tag
Удаление локальной адресной книги	v1/marker/delete_usertag
Создание контакта в адресной книге	v1/perseus/create_contact
Удаление контакта в адресной книге	v1/marker/remove_tags_from_objects
Создание группы рассылки Создание группы/Create a Group	v1/erakles/create_entities v1/erakles/create_emails v1/perseus/save_profile
Изменение группы рассылки Изменение группы/Change a Group	v1/perseus/update_profile
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
Создание подразделения/Create a Subdivision	v1/arachne/organizational_unit/save v1/arachne/link/operate
Создание проектной группы/Create a Workgroup	v1/arachne/organizational_group/save
Создание новой должности в справочнике оргструктуры/Create Occupations	v1/arachne/occupation/save v1/arachne/link/operate
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

Название события	Список запросов
	v1/perseus/save_profile v1/theseus/create_credentials v1/erakles/change_status v1/sophokles/subjects_init
Удаление ресурса/Delete a Resource	v1/erakles/change_status
Обновить ресурс/Update resource	v1/erakles/update_entity v1/perseus/update_profile
Выход из системы/Log Out	v1/minos/delete_all_sessions
Изменение пароля/Change a Password	v1/theseus/change_password
Изменение профиля пользователя/Change User Profile	v1/perseus/update_profile
Блокирование пользователя/Block a User	v1/erakles/change_status v1/erakles/set_blocking_reason
Настройка календаря/Calendar settings changed	v1/hog/update_calendar_schedule
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 учётной записи	/v1/erakles/set_shared_access
Общий доступ к учётной записи – Предоставить право писать от моего имени	/v1/erakles/set_shared_access

Название события	Список запросов
Общий доступ к учётной записи – Предоставить право писать с моей учётной записи	/v1/erakles/set_shared_access
Общий доступ к учётной записи – Отозвать разрешение на отправку от моего имени	/v1/erakles/set_shared_access
Общий доступ к учётной записи – Отозвать разрешение писать с моей учётной записи	/v1/erakles/set_shared_access
Общий доступ к учётной записи – Закрывать доступ	/v1/erakles/unset_shared_access
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 "Удалённые"/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
Отметить непрочитанным/Mark as unread	marker/update_flag
Отметить как спам/Mark as Spam	/v1/marker/delete_objects

Название события	Список запросов
Копирование сообщения/Copy message	marker/add_tags_to_objects
Перемещение сообщения/Move message	marker/move_tags_from_objects
Создание фильтра сообщений/Create message filter	/v1/hog/add_rule
Настройка автоматического ответа/Set automatic reply	atlas/save_template hog/update_auto_respond_event_invitations hog/edit_rule
Архивация сообщений/Archive message	marker/move_tags_from_objects
Удаление сообщения/Message delete	marker/delete_objects
Вставка объекта в сообщение/Insert object into message body	attach/load_embed

Таблица 185 – Перечень отслеживаемых команд IMAP

Событие	Команда IMAP
Проверка поддержки команд IMAP сервером	CAPABILITY
Выход из системы/Log Out	LOGOUT
Поддержка активности во время сеанса, триггер для периодического запроса о состоянии сервера	NOOP
Проверка возможности начала аутентификации по TLS	STARTTLS
Аутентификация клиента (не пользователя)	AUTHENTICATE
Аутентификация в системе/Authentication	LOGIN
Получение доступа к почтовому ящику	SELECT
Получение доступа к read-only ящику пользователя	EXAMINE
Создание почтового ящика	CREATE
Удаление пользователя/Delete a User (удаление почтового ящика)	DELETE
Изменение профиля пользователя/Change User Profile (переименование почтового ящика)	RENAME
Настройка общего доступа к почтовому ящику/Mailbox Shared Access (добавление прав доступа к другому почтовому ящику)	SUBSCRIBE

Событие	Команда IMAP
Удаление прав доступа к другому почтовому ящику	UNSUBSCRIBE
Получение списка почтовых ящиков по заданным критериям	LIST
Получение списка почтовых ящиков, активизированных командой SUBSCRIBE	LSUB
Получение статуса выбранного почтового ящика	STATUS
Отправка нового сообщения/Message Sent	APPEND
Создание слепка текущего почтового ящика	CHECK
Очистка папки «Удалённые»/Empty Trash (удаление сообщений, помеченных на удаление)	CLOSE
Получение ответа по каждому удаленному письму	EXPUNGE
Поиск письма по заданному критерию	SEARCH
Получение указанных данных сообщения	FETCH
Отметить прочитанным/Mark as Read	STORE
Удаление сообщения/Message Delete	STORE
Копирование сообщения/Copy Message	COPY
Префикс для команд FETCH, STORE и COPY	UID

16.6 Дополнительные меры защиты ПО «Mailion»

Для предотвращения несанкционированного доступа в отношении файлов конфигурации, относящихся к ПО «Mailion» и содержащихся в каталогах `/srv/docker/*/conf*/`, рекомендуется обеспечить:

1. Разграничение прав доступа в помещение или стойку с установленными экземплярами ПО «Mailion» согласно составленному «белому списку» работников Клиента, обладающих необходимыми полномочиями.
2. Разграничение прав доступа для программного доступа в хостовую ОС согласно «белому списку» работников Клиента, обладающих необходимыми полномочиями.
3. Использование наложенных сертифицированных средств защиты от несанкционированного доступа.

По умолчанию в отношении каталога `/srv/docker/` установлены права доступа исключительно для суперпользователя, которые наследуются в отношении вложенных каталогов:

```
[root@ucs-infra-1 ~]# ls -ld /srv/docker/  
drwxr-x---. 14 root root 189 Jan 10 13:21 /srv/docker/
```

Подробные сведения об администрировании в ОС Astra Linux Special Edition 1.7 представлены в документе РУСБ.10015-01 95 01 «Операционная система специального назначения «Astra Linux Special Edition». Руководство администратора».

17 ВОЗМОЖНЫЕ СИТУАЦИИ И СПОСОБЫ РЕШЕНИЯ

Возможные ситуации при эксплуатации **Панели администрирования** ПО «Mailion» и способы решения приведены в таблице 186.

Таблица 186 – Возможные ситуации и способы решения

Описание ситуации	Способ решения
Не получается авторизоваться в ПО «Mailion»	Проверить корректность вводимого логина и пароля
Отображается сообщение: «Не удалось получить данные» в нижнем левом углу экрана	Обновить страницу полностью: – нажать на значок обновления на странице браузера; – нажать клавишу F5.
Бесконечная загрузка страницы	Необходимо обратить внимание, если какие-либо поля ввода были заполнены, то они удалятся. Следует предварительно скопировать или сохранить данные из полей ввода
При переходе в какой-либо раздел Панели управления отсутствуют созданные записи	

18 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Контактная информация службы технической поддержки ООО «Новые облачные технологии» в случае возникновения вопросов, не описанных в данном руководстве:

- Адрес электронной почты: support@service.myoffice.ru
- Телефон: 8-800-222-1-888.

ПРИЛОЖЕНИЕ А. ПРИМЕР НАПИСАНИЯ ВНЕШНИХ DNS-ЗАПИСЕЙ

Имя записи	Пример написания записи
api	api-test.example.com IN A <ucs_frontend_vip>
auth	auth-test.example.com IN A <ucs_frontend_vip>
autoconfig	autoconfig-test.example.com IN A <ucs_frontend_vip>
avatars	avatars-test.example.com IN A <ucs_frontend_vip>
caldav	caldav-test.example.com. 900 IN CNAME <ucs_frontend_vip>
carddav	carddav-test.example.com. 878 IN CNAME <ucs_frontend_vip>
db	db-test.example.com IN A <ucs_frontend_vip>
grpc	grpc-test.example.com IN A <ucs_frontend_vip>
imap	imap-test.example.com IN A <ucs_frontend_vip>
mail	mail-test.example.com IN A <ucs_frontend_vip>
mail._domainkey	mail._domainkey.test.example.com. 899 IN TXT "v=DKIM1;" "g=*;" "k=rsa;" "p=<DKIM_KEY>"
mx1	mx-test.example.com. 900 IN A ucs-mail-1.test.example.com
mx2	mx-test.example.com. 900 IN A ucs-mail-2.test.example.com
preview	preview-test.example.com. 900 IN CNAME <ucs_frontend_vip>
relay	relay-test.example.com. 900 IN A <ucs_mail_vip>
resources	resources-test.example.com. 900 IN A <ucs_frontend_vip>
secured	secured-test.example.com. 900 IN A <ucs_frontend_vip>
smtp	smtp-test.example.com IN A <ucs_mail_vip>
_adsp._domainkey	_adsp._domainkey.test.example.com. 900 IN TXT "dkim=all"
_autodiscover._tcp	_autodiscover._tcp.test.example.com. 900 IN SRV 0 0 443 <mailion_external_domain>
_caldavs._tcp	_caldavs._tcp.test.example.com. 900 IN SRV 0 1 6787 caldav-test.example.com.
_carddavs._tcp	_carddavs._tcp.test.example.com. 900 IN SRV 0 1 6787 carddav-test.example.com.
_grpcsec._tcp	_grpcsec._tcp.test.example.com. 900 IN SRV 0 0 3142 grpc-test.example.com.
_imap._tcp	_imap._tcp.test.example.com. 900 IN SRV 10 0 143 imap-test.example.com.
_imaps._tcp	_imaps._tcp.test.example.com. 900 IN SRV 0 0 993 imap-test.example.com.
_smtps._tcp	_smtps._tcp.test.example.com. 900 IN SRV 0 0 465 smtp-test.example.com.
_submission._tcp	_submission._tcp.test.example.com. 900 IN SRV 0 0 587 smtp-test.example.com.

Имя записи	Пример написания записи
_submissions._tcp	_submissions._tcp.test.example.com. 900 IN SRV 0 0 465 smtp-test.example.com.

ПРИЛОЖЕНИЕ Б. НАСТРОЙКИ INVENTORY ФАЙЛА ДЛЯ РАБОТЫ С VAULT

С Vault работают следующие значения:

```
integrations:
  co_auth:
    auth_uri: "https://auth-uno.devoffice.ru/oauth2/srv/token"
    client_id: "vault:cloud_office_client_id"
    client_secret: "vault:cloud_office_client_secret"
    external_api_domain: "coapi-uno.devoffice.ru"
    external_files_link: "files-uno.devoffice.ru"
    redirect_uri: "https://dummyurl.com/callback"
  google_oauth:
    token_link: "vault:google_oauth_token_link"
    client_id: "vault:google_oauth_client_id"
    client_secret: "vault:google_oauth_client_secret"
  microsoft:
    "IS7YluhZ318G7Sm89SkkfZbO":
      ads:
        base_dn: "dc=AD,dc=STAGEOFFICE,dc=RU"
        bind_user: "AD\\ADUSR25"
        bind_password: "vault:ms_ad_password"
        name: "AD"
      servers:
        - endpoint: "mdcad-dc-01.ad.stageoffice.ru:636"
          tls:
            ca_filename: "mdcad-dc-01.ad.stageoffice.ru.pem"
            cert_file: ""
            key_file: ""
            use_tls: true
            use_dc: false
      exchanges:
        impersonation_username: "AD\\ADUSR01"
        impersonation_password: "vault:ms_exchange_impersonation"
      servers:
        - ca_filename: "mdcad-dc-01.ad.stageoffice.ru.pem"
          endpoint: "https://exchange-ad.ad.stageoffice.ru/EWS/exchange.asmx"
          timeout: "1m"
          tls_handshake_timeout: "2s"
          tls_min_version: "tls1_2"
          useragent: "ucs-mexa"
  samba_dc:
    "xeGh0EisCah5thooShoo7bur":
      smb:
        base_dn: "DC=myoffice,DC=group"
        bind_user: "CN=aduser,OU=Tech,OU=CO_Users,DC=myoffice,DC=group"
        bind_password: "vault:integrations_samba_dc_account_password"
```



```
name: "myoffice"
servers:
  - endpoint: "winsrv-bdc.myoffice.group:636"
    tls:
      ca_filename: "winsrv-bdc.myoffice.group.pem"
      cert_file: ""
      key_file: ""
      use_tls: true
    use_dc: false
"PeZh0WisXah5thooWhoo9bgG":
smb:
  base_dn: "DC=samba-dc-test,DC=stageoffice,DC=ru"
  bind_user: "Administrator"
  bind_password: "vault:integrations_samba_dc_account_password"
  name: "STAGEOFFICE.RU"
servers:
  - endpoint: "samba-dc-test.stageoffice.ru:389"
    tls:
      ca_filename: ""
      cert_file: ""
      key_file: ""
      use_tls: false
    use_dc: false
freeipa:
"zuif6jeifQueey5ahWattoo0o":
dcs:
  base_dn: "dc=devoffice,dc=ru"
  bind_user: "admin"
  bind_password: "vault:integrations_freeipa_account_password"
  name: "FreeIPA"
servers:
  - endpoint: "freeipa-test.devoffice.ru:389"
    tls:
      ca_filename: ""
      cert_file: ""
      key_file: ""
      use_tls: false
    use_dc: false
aldpro:
"ALDh9ZisXah5thooWhoo9bgZ":
ald:
  base_dn: "DC=domain,DC=test"
  bind_user: "admin"
  bind_password: "vault:integrations_aldpro_account_password"
  name: "ALDPRO"
servers:
  - endpoint: "10.7.96.28:389"
    tls:
```

```
ca_filename: ""
cert_file: ""
key_file: ""
use_tls: false
use_dc: false
psn:
  account_organizer_email: "xdev59@lime.myoffice-app.ru"
  account_link: "https://mail-lime.myoffice-app.ru/dav.php/calendars"
  account_password: "vault:integrations_psn_account_password"
  account_domains: ["lime.myoffice-app.ru"]
alertmanager_alerta_api_key: "{{ vault_secrets['alerta_api_key'] }}"
arangodb_bearer_token: "vault:arango_bearer_token"
arangodb_users:
  ektor:
    password: "{{ vault_secrets['arango_ektor_pwd'] }}"
    password_mask: "vault:arango_ektor_pwd"
  sophokles:
    password: "{{ vault_secrets['arango_sophokles_pwd'] }}"
    password_mask: "vault:arango_sophokles_pwd"
  euripides:
    password: "{{ vault_secrets['arango_euripides_pwd'] }}"
    password_mask: "vault:arango_euripides_pwd"
  root:
    password: "{{ vault_secrets['arango_root_pwd'] }}"
    password_mask: "vault:arango_root_pwd"
codec_secret_key:
  rcr: "vault:codec_secret_key_rcr"
  secret_link: "vault:codec_secret_key_secret_link"
  values_codec: "vault:codec_secret_key_values_codec"
dirbek_replication_token: "vault:dirbek_replication_token"
dispersed_object_store_management_token: "vault:dos_management_token"
hydra_get_service_list_token: "vault:hydra_management_token"
house_ldapauth_password_salt: "vault:house_ldapauth_password_salt"
jwt_key:
  mask: true #включение jwt_key_mask для включения с vault_hosted
  priv_mask: "vault:jwt_pvt_key"
  pub_mask: "vault:jwt_pub_key"
  priv: "{{ vault_secrets['jwt_pvt_key'] }}"
  pub: "{{ vault_secrets['jwt_pub_key'] }}"
keepalived_vrrp_instances:
  ucs_frontend:
```

```
password: "vault:keepalived_front_pwd"
ucs_external_balancers:
  password: "vault:keepalived_external_balancers_pwd"
ucs_internal_balancers:
  password: "vault:keepalived_internal_balancers_pwd"
ucs_mail:
  password: "vault:keepalived_mail_pwd"
  virtual_ip: "192.168.216.35"

grafana_admin_password: "{{ vault_secrets['grafana_admin_pwd'] }}"

mailbek_replication_token: "vault:mailbek_replication_token"

mailion_installation_admin_password: "vault:ucs_installation_admin_password"
mailion_installation_backuper_password: "vault:ucs_installation_backuper_password"

mailion_service_accounts:
  adonis: "vault:ucs_service_account_adonis"
  ararat: "vault:ucs_service_account_ararat"
  ares: "vault:ucs_service_account_ares"
  ariadne: "vault:ucs_service_account_ariadne"
  atlas: "vault:ucs_service_account_atlas"
  authorization_plugin: "vault:ucs_service_account_authorization"
  clotho: "vault:ucs_service_account_clotho"
  cox: "vault:ucs_service_account_cox"
  dafnis: "vault:ucs_service_account_dafnis"
  dflink_plugin: "vault:ucs_service_account_dflink"
  elysion: "vault:ucs_service_account_elysion"
  erakles: "vault:ucs_service_account_erakles"
  ermis: "vault:ucs_service_account_ermis"
  hog: "vault:ucs_service_account_hog"
  homeros: "vault:ucs_service_account_homeros"
  house: "vault:ucs_service_account_house"
  imap: "vault:ucs_service_account_imap"
  kex: "vault:ucs_service_account_kex"
  kongur: "vault:ucs_service_account_kongur"
  kronos: "vault:ucs_service_account_kronos"
  leda: "vault:ucs_service_account_leda"
  lntp: "vault:ucs_service_account_lntp"
  marker: "vault:ucs_service_account_marker"
  mars: "vault:ucs_service_account_mars"
  minos: "vault:ucs_service_account_minos"
  orpheus: "vault:ucs_service_account_orpheus"
  othrys: "vault:ucs_service_account_othrys"
  paranoid: "vault:ucs_service_account_paranoid"
  pegasus: "vault:ucs_service_account_pegasus"
  perseus: "vault:ucs_service_account_perseus"
  phalanx: "vault:ucs_service_account_phalanx"
```

```
razor: "vault:ucs_service_account_razor"
saml_plugin: "vault:ucs_service_account_saml_plugin"
theseus: "vault:ucs_service_account_theseus"
viper: "vault:ucs_service_account_viper"
woof: "vault:ucs_service_account_woof"
zeus: "vault:ucs_service_account_zeus"

mars_scc_ca_file: "{{ vault_secrets['mars_scc_ca_file'] }}"
mars_scc_client_cert_file: "{{ vault_secrets['mars_scc_client_cert_file'] }}"
mars_scc_key_file: "{{ vault_secrets['mars_scc_key_file'] }}"

mongodb_exporter_password:
"{{ vault_secrets['ucs_mongodb_mongodb_exporter_password'] }}"

mongodb_management_users:
  achill:
    password: "vault:ucs_mongodb_achill_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_achill_password'] }}"
  beef:
    password: "vault:ucs_mongodb_beef_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_beef_password'] }}"
  clotho:
    password: "vault:ucs_mongodb_clotho_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_clotho_password'] }}"
  daidal:
    password: "vault:ucs_mongodb_daidal_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_daidal_password'] }}"
  ektor:
    password: "vault:ucs_mongodb_ektor_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_ektor_password'] }}"
  erakles:
    password: "vault:ucs_mongodb_erakles_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_erakles_password'] }}"
  eratosthenis:
    password: "vault:ucs_mongodb_eratosthenis_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_eratosthenis_password'] }}"
  hog:
    password: "vault:ucs_mongodb_hog_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_hog_password'] }}"
  homeros:
    password: "vault:ucs_mongodb_homeros_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_homeros_password'] }}"
  marker:
    password: "vault:ucs_mongodb_marker_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_marker_password'] }}"
  mongodb_exporter:
    password: "vault_secrets:ucs_mongodb_mongodb_exporter_password"
    password_plain: "{{ vault_secrets['ucs_mongodb_mongodb_exporter_password'] }}"
```

```
kongur:
  password: "vault:ucs_mongodb_kongur_password"
  password_plain: "{{ vault_secrets['ucs_mongodb_kongur_password'] }}"
kronos:
  password: "vault:ucs_mongodb_kronos_password"
  password_plain: "{{ vault_secrets['ucs_mongodb_kronos_password'] }}"
odusseus:
  password: "vault:ucs_mongodb_odusseus_password"
  password_plain: "{{ vault_secrets['ucs_mongodb_odusseus_password'] }}"
perseus:
  password: "vault:ucs_mongodb_perseus_password"
  password_plain: "{{ vault_secrets['ucs_mongodb_perseus_password'] }}"
sophokles:
  password: "vault:ucs_mongodb_sophokles_password"
  password_plain: "{{ vault_secrets['ucs_mongodb_sophokles_password'] }}"
talaos:
  password: "vault:ucs_mongodb_talaos_password"
  password_plain: "{{ vault_secrets['ucs_mongodb_talaos_password'] }}"
themis:
  password: "vault:ucs_mongodb_themis_password"
  password_plain: "{{ vault_secrets['ucs_mongodb_themis_password'] }}"
theseus:
  password: "vault:ucs_mongodb_theseus_password"
  password_plain: "{{ vault_secrets['ucs_mongodb_theseus_password'] }}"
thoth:
  password: "vault:ucs_mongodb_thoth_password"
  password_plain: "{{ vault_secrets['ucs_mongodb_thoth_password'] }}"

mongodb_root_password: "{{ vault_secrets['mongodb_root_password'] }}"
mongodb_secured_key: "{{ vault_secrets['mongodb_secured_key'] }}"

mongo_express_config_basicauth_password:
  "{{ vault_secrets['mongo_express_basicauth_password'] }}"
mongo_express_mongodb_cluster: "{{ groups['ucs_mongodb'] }}"

nats_authorization_password: "vault:nats_authorization_password"
nats_authorization_password_plain: "{{ vault_secrets['nats_authorization_password'] }}"
nats_backup_authorization_password_plain: "{{ nats_authorization_password_plain }}"
nats_cluster_authorization_password:
  "{{ vault_secrets['nats_cluster_authorization_password'] }}"

# санитизация redis санинела включена
redis_sentinel_sanitized_enabled: true

# в конфигурациях приложений мы используем
# маскированные пароли для редиса
```

```
redis_dafnis_password_mask: "vault:redis_dafnis_password"
redis_dowal_password_mask: "vault:redis_dowal_password"
redis_ektor_password_mask: "vault:redis_ektor_password"
redis_erakles_password_mask: "vault:redis_erakles_password"
redis_euripides_password_mask: "vault:redis_euripides_password"
redis_hog_password_mask: "vault:redis_hog_password"
redis_homeros_password_mask: "vault:redis_homeros_password"
redis_leda_password_mask: "vault:redis_leda_password"
redis_mars_password_mask: "vault:redis_mars_password"
redis_minos_password_mask: "vault:redis_minos_password"
redis_sdd_password_mask: "vault:redis_sdd_password"
redis_viper_password_mask: "vault:redis_viper_password"

redis_dafnis_password: "{{ vault_secrets['redis_dafnis_password'] }}"
redis_dowal_password: "{{ vault_secrets['redis_dowal_password'] }}"
redis_ektor_password: "{{ vault_secrets['redis_ektor_password'] }}"
redis_erakles_password: "{{ vault_secrets['redis_erakles_password'] }}"
redis_euripides_password: "{{ vault_secrets['redis_euripides_password'] }}"
redis_hog_password: "{{ vault_secrets['redis_hog_password'] }}"
redis_homeros_password: "{{ vault_secrets['redis_homeros_password'] }}"
redis_leda_password: "{{ vault_secrets['redis_leda_password'] }}"
redis_mars_password: "{{ vault_secrets['redis_mars_password'] }}"
redis_minos_password: "{{ vault_secrets['redis_minos_password'] }}"
redis_rspamd_password: "{{ vault_secrets['redis_rspamd_password'] }}"
redis_sdd_password: "{{ vault_secrets['redis_sdd_password'] }}"
redis_viper_password: "{{ vault_secrets['redis_viper_password'] }}"

rethinkdb:
  users:
    admin:
      password: "vault:rethinkdb_admin"
    read:
      password: "vault:rethinkdb_read"
    write:
      password: "vault:rethinkdb_write"
  tags:
    - "ru"
    - "ru_yankee"

rspamd_web_password: "{{ vault_secrets['rspamd_web_pwd'] }}"
weaver_rspamd_web_password: "vault:rspamd_web_pwd"

servus: "vault:servus"
#servus_plain_text: "{{ vault_secrets['servus'] }}"

sophokles_access_token: "vault:sophokles_access_token"

theseus_cipher_key: "vault:theseus_cipher_key"
```

```

tls_certs_remote_token_key: "{{ vault_secrets['tls_certs_remote_token_key'] }}"

tiphys_get_service_list_token: "vault:tiphys_management_token"

tripoli_replication_token: "vault:tripoli_replication_token"

wal_terminator_nexus_login: "{{ lookup('community.general.hashi_vault',
'infra/data/nexus/ansible').login }}"
wal_terminator_nexus_password: "{{ lookup('community.general.hashi_vault',
'infra/data/nexus/ansible').password }}"
wal_terminator_squadus_id: "{{ lookup('community.general.hashi_vault',
'infra/data/squadus/bot').id }}"
wal_terminator_squadus_token: "{{ lookup('community.general.hashi_vault',
'infra/data/squadus/bot').token }}"

# skype/iva are used in ares service only:
vcs:
  type:
    skype_4_business:
      ares_vcs_type: "skype_4_business"
      ares_vcs_endpoint: "{{ vault_secrets['vcs_skype_endpoint'] }}"
      ares_vcs_login: "vault:vcs_skype_login"
      ares_vcs_password: "vault:vcs_skype_password"
      ares_vcs_skip_insecure_tls: true
    iva:
      ares_vcs_type: "iva"
      ares_vcs_endpoint: "vault:vcs_iva_endpoint"
      ares_vcs_login: "vault:vcs_iva_login"
      ares_vcs_password: "vault:vcs_iva_password"
      ares_vcs_skip_insecure_tls: true

```

Есть два типа использования Vault в переменных:

1. Чтение значений напрямую из Vault, такие переменные имеют вид на примере ektor:

```

ektor:
  password: "{{ vault_secrets['arango_ektor_pwd'] }}"

```

При разочаровании сервиса ektor, ansible обращается в Vault для получения значения переменной **password** и после подставляет это значение напрямую в конфигурационный файл, поэтому в **config** будет виден пароль в открытом виде.

2. Значение переменной задано в маскированном виде внутри конфигурационного файла и считывается из Vault самим сервисом во время старта, т. е. сервис сам идет в Vault и забирает значения всех секретов через API:

```

ektor:

```

```
password_mask: "vault:arango_ektor_pwd"
```

Переменная имеет маскированный вид и будет отображаться в конфигурационном файле как **vault:arango_ektor_pwd**.

Это используется для того, чтобы хранить пароли в маскированном виде в конфигурационном файле и перечитывать переменные без разворота нового конфигурационного файла при изменении значений. Чтобы перечитать новые значения потребуется только перезапуск сервиса.

Также остается поддержка обратной совместимости, при нежелании работать с маскированными переменными и желании передачи значений Vault-переменных в обычном виде (пункт 1).

Для интеграции с Vault необходимо задать следующие переменные внутри inventory файла:

```
vault_integration: vault_integration:
  VAULT_TOKEN: "{{ vault_secrets['vault_token'] }}" # Здесь указывается, что для
приложений токен будет браться из самого Vault. Сам токен туда попадает на одном
из предыдущих шагов
  VAULT_ADDRESS: "https://vault.server.company:8200" # URL, полный адрес до Vault-
сервера вместе со схемой и портом
  VAULT_KV_VERSION: "v1" # Версия api Vault, менять не нужно
  VAULT_SECRET_PATH: "mailion/data/installation" # НЕ МЕНЯТЬ! Путь, по которому
приложения будут забирать секреты. Поле data здесь необходимо, так как это
специфика работы Vault api.
##set path for secrets in vault storage
vault_secret_path:
  ipa: "mailion/data/installation" # путь до хранения секретов, у клиента должно быть
указан одинаково во всех случаях перечисленных ниже
  exchange: "mailion/data/installation" #путь до хранения секретов, у клиента должно быть
указан одинаково во всех случаях, перечисленных ниже
  ad: "mailion/data/installation" # путь до хранения секретов, у клиента должно быть указан
одинаково во всех случаях, перечисленных ниже
  main: "mailion/data/installation" # путь до хранения секретов, у клиента должно быть
указан одинаково во всех случаях, перечисленных ниже
```

Для настройки для Vault потребуется в inventory файле заменить/добавить соответствующие переменные, указанные в секции выше.

Важно – Переменные из секции не являются финальной версией и должны быть настроены исходя из требований стенда.

ПРИЛОЖЕНИЕ В. КОМАНДЫ, ВЫПОЛНЯЕМЫЕ С ПОМОЩЬЮ ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ, И ИХ ОПИСАНИЕ

Доступные команды	Описание
Add_email	Добавить E-mail к объекту
Add_entity_to_group	Связать объект с группой
Add_org_structure_link	Добавить связь между двумя объектами элементов оргструктуры
Add_users_to_gal_tag	Добавить пользователей к GAL-тегу
Change_status	Изменить статус объекта
Check_gal_user	Проверить GAL-пользователя в тенанте
Check_group_all	Проверить уникальную группу в тенанте
Completion	Сгенерировать сценарий автозавершения для указанной командной оболочки
Create_domain	Создать новый домен в тенанте
Create_gal_user	Создать системного GAL-пользователя
Create_group	Создать группу
Create_group_all	Создать уникальную группу в тенанте
Create_login	Создать логин объекта
Create_oauth_client	Создать OAuth клиент
Create_password	Создать пароль для логина
Create_resource	Создать ресурс
Create_tenant	Создать новый тенант
Create_tenant_admin	Создать администратора тенанта
Create_tenant_gal_tag	Создать GAL-тег для тенанта
Create_tenant_quotas_profile	Создать квоты для профиля тенанта
Create_user	Создать пользователя
Create_user_quotas_profile	Создать квоты для пользователя
Create_users_bratch	Создать пользовательскую группу
Delete_all_related_messages_by_message_id	Удалить письма у всех получателей в рамках тенанта
Delete_domain	Удалить домен
Delete_entity_audit_levels	Удалить уровни аудита объекта
Delete_gal_tag	Удалить GAL-тег

Доступные команды	Описание
Delete_group	Удалить группу
Delete_login	Удалить логин
Delete_oauth_client	Удалить OAuth клиент
Delete_org_structure_element	Удалить элемент оргструктуры
Delete_tenant	Удалить тенант
Delete_tenant_audit_levels	Удалить уровни аудита тенанта
Delete_tenant_quotas_profile	Удалить квоты для профиля тенанта
Dynamic_group_filling_status	Проверить статус заполнения динамических групп
Export_audit_events_by_app_name_as_file	Экспортировать события аудита по имени приложения в виде файла
Export_audit_events_by_methods_codes_as_file	Экспортировать события аудита по коду методов в виде файла
Export_audit_events_by_services_names_as_file	Экспортировать события аудита по имени службы в виде файла
Find_domain	Найти домен по идентификатору или имени хоста
Generate	Сгенерировать bash файл для автозавершения команды
Get_audit_events_by_app_name	Получить события аудита по имени приложения
Get_audit_events_by_methods_codes	Получить события аудита по коду методов
Get_audit_events_by_services_codes	Получить события аудита по коду службы
Get_entity_audit_levels	Получить уровни события аудита
Get_oauth_client	Получить параметры OAuth клиента
Get_orgstructure_element_by_id	Вернуть элемент оргструктуры с получением идентификатора и типа объекта
Get_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

Доступные команды	Описание
help	Помощь по поводу любой команды
List_domains	Список доменов в тенанте
List_entities	Список объектов по идентификатору региона/тенанта, E-mail-у 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
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_entity_audit_levels	Обновить уровни аудита или объект. Создать, если значения отсутствуют
Update_group_profile	Создать или обновить профиль группы
Update_oauth_client	Обновить параметры OAuth клиента
Update_reserve_email	Обновить резервный E-mail пользователя

Доступные команды	Описание
Update_resource	Обновить ресурс
Update_resource_profile	Создать или обновить профиль ресурса
Update_roles	Создать или удалить роли объекта
Update_tenant	Обновить информацию о тенанте
Update_tenant_audit_levels	Обновить уровни аудита тенанта. Создать, если значения отсутствуют
Update_tenant_quotas_profile	Обновить квоты профиля тенанта
Update_user_profile	Создать или обновить профиль пользователя
Update_user_quotas_profile	Обновить квоты профиля пользователя
Upload_avatars	Обновить аватары домена

ПРИЛОЖЕНИЕ Г. ПРИМЕРЫ JSON-ФАЙЛОВ ДЛЯ КОМАНД, ВЫПОЛНЯЕМЫХ С ПОМОЩЬЮ ИНТЕРФЕЙСА ПРОГРАММНОЙ СТРОКИ

Г.1 Файл настроек импорта пользователей

Пример файла настроек `import_config.json` приведен ниже. Описание полей приведено в таблице 187.

```
{
  "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"
  ],
  "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 187 – Описание полей файла настроек `import_config.json`

Параметр	Тип	Описание
<code>token-name</code>	Str	Всегда имеет значение "ucs-access-token"

Параметр	Тип	Описание
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
gal_tags	Str	Список идентификаторов gal
user_data_path	Str	Путь к файлу с описанием импортируемых пользователей в одном из поддерживаемых форматов
user_data_format	Str	Формат файла импорта, может принимать одно из значений: JSON, CSV
rejected_users_path	Str	Путь к файлу, в который будут записываться пользователи, в процессе импорта которых возникла какая-либо ошибка
quotas	Str	Список квот для создаваемых пользователей: – ONE_MAIL_SIZE (размер письма); – ALL_MAILS_SIZE (размер всех писем); – ALL_MAIL_ATTACHMENTS_SIZE (размер всех вложений в письме)
roles	Str	Список идентификаторов дополнительных ролей пользователя

Г.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"
]
}
```

Г.3 Список глобальных адресных книг

Пример файла `get_tenant_gals.json` приведен ниже. Описание полей файла настроек приведено в таблице 188.

```
{
  "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 188 – Описание полей файла настроек `get_tenant_gals.json`

Параметр	Тип	Описание
<code>token-name</code>	Str	Всегда имеет значение "ucs-access-token"
<code>admin</code>	Str	Логин и пароль пользователя, от имени которого будет выполняться импорт, обычно это администратор тенанта или инсталляции
<code>cox</code>	Str	Подключение к Mailion
<code>tls_settings</code>	Str	Сертификаты, используемые для подключения к системе
<code>tenant_id</code>	Str	Идентификатор тенанта
<code>gal_tags</code>	Str	Список идентификаторов GAL
<code>user_data_path</code>	Str	Путь к файлу с описанием импортируемых пользователей в одном из поддерживаемых форматов

Г.4 Файл настроек импорта групп

Пример файла настроек **settings.json** приведен ниже. Описание полей приведено в таблице 189.

```
{
  "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 189 – 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

Параметр	Тип	Описание
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

Г.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"
  ]
}
```

Г.6 Файл настроек для импорта связей групп

Пример файла настроек **settings.json** приведен ниже. Описание полей приведено в таблице 190.

```
{
  "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 190 – Описание полей файла настроек **settings.json**

Параметр	Тип	Обязательность	Описание
token-name	Str	+	Всегда имеет значение "ucs-access-token"
admin	Str	+	Логин и пароль пользователя, от имени которого будет выполняться импорт, обычно это администратор тенанта или инсталляции
cox	Str	+	Подключение к Mailion
tls_settings	Str	+	Сертификаты, используемые для подключения к системе
group_links_data_path	Str	+	Путь к файлу с описанием импортируемых ресурсов в одном из поддерживаемых форматов. Если файл имеет расширение .json или .csv, то параметр groups_links_data_format можно не

Параметр	Тип	Обязательность	Описание
			задавать, формат будет выбран по расширению файла
group_links_data_format	Str	-	Формат файла импорта, может принимать одно из значений: JSON, CSV. Необязательный параметр, если у файла, указанного в параметре groups_links_data_path, есть расширение .json или .csv
rejected_groups_links_path	Str	-	Путь к файлу, в который система будет записывать группу, в процессе импорта которой возникла какая-либо ошибка. Если этот параметр не будет задан, то будет использоваться имя файла по умолчанию ("rejected_groups.json") и такой файл будет создан в той же директории, что и файл, переданный для импорта

Г.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"
  ]
}
```



```
]
}
```

Г.8 Файл настроек импорта ресурсов

Пример файла настроек **settings.json** приведен ниже. Описание полей приведено в таблице 191.

```
{
  "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 191 – Описание полей файла настроек **settings.json**

Параметр	Тип	Обязательность	Описание
token-name	Str	+	Всегда имеет значение "ucs-access-token"
admin	Str	+	Логин и пароль пользователя, от имени которого будет выполняться импорт,

Параметр	Тип	Обязательность	Описание
			обычно это администратор тенанта или инсталляции
cox	Str	+	Подключение к Mailion
tls_settings	Str	+	Сертификаты, используемые для подключения к системе
tenant_id	Str	+	Идентификатор тенанта UUID-строки
region_id	Str	+	Идентификатор региона в формате UUID-строки
gal_tags	Str	+	Список идентификаторов GAL
resources_data_path	Str	+	Путь к файлу с описанием импортируемых пользователей в одном из поддерживаемых форматов
resources_data_format	Str	-	Формат файла импорта, может принимать одно из значений: JSON, CSV
rejected_resources_path	Str	-	Путь к файлу, в который будут записываться пользователи, в процессе импорта которых возникла какая-либо ошибка

Г.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"
]
}
```

Г.10 Конфигурационный файл для миграции календаря из Microsoft Exchange в ПО «Mailion»

Пример конфигурационного файла приведен ниже:

```
{
  "daidal": {
    "balancer_endpoints": [
      "hydra.ucs-apps-1.installation.example.net:50053"
    ],
    "compression": "none",
    "keep_alive": false,
    "keep_alive_time": "15s",
    "keep_alive_timeout": "10s",
    "load_balanced": true,
    "request_timeout": "10s",
    "service_name": "daidal",
    "use_tls": true,
    "use_tls_balancer": true
  },
  "dispersed_object_store": {
    "balancer_endpoints": [
```

```

    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "methods": {
    "increment_copies": {
      "success_copies_num": "quorum"
    },
    "read": {
      "success_copies_num": "any"
    },
    "write": {
      "success_copies_num": "quorum"
    }
  },
  "namespace": "attach",
  "request_timeout": "10s",
  "service_name": "dispersed-object-store",
  "temporary_ttl": "1h",
  "use_tls": true,
  "use_tls_balancer": true
},
"erakles": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "erakles",
  "use_tls": true,
  "use_tls_balancer": true
},
"external_sync": {
  "exchanges": {
    "IS7YlthZ318G7Sm89SkkfZbO": {
      "impersonation_password": "vault:ms_exchange_impersonation",
      "impersonation_username": "AD\\ADUSR01",
      "servers": [
        {
          "ca_file": "/home/admin-msk/kex/cert/mdcad-dc-01.ad.example.net.pem",

```

```
        "endpoint": "https://exchange-ad.ad.example.net/EWS/exchange.asmx",
        "timeout": "1m",
        "tls_handshake_timeout": "2s",
        "tls_min_version": "tls1_2"
      }
    ],
    "useragent": "ucs-mexa"
  }
},
"hog": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "hog",
  "use_tls": true,
  "use_tls_balancer": true
},
"kongur": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "kongur",
  "use_tls": true,
  "use_tls_balancer": true
},
"logging": {
  "dump_level": "debug",
  "ultra_human": true
},
"marker": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
```

```
"keep_alive": false,
"keep_alive_time": "15s",
"keep_alive_timeout": "10s",
"load_balanced": true,
"request_timeout": "10s",
"service_name": "marker",
"use_tls": true,
"use_tls_balancer": true
},
"minos": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "minos",
  "use_tls": true,
  "use_tls_balancer": true
},
"report_logging": {
  "buffer_capacity": 512,
  "colorize": false,
  "development": true,
  "disable_caller": false,
  "dump_level": "error",
  "elastic_config": null,
  "enable_dump": false,
  "enable_stacktrace": false,
  "file_config": {
    "path": "report.txt"
  },
  "identity": "m2e",
  "level": "debug",
  "output_format": "text",
  "sampling": null,
  "show_secrets": true,
  "skip_callers": 0,
  "type": "file",
  "ultra_human": false,
  "ultra_human_fields": null
},
"server": {
  "balancer_endpoints": [
```

```
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "discovery_type": "etcd",
  "keep_alive": false,
  "keep_alive_balancer": false,
  "listen_endpoint": "0.0.0.0:6788",
  "load_balanced": true,
  "max_recv_size": "0B",
  "max_send_size": "0B",
  "service_address": "kex.ucs-apps-1.installation.example.net",
  "service_name": "kex",
  "use_tls": true,
  "use_tls_balancer": true
},
"service_auth": {
  "basic": {
    "login": "kex_login",
    "password": "vault:ucs_service_account_kex"
  },
  "type": "basic"
},
"sophokles": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "sophokles",
  "use_tls": true,
  "use_tls_balancer": true
},
"tls_settings": {
  "ca_file": "/home/admin-msk/kex/certs/ucs-infra-1.installation.example.net-main-ca.pem",
  "client_auth_type": "require_and_verify_client_cert",
  "client_cert_file": "/home/admin-msk/kex/certs/kex.ucs-apps-1.installation.example.net-main-client.pem",
  "key_file": "/home/admin-msk/kex/certs/kex.ucs-apps-1.installation.example.net-main-key.pem",
  "server_cert_file": "/home/admin-msk/kex/certs/kex.ucs-apps-1.installation.example.net-main-server.pem",
  "server_name_override": "",
  "tls_min_version": "tls1_2"
}
```



```

},
"tracer": {
  "reporter": {
    "buffer_flush_interval": "1s",
    "collector_endpoint": "ucs-infra-1.installation.example.net:6831",
    "log_spans": false,
    "queue_size": 10
  },
  "sampler": {
    "param": 1,
    "type": "const"
  },
  "use_tracer": false
},
"ucr_codec": {
  "cipher_key": "vault:codec_secret_key_rcr",
  "doc_preview_url_prefix": "https://api-installation.example.net/doc_preview",
  "mail_source_url_prefix": "https://api-installation.example.net/mail_source",
  "rcr_url_prefix": "https://api-installation.example.net/attach/read"
}
}

```

Г.11 Конфигурационный файл для миграции календаря из ПО «Mailion» в Microsoft Exchange

Пример конфигурационного файла приведен ниже:

```

{
  "daidal": {
    "balancer_endpoints": [
      "hydra.ucs-apps-1.installation.example.net:50053"
    ],
    "compression": "none",
    "keep_alive": false,
    "keep_alive_time": "15s",
    "keep_alive_timeout": "10s",
    "load_balanced": true,
    "request_timeout": "10s",
    "service_name": "daidal",
    "use_tls": true,
    "use_tls_balancer": true
  },
  "dispersed_object_store": {
    "balancer_endpoints": [
      "hydra.ucs-apps-1.installation.example.net:50053"
    ],
  },
}

```

```
"compression": "none",
"keep_alive": false,
"keep_alive_time": "15s",
"keep_alive_timeout": "10s",
"load_balanced": true,
"methods": {
  "increment_copies": {
    "success_copies_num": "quorum"
  },
  "read": {
    "success_copies_num": "any"
  },
  "write": {
    "success_copies_num": "quorum"
  }
},
"namespace": "attach",
"request_timeout": "10s",
"service_name": "dispersed-object-store",
"temporary_ttl": "1h",
"use_tls": true,
"use_tls_balancer": true
},
"erakles": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "erakles",
  "use_tls": true,
  "use_tls_balancer": true
},
"exponential_backoff": {
  "forever": false,
  "init_interval": "2s",
  "max_elapsed_time": "30s",
  "max_interval": "10s",
  "multiplier": 1.5,
  "randomization_factor": 0.5
},
"external_sync": {
  "exchanges": {
```

```
"IS7YluhZ318G7Sm89SkkfZbO": {
  "impersonation_password": "vault.ms_exchange_impersonation",
  "impersonation_username": "AD\\ADUSR01",
  "servers": [
    {
      "ca_file": "/home/admin-msk/kex/cert/mdcad-dc-01.ad.example.net.pem",
      "endpoint": "https://exchange-ad.ad.example.net/EWS/exchange.asmx",
      "timeout": "1m",
      "tls_handshake_timeout": "2s",
      "tls_min_version": "tls1_2"
    }
  ],
  "useragent": "ucs-mexa"
}
},
"hog": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "hog",
  "use_tls": true,
  "use_tls_balancer": true
},
"ical": {
  "calscale": "GREGORIAN",
  "prod_id": "Mailion Mailion_1.6.1",
  "version": "2.0"
},
"kongur": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "kongur",
  "use_tls": true,
```

```
"use_tls_balancer": true
},
"kronos": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "is_external": false,
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "retry_policy": {
    "count": 3,
    "delay": "5m"
  },
  "service_name": "kronos",
  "use_tls": true,
  "use_tls_balancer": true
},
"logging": {
  "dump_level": "debug",
  "ultra_human": true
},
"marker": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "marker",
  "use_tls": true,
  "use_tls_balancer": true
},
"minos": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
```

```
"load_balanced": true,
"request_timeout": "10s",
"service_name": "minos",
"use_tls": true,
"use_tls_balancer": true
},
"mixer": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "mixer",
  "use_tls": true,
  "use_tls_balancer": true
},
"report_logging": {
  "buffer_capacity": 512,
  "colorize": false,
  "development": true,
  "disable_caller": false,
  "dump_level": "error",
  "elastic_config": null,
  "enable_dump": false,
  "enable_stacktrace": false,
  "file_config": {
    "path": "report.txt"
  },
  "identity": "m2e",
  "level": "debug",
  "output_format": "text",
  "sampling": null,
  "show_secrets": true,
  "skip_callers": 0,
  "type": "file",
  "ultra_human": false,
  "ultra_human_fields": null
},
"server": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
```

```
"discovery_type": "etcd",
"keep_alive": false,
"keep_alive_balancer": false,
"listen_endpoint": "0.0.0.0:6788",
"load_balanced": true,
"max_recv_size": "0B",
"max_send_size": "0B",
"service_address": "kex.ucs-apps-1.installation.example.net",
"service_name": "kex",
"use_tls": true,
"use_tls_balancer": true
},
"service_auth": {
  "basic": {
    "login": "kex_login",
    "password": "vault:ucs_service_account_kex"
  },
  "type": "basic"
},
"sophokles": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053"
  ],
  "compression": "none",
  "keep_alive": false,
  "keep_alive_time": "15s",
  "keep_alive_timeout": "10s",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "sophokles",
  "use_tls": true,
  "use_tls_balancer": true
},
"tls_settings": {
  "ca_file": "/home/admin-msk/kex/certs/ucs-infra-1.installation.example.net-main-ca.pem",
  "client_auth_type": "require_and_verify_client_cert",
  "client_cert_file": "/home/admin-msk/kex/certs/kex.ucs-apps-1.installation.example.net-main-client.pem",
  "key_file": "/home/admin-msk/kex/certs/kex.ucs-apps-1.installation.example.net-main-key.pem",
  "server_cert_file": "/home/admin-msk/kex/certs/kex.ucs-apps-1.installation.example.net-main-server.pem",
  "server_name_override": "",
  "tls_min_version": "tls1_2"
},
"tracer": {
  "reporter": {
```

```

    "buffer_flush_interval": "1s",
    "collector_endpoint": "ucs-infra-1.installation.example.net:6831",
    "log_spans": false,
    "queue_size": 10
  },
  "sampler": {
    "param": 1,
    "type": "const"
  },
  "use_tracer": false
},
"ucr_codec": {
  "cipher_key": "vault:codec_secret_key_rcr",
  "doc_preview_url_prefix": "https://api-installation.example.net/doc_preview",
  "mail_source_url_prefix": "https://api-installation.example.net/mail_source",
  "rcr_url_prefix": "https://api-installation.example.net/attach/read"
},
"ultar": {
  "max_cal_size": -1,
  "max_desc_size": 1024,
  "max_sum_size": 255
}
}

```

Г.12 Конфигурационный файл для миграции почты из Microsoft Exchange в ПО «Mailion», из ПО «Mailion» в Microsoft Exchange

Пример конфигурационного файла приведен ниже:

```

{
  "atlas": {
    "balancer_endpoints": [
      "hydra.ucs-apps-1.installation.example.net:50053",
      "hydra.ucs-apps-2.installation.example.net:50053"
    ],
    "compression": "none",
    "load_balanced": true,
    "max_recv_size": "0B",
    "max_send_size": "0B",
    "request_timeout": "10s",
    "service_name": "atlas",
    "use_tls": true,
    "use_tls_balancer": true
  },
  "beef": {
    "balancer_endpoints": [

```

```

    "hydra.ucs-apps-1.installation.example.net:50053",
    "hydra.ucs-apps-2.installation.example.net:50053"
  ],
  "compression": "none",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "beef",
  "use_tls": true,
  "use_tls_balancer": true
},
"daidal": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053",
    "hydra.ucs-apps-2.installation.example.net:50053"
  ],
  "compression": "none",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "daidal",
  "use_tls": true,
  "use_tls_balancer": true
},
"erakles": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053",
    "hydra.ucs-apps-2.installation.example.net:50053"
  ],
  "compression": "none",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "erakles",
  "use_tls": true,
  "use_tls_balancer": true
},
"xync": {
  "enabled": false,
  "sync_chunk_length": 100,
  "message_size_limit": "30Mb",
  "save_message_timeout": "1m0s"
},
"external_sync": {
  "exchanges": {
    "IS7YluhZ318G7Sm89SkkfZbO": {
      "impersonation_password": "RhtgjcmmLe[f",
      "impersonation_username": "AD\\ADUSR01",
      "servers": [
        {

```



```
        "ca_file": "/etc/pki/tls/certs/mdcad-dc-01.ad.example.net.pem",
        "endpoint": "https://exchange-ad.ad.example.net/EWS/exchange.asmx",
        "timeout": "1m",
        "tls_handshake_timeout": "2s",
        "tls_min_version": "tls1_2"
    }
  ],
}
},
"hog": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053",
    "hydra.ucs-apps-2.installation.example.net:50053"
  ],
  "compression": "none",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "hog",
  "use_tls": true,
  "use_tls_balancer": true
},
"logging": {
  "buffer_capacity": 512,
  "development": true,
  "dump_level": "error",
  "enable_dump": false,
  "identity": "viper",
  "level": "debug",
  "meta_fields_param_prefix": "nctlog_",
  "output_format": "text",
  "show_secrets": true,
  "syslog_config": {
    "address": "172.17.0.1:514",
    "network": "udp"
  },
  "type": "syslog"
},
"marker": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053",
    "hydra.ucs-apps-2.installation.example.net:50053"
  ],
  "compression": "none",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "marker",
```

```
"use_tls": true,
"use_tls_balancer": true
},
"minos": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053",
    "hydra.ucs-apps-2.installation.example.net:50053"
  ],
  "compression": "none",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "minos",
  "use_tls": true,
  "use_tls_balancer": true
},
"server": {
  "compression": "none",
  "discovery_type": "native",
  "listen_endpoint": ":8181",
  "load_balanced": false,
  "max_rcv_size": "0B",
  "max_send_size": "0B",
  "service_name": "viper",
  "use_tls": false,
  "use_tls_balancer": false
},
"service_auth": {
  "basic": {
    "login": "viper_login",
    "password": "ieg9ShohngaevoiXohZo"
  },
  "type": "basic"
},
"sophokles": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053",
    "hydra.ucs-apps-2.installation.example.net:50053"
  ],
  "compression": "none",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "sophokles",
  "use_tls": true,
  "use_tls_balancer": true
},
"tls_settings": {
  "ca_file": "/etc/pki/tls/certs/ucs-infra-1.installation.example.net-main-ca.pem",
```

```
"client_auth_type": "require_and_verify_client_cert",
"client_cert_file": "/etc/pki/tls/certs/viper.ucs-apps-1.installation.example.net-main-
client.pem",
"key_file": "/etc/pki/tls/private/viper.ucs-apps-1.installation.example.net-main-key.pem",
"server_cert_file": "/etc/pki/tls/certs/viper.ucs-apps-1.installation.example.net-main-
server.pem",
"server_name_override": "",
"tls_min_version": "tls1_2"
},
"tracer": {
  "reporter": {
    "buffer_flush_interval": "1s",
    "collector_endpoint": "jaeger.example.net:6831",
    "log_spans": false,
    "queue_size": 10
  },
  "sampler": {
    "param": 1,
    "type": "const"
  },
  "use_tracer": true
},
"ucr_codec": {
  "cipher_key": "Ivu6Z0hD3C52fMKvIHK2WEerNyL71EMcIDhnGSQy95U=",
  "doc_preview_url_prefix": "https://api-installation.example.net/doc_preview",
  "mail_source_url_prefix": "https://api-installation.example.net/mail_source",
  "rcr_url_prefix": "https://api-installation.example.net/attach/read"
},
"viper": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053",
    "hydra.ucs-apps-2.installation.example.net:50053"
  ],
  "compression": "none",
  "load_balanced": true,
  "request_timeout": "10s",
  "service_name": "viper",
  "use_tls": true,
  "use_tls_balancer": true
},
"weaver": {
  "balancer_endpoints": [
    "hydra.ucs-apps-1.installation.example.net:50053",
    "hydra.ucs-apps-2.installation.example.net:50053"
  ],
  "compression": "none",
  "load_balanced": true,
```

```
"request_timeout": "10s",  
"service_name": "weaver",  
"use_tls": true,  
"use_tls_balancer": true  
}  
}
```