

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство администратора. Часть 1

Подсистема безопасности

Версия документа 1.3

Листов 215

АННОТАЦИЯ

Настоящий документ является первой частью руководства администратора прикладного программного обеспечения «Аврора Центр» релиз 2.2.2 (далее — ППО).

Руководство администратора состоит из четырех частей:

- «Руководство администратора. Часть 1. Подсистема безопасности»;
- «Руководство администратора. Часть 2. Подсистема «Маркет»;
- «Руководство администратора. Часть 3. Подсистема Платформа управления»;
- «Руководство администратора. Часть 4. Подсистема установки системных пакетов».

Настоящий документ содержит общую информацию о ППО, описание установки и конфигурационных файлов, а также описание установки мобильных приложений (МП).

СОДЕРЖАНИЕ

1. Общая информация	8
1.1. Назначение и состав ППО.....	8
1.2. Субъекты доступа и права на доступ к интерфейсам ППО	10
1.2.1. Субъекты доступа (роли) ППО.....	10
1.2.2. Права на доступ к интерфейсам ППО.....	11
1.3. Назначение и состав ПБ.....	12
1.4. Описание принципов безопасной работы средства.....	13
1.4.1. Общая информация	13
1.4.2. Компрометация паролей	14
1.4.3. Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения.....	14
1.4.4. Лицензионное соглашение.....	14
1.5. Условия выполнения.....	15
2. Подготовка к работе	19
2.1. Начало сеанса работы.....	19
2.2. Описание интерфейса.....	21
2.2.1. Верхняя панель	22
2.2.2. Рабочая область.....	23
2.2.3. Область фильтров	24
3. Выполнение программы.....	27
3.1. Консоль администратора ПБ. Раздел «Администрирование».....	27
3.1.1. Работа в подразделе «Учетные записи».....	27
3.2. Консоль администратора ПБ. Раздел «Мониторинг»	44
3.2.1. Работа в подразделе «Аудит».....	44

3.3. Окончание сеанса работы	49
4. Описание установки ППО	50
4.1. Общая информация	50
4.2. Порядок действий по приемке ППО.....	51
4.2.1. Проверка комплектности	51
4.2.2. Проверка контрольных сумм	51
4.2.3. Проверка качества изготовления	52
4.3. Порядок установки компонентов среды функционирования	52
4.3.1. Порядок установки и настройки ОС на управляющей ПЭВМ, серверах приложений и серверах БД.....	52
4.3.2. Порядок развертывания и настройки управляющей ПЭВМ.....	55
4.3.3. Порядок установки и настройки компонент среды функционирования серверов приложений.....	56
4.3.4. Порядок установки и настройки СУБД PostgreSQL (Postgres Pro)	60
4.4. Порядок установки ППО	64
4.5. Адреса веб-консолей.....	79
4.6. Пример настройки единого файлового хранилища.....	79
4.7. Действия по безопасной установке и настройке средства.....	81
4.8. Действия по реализации функций безопасности среды функционирования ППО	83
4.8.1. Установка, настройка и эксплуатация СЗИ НСД.....	83
4.8.2. Меры по межсетевому экранированию	83
4.9. Проверка корректности установки и функционирования ППО.....	84
4.10. Описание параметров конфигурационных файлов сценариев установки среды функционирования и ППО.....	86

4.10.1. Конфигурационные файлы сценариев установки среды функционирования	86
4.10.2. Конфигурационные файлы сценариев установки подсистем ППО	90
5. Резервное копирование	114
5.1. Резервное копирование после установки (обновления) ППО	114
5.2. Периодическое резервное копирование и резервное копирование перед установкой обновлений	114
5.2.1. Резервное копирование данных	114
5.2.2. Резервное копирование ППО	115
5.2.3. Резервное копирование компонентов среды функционирования	115
6. Обновление ППО	117
7. Управление сервисами и настройками сервисов (подсистем) ППО	119
7.1. Управление сервисами ППО	119
7.2. Управление настройками сервисов и подсистем ППО	122
7.2.1. Способ 1 (рекомендуемый)	122
7.2.2. Способ 2	123
8. Описание параметров конфигурационных файлов модулей ППО	125
8.1. Описание конфигурационных файлов ПБ	125
8.1.1. Общий конфигурационный файл ПБ (файл: /var/ocs/auth/config.yml)	125
8.1.2. Конфигурационный файл сервиса ocs-auth-accounts-devices-api (файл: /var/ocs/auth/ocs-auth-accounts-devices-api/ocs-auth-accounts-devices-api.yml)	127
8.1.3. Конфигурационный файл сервиса ocs-auth-accounts-users-api (файл: /var/ocs/auth/ocs-auth-accounts-users-api/ocs-auth-accounts-users-api.yml)	129
8.1.4. Конфигурационный файл сервиса ocs-auth-adminconsole-ui (файл: /var/ocs/auth/ocs-auth-adminconsole-ui/ocs-auth-adminconsole-ui.yml)	134

8.1.5. Конфигурационный файл сервиса ocs-auth-audit-api (файл: /var/ocs/auth/ocs-auth-audit-api/ocs-auth-audit-api.yml).....	143
8.1.6. Конфигурационный файл сервиса ocs-auth-idp-api (файл: /var/ocs/auth/ocs-auth-idp-api/ocs-auth-idp-api.yml)	146
8.1.7. Конфигурационный файл сервиса ocs-auth-idp-ui (файл: /var/ocs/auth/ocs-auth-idp-ui/ocs-auth-idp-ui.yml).....	150
8.1.8. Конфигурационный файл сервиса ocs-auth-server-admin (файл: /var/ocs/auth/ocs-auth-server-admin/ocs-auth-server-admin.yml).....	152
8.1.9. Конфигурационный файл сервиса ocs-auth-server-public (файл: /var/ocs/auth/ocs-auth-server-public/ocs-auth-server-public.yml)	157
8.2. Конфигурационные файлы ПМ	161
8.2.1. Общий конфигурационный файл ПМ (файл: /var/ocs/appstore/config.yml).....	161
8.2.2. Конфигурационный файл сервиса ocs-appstore-adminconsole-ui (файл: /var/ocs/appstore/ocs-appstore-adminconsole-ui/ocs-appstore-adminconsole-ui.yml)	167
8.2.3. Конфигурационный файл сервиса ocs-appstore-applications-api (файл: /var/ocs/appstore/ocs-appstore-applications-api/ocs-appstore-applications-api.yml).....	171
8.2.4. Конфигурационный файл сервиса ocs-appstore-devconsole-ui (файл: /var/ocs/appstore/ocs-appstore-devconsole-ui/ocs-appstore-devconsole-ui.yml) .	174
8.3. Описание конфигурационных файлов ПУ	180
8.3.1. Общий конфигурационный файл ПУ (файл: /var/ocs/emm/config.yml)	180
8.3.2. Конфигурационный файл сервиса ocs-emm-adminconcole-ui (файл: /var/ocs/emm/ocs-emm-adminconsole-ui/ocs-emm-adminconsole-ui.yml)	188
8.3.3. Конфигурационный файл сервиса ocs-emm-applications-api (файл: /var/ocs/emm/ocs-emm-applications-api/ocs-emm-applications-api.yml).....	192
8.3.4. Конфигурационный файл сервиса ocs-emm-devices-api (файл: /var/ocs/emm/ocs-emm-devices-api/ocs-emm-devices-api.yml)	193

8.3.5. Конфигурационный файл сервиса ocs-emm-dispatcher-api (файл: /var/ocs/emm/ocs-emm-dispatcher-api/ocs-emm-dispatcher-api.yml)	194
8.3.6. Конфигурационный файл сервиса ocs-emm-enrollments-api (файл: /var/ocs/emm/ocs-emm-enrollments-api/ocs-emm-enrollments-api.yml)	196
8.3.7. Конфигурационный файл сервиса ocs-emm-policies-api (файл: /var/ocs/emm/ocs-emm-policies-api/ocs-emm-policies-api.yml)	197
8.3.8. Конфигурационный файл сервиса ocs-emm-reports-api (файл: /var/ocs/emm/ocs-emm-reports-api/ocs-emm-reports-api.yml).....	199
8.3.9. Конфигурационный файл сервиса ocs-emm-state-manager-api (файл: /var/ocs/emm/ocs-emm-state-manager-api/ocs-emm-state-manager-api.yml)	200
8.3.10. Конфигурационный файл сервиса ocs-emm-users-api (файл: /var/ocs/emm/ocs-emm-users-api/ocs-emm-users-api.yml)	201
8.3.11. Конфигурационный файл сервиса ocs-emm-journal-api (файл: /var/ocs/emm/ocs-emm-journal-api/ocs-emm-journal-api.yml).....	203
8.4. Описание конфигурационных файлов ПУСП.....	204
8.4.1. Общий конфигурационный файл ПУСП (файл: /var/ocs/pkgrepo/config.yml).....	204
8.4.2. Конфигурационный файл сервиса pkgrepo (файл: /var/ocs/pkgrepo/ocs-pkgrepo-pkg-repo-api/ocs-pkgrepo-pkg-repo-api.yml)	206
9. Сообщения об ошибках	208
Перечень терминов и сокращений	210

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1. Назначение и состав ППО

ППО предназначено для управления мобильными устройствами (МУ) под управлением защищенной мобильной операционной системы общего назначения на базе Sailfish Mobile OS RUS, имеющей действительный сертификат соответствия ФСТЭК России, и/или операционной системы (ОС) Аврора, имеющей действительный сертификат соответствия ФСТЭК России, (далее — ЗМОС) и управления жизненным циклом приложений, а также для автоматизированной обработки следующих видов информации:

- общедоступная информация;
- информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну, подлежащая защите в соответствии с требованиями действующего законодательства Российской Федерации в области информационной безопасности.

ППО является прикладным программным обеспечением со встроенными механизмами защиты информации от несанкционированного доступа. ППО предназначено для использования:

- в государственных информационных системах, не содержащих информации, составляющей государственной тайны, до 1 класса защищенности включительно в соответствии с документом «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденным приказом ФСТЭК России от 11 февраля 2013 г. № 17;

– в информационных системах персональных данных до 1 уровня защищенности включительно в соответствии с документом «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18 февраля 2013 г. № 21;

– в автоматизированных системах управления до 1 класса защищенности включительно в соответствии с документом «Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», утвержденным приказом ФСТЭК России от 14 августа 2014 г. № 31.

ППО состоит из следующих подсистем:

- подсистема безопасности (ПБ);
- подсистема «Маркет» (ПМ);
- подсистема Платформа управления (ПУ);
- подсистема установки системных пакетов (ПУСП).

Взаимодействие между подсистемами и компонентами подсистем осуществляется с использованием протокола HTTP стандарт RFC 2616, при этом обмен данными осуществляется в формате RFC 8259 (JSON).

В качестве сервера базы данных (БД) используется сервер с установленной системой управления базами данных (СУБД) Postgres Pro, PostgreSQL 10.4 или PostgreSQL 11.2, в которой хранятся данные ППО, для чего при развертывании создается специальная БД. Для хранения информации о сессиях используется СУБД Redis.

1.2. Субъекты доступа и права на доступ к интерфейсам ППО

1.2.1. Субъекты доступа (роли) ППО

Субъектами доступа должны являться пользователи и МП «Аврора Центр» (процесс МП «Аврора Центр») ППО. Субъекту доступа может быть назначена одна или несколько из следующих перечисленных ролей:

- роль МП «Аврора Центр» - роль назначается учетным записям МП «Аврора Центр» (сервис/процесс без участия пользователей, который управляет МУ);
- роль Администратора учетных записей позволяет осуществлять управление учетными записями;
- роль Оператора аудита позволяет осуществлять действия по работе с журналом регистрации событий ППО;
- роль Администратора Платформы Управления позволяет осуществлять все действия по управлению ПУ через интерфейс ППО;
- роль Администратора Аврора Маркет позволяет осуществлять все действия по управлению ПМ через интерфейс ППО;
- роль Разработчика позволяет осуществлять добавление новых и обновление ранее загруженных приложений в ПМ, а также получать информацию о приложениях;
- роль Пользователя Аврора Маркет позволяет осуществлять загрузку приложений из ПМ, а также получать информацию о приложениях.

В ППО в обязательном порядке должна присутствовать предустановленная учетная запись пользователя admin с ролью Администратора учетных записей

1.2.2. Права на доступ к интерфейсам ППО

Описание назначения разделов интерфейса ППО приведено далее в таблице (Таблица 1).

Таблица 1

Раздел	Подраздел	Подсистема	Наименование консоли / Права на доступ у роли
Мониторинг	Индикаторы	ПУ	Консоль администратора ПУ Администратор Платформы Управления
	Аудит	ПБ	Консоли администратора ПБ Права на доступ: Оператор аудита
Управление	Устройства	ПУ	Консоль администратора ПУ Администратор Платформы Управления
	Пользователи	ПУ	Консоль администратора ПУ Администратор Платформы Управления
	Политики	ПУ	Консоль администратора ПУ Администратор Платформы Управления
	Приложения	ПМ	Консоль администратора ПМ Администратор Аврора Маркет
	Витрины	ПМ	Консоль администратора ПМ Администратор Аврора Маркет
Администрирование	Учетные записи	ПБ	Консоль администратора ПБ Администратор учетных записей
	Настройки	ПУ	Консоль администратора ПУ Администратор Платформы Управления
	Орг. структура	ПУ	Консоль администратора ПУ Администратор Платформы Управления
Консоль разработчика ПМ		ПМ	Консоль разработчика ПМ Разработчик
МП «Аврора Маркет»		ПМ	Пользователь Аврора Маркет
МП «Аврора Центр»		ПУ	Сервис/процесс МП «Аврора Центр»

Состав разделов/подразделов интерфейса ППО может отличаться. Интерфейс верхней панели зависит от варианта поставки ППО

1.3. Назначение и состав ПБ

В ПБ реализованы функции безопасности ППО.

ПБ предназначена для:

- идентификации и аутентификацию пользователей МУ;
- управления идентификаторами пользователей и МУ;
- управления средствами аутентификации;
- управления учетными записями пользователей и МУ;
- ролевого управления доступом субъектов доступа к объектам доступа;
- регистрации событий безопасности;
- предоставления интерфейса пользователям ПБ.

ПБ состоит из следующих компонентов:

- Консоль администратора ПБ;
- Консоль входа пользователей;
- Сервер приложений ПБ.

С помощью Консоли администратора ПБ осуществляется управление учетными записями пользователей ППО и работа с журналом регистрации событий. Работа с Консолью администратора ПБ осуществляется пользователями с ролью Администратор учетных записей и Оператор аудита. Подробное описание функциональных действий с Консолью администратора ПБ приведено в разделе 2 настоящего документа.

С помощью Консоли входа пользователей осуществляется ввод идентификационной и аутентификационной информации пользователями ППО. Работа с Консолью входа пользователей осуществляется пользователем с ролью Оператор аудита. Подробное описание функциональных действий с Консолью входа пользователей приведено в подразделе 3.2 настоящего документа.

Сервер приложений ПБ представляет собой совокупность веб-приложений, реализующих функции безопасности, а также позволяющих хранить в БД и предоставлять субъектам доступа ППО доступ к данным об учетных записях пользователей и журналу регистрации событий.

1.4. Описание принципов безопасной работы средства

1.4.1. Общая информация

ППО реализует следующие функции безопасности:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- регистрация событий безопасности.

При использовании ППО должны выполняться следующие меры по защите информации от несанкционированного доступа к информации:

- необходимо соблюдать парольную политику;
- пароль не должен включать в себя легко вычисляемые сочетания символов;
- личный пароль пользователь не имеет права сообщать никому;
- при вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

При эксплуатации ППО запрещено:

- оставлять без контроля не заблокированные программные средства и/или ППО;
- разглашать пароли, выводить пароли на дисплей, принтер или иные средства отображения информации.

1.4.2. Компрометация паролей

Под компрометацией паролей следует понимать следующее:

- физическую утерю носителя с парольной информацией;
- передачу идентификационной информации по открытым каналам связи;
- перехват пароля при распределении идентификаторов;
- сознательную передачу информации постороннему лицу.

При компрометации пароля пользователь обязан незамедлительно оповестить Администратора учетных записей.

1.4.3. Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасные значения

Настройки (параметры) безопасности ППО доступны только пользователям с ролью Администратор учетных записей и заключаются в возможности управления ролями пользователей ППО.

Пользователям должны назначаться минимальные права и привилегии, необходимые для выполнения ими своих должностных обязанностей (функций).

1.4.4. Лицензионное соглашение

Перед использованием ППО пользователю необходимо ознакомиться с условиями Лицензионного соглашения, доступного к просмотру в нижнем левом углу каждого из подразделов интерфейса ППО (Рисунок 1). При нажатии на активную ссылку «Лицензионное соглашение» отобразится текст Лицензионного соглашения.

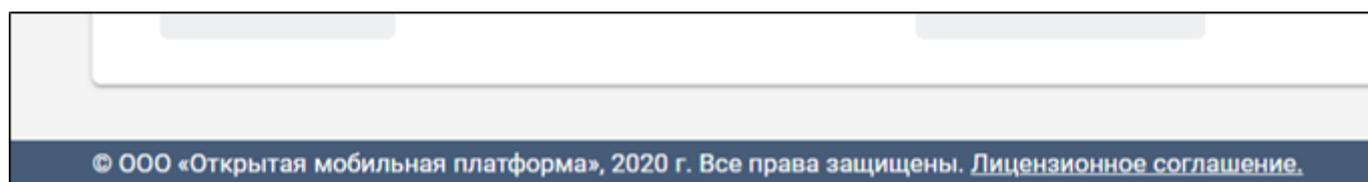


Рисунок 1

Любое использование пользователем ППО означает полное и безоговорочное принятие пользователем условий Лицензионного соглашения.

1.5. Условия выполнения

Для функционирования ППО необходимы следующие программно-технические средства.

В таблице (Таблица 2) приведены аппаратно-программные характеристики сервера приложений ППО.

Таблица 2

Параметр	Значение
Минимальные аппаратные характеристики¹	
Процессор	2 ядра
Объем оперативной памяти	не менее 4 Гб
Свободное место на жестком диске	не менее 10 Гб
Рекомендуемые характеристики	
Процессор	не ниже Intel® Xeon, с частотой 2,00 ГГц, 6 ядер
Объем оперативной памяти	не менее 12 Гб
Свободное место на жестком диске	не менее 150 Гб
Программные характеристики	
Операционная система	Одна из следующих ОС: – CentOS версии 7 или выше; – Альт 8 СП ²
Балансировщик микросервисов	Nginx Web Server версии 1.10 или выше
Система обнаружения сервисов	Consul версии 1.6 или выше
Средство управления конфигурациями микросервисов	Consul Template версии 0.20 или выше

¹ Для пилотных проектов, до 20 МУ.

² Альт 8 СП (сертификат соответствия ФСТЭК России № 3866, действителен до 10 августа 2023 г.).

Параметр	Значение
Сервис гарантированной доставки сообщений	Nats Streaming Server версии 0.16.2 или выше
Прикладное программное обеспечение	ППО «Аврора Центр»

В таблице (Таблица 3) приведены аппаратно-программные характеристики серверов БД.

Таблица 3

Параметр	Значение
Минимальные аппаратные характеристики³	
Процессор	2 ядра
Объем оперативной памяти	не менее 2 Гб
Свободное место на жестком диске	не менее 10 Гб
Рекомендуемые характеристики	
Процессор	не ниже Intel® Xeon, с частотой 2,00 ГГц, 12 ядер
Объем оперативной памяти	не менее 32 Гб
Свободное место на жестком диске	не менее 500 Гб
Программные характеристики	
Операционная система	Одна из следующих ОС: – CentOS версии 7 или выше; – Альт 8 СП ⁴

³ Для пилотных проектов, до 20 МУ.

⁴ Альт 8 СП (сертификат соответствия ФСТЭК России № 3866, действителен до 10 августа 2023 г.)

Параметр	Значение
СУБД	Одна из следующих СУБД: – Postgres Pro ⁵ ; – PostgreSQL 10.4 или выше (для ОС Альт 8 СП); – PostgreSQL 11.2 или выше (для ОС CentOS)
СУБД для хранения сессий	Redis 3.2.12 или выше
Расширение СУБД PostgreSQL для партиционирования таблиц БД	pg_partman 4 или выше
Расширение СУБД PostgreSQL поддерживающее быстрый поиск схожих строк	pg_trgm

В таблице (Таблица 4) приведены программные характеристики МУ.

Таблица 4

Параметр	Значение
Операционная система	Одна из следующих ОС: – защищенная мобильная ОС общего назначения на базе Sailfish Mobile OS RUS, имеющая действительный сертификат соответствия ФСТЭК России; – ОС Аврора, имеющая действительный сертификат соответствия ФСТЭК России
Прикладное программное обеспечение	– МП «Аврора Центр»; – МП «Аврора Маркет»

⁵ СУБД «Postgres Pro» (сертификат соответствия ФСТЭК России № 3637, действителен до 05 октября 2019 г., техническая поддержка до 05.10.2029 г.)

Для работы пользователей с веб-интерфейсом серверов приложений ППО должны использоваться веб-браузеры поддерживающие технологии: TLS, CSS3, HTML5, ECMAScript 5 и Cookie.

Варианты конфигурации среды функционирования, в которых проводилось тестирование ППО приведены в таблице (Таблица 5).

Таблица 5

ОС	СУБД	СЗИ НСД
Сервер приложений		
CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64		СЗИ НСД «Dallas Lock Linux» ⁶
CentOS-7.5.1804, kernel: 3.10.0-862.11.6.el7.x86_64		Специальное программное обеспечение (СПО) СЗИ НСД «Аккорд-Х К» ⁷
CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64		СЗИ «Secret Net LSP» ⁸
Альт 8 СП		
Сервер БД/сервер БД и сервер приложений		
CentOS-7.5.1804, kernel: 3.10.0-862.11.6.el7.x86_64	PostgreSQL 11.5	СПО СЗИ НСД «Аккорд-Х К»
CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64	PostgreSQL 11.5	СЗИ НСД «Dallas Lock Linux»
CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64	PostgreSQL 11.5	СЗИ «Secret Net LSP»
Альт 8 СП	Postgres Pro	
Альт 8 СП	PostgreSQL 10.4	

⁶ СЗИ НСД «Dallas Lock Linux» (сертификат соответствия ФСТЭК России № 3594, действителен до 04 июля 2024 г.).

⁷ СПО СЗИ НСД «Аккорд-Х К» (сертификат соответствия ФСТЭК России № 3760, действителен до 04 июля 2020 г., техническая поддержка до 31.01.2025 г.).

⁸ СЗИ «Secret Net LSP» (сертификат соответствия ФСТЭК России № 2790, действителен до 18 декабря 2023 г.).

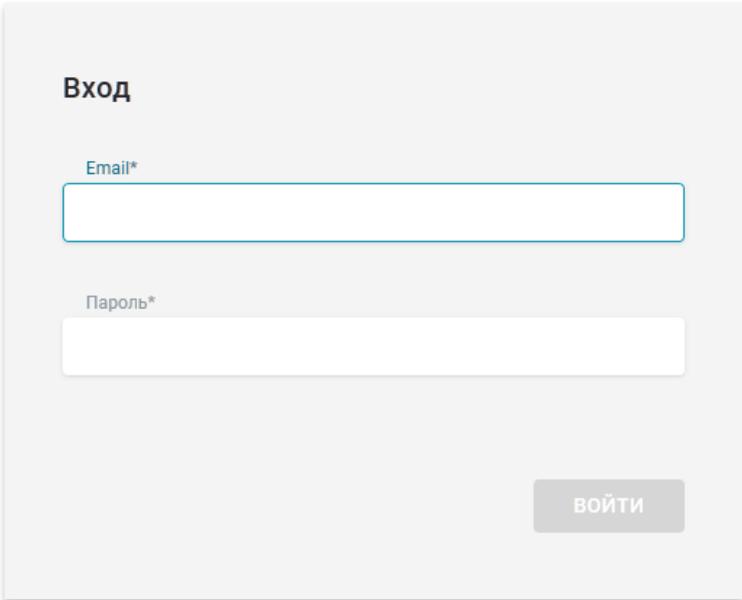
2. ПОДГОТОВКА К РАБОТЕ

2.1. Начало сеанса работы

Для аутентификации в Консоли администратора ПБ необходимо выполнить следующие действия:

- в веб-браузере перейти по адресу Консоли администратора ПБ;
- в Консоли входа пользователей выполнить следующее:
 - заполнить поля «Email» и «Пароль»;
 - нажать кнопку «Войти» (Рисунок 2).

Учетная запись пользователя с ролью Администратор учетных записей создается при установке ПБ с логином «admin@omprussia.ru» и паролем «admin»



The image shows a login form with the following elements:

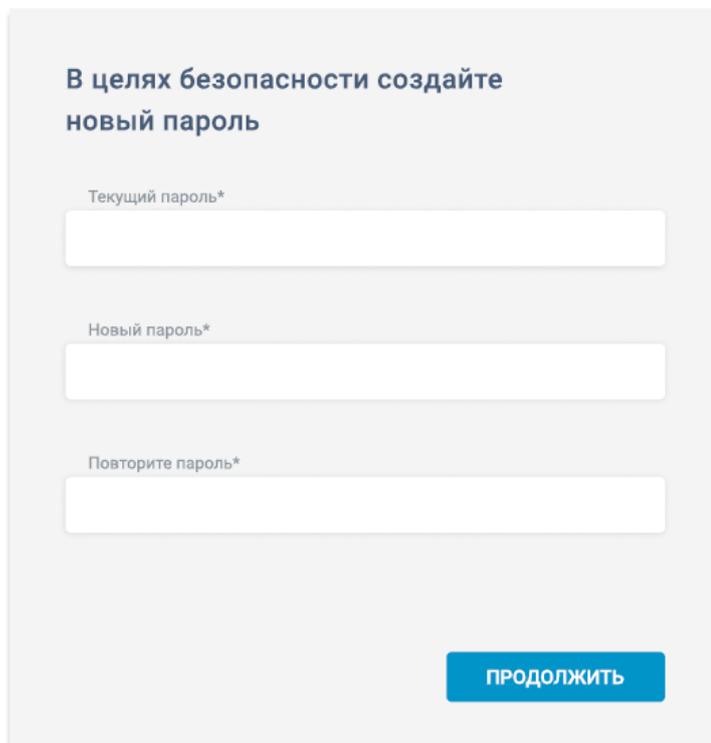
- Title: **Вход**
- Label: Email*
- Input field: A rectangular text box for entering the email address.
- Label: Пароль*
- Input field: A rectangular text box for entering the password.
- Button: A button labeled **ВОЙТИ** (Login).

Рисунок 2

При первом входе пользователю ПБ будет предложено в целях безопасности сменить пароль. Для этого в открывшемся окне необходимо выполнить следующие действия:

- ввести текущий пароль;
- ввести новый пароль;
- повторно ввести новый пароль;

– нажать кнопку «Продолжить» (Рисунок 3).



**В целях безопасности создайте
новый пароль**

Текущий пароль*

Новый пароль*

Повторите пароль*

ПРОДОЛЖИТЬ

Рисунок 3

Новый пароль должен содержать:

- от 8 до 255 символов;
- заглавные буквы;
- строчные буквы;
- цифры;
- спецсимволы.

1. Срок действия установленного пароля составляет 60 дней. По истечении срока действия необходимо сменить пароль. Откроется соответствующее окно (см. Рисунок 3). Смена устаревшего пароля выполняется аналогично смене пароля при первом входе

2. Новый пароль должен отличаться от трех ранее вводимых паролей

По умолчанию для каждого пользователя возможно не более двух параллельных (одновременных) сессий доступа.

При превышении допустимого количества сессий отобразится окно с информационным сообщением (Рисунок 4).

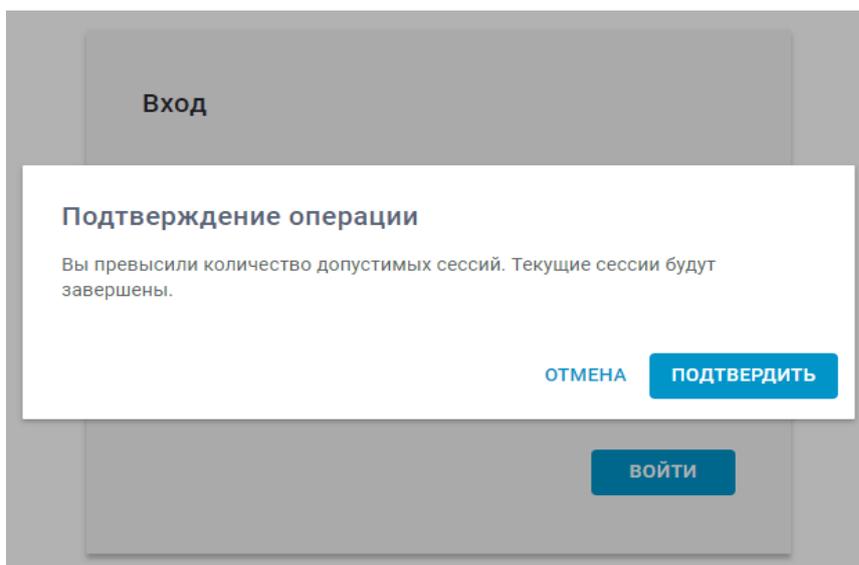


Рисунок 4

При нажатии кнопки «Подтвердить» все текущие сессии будут завершены, выполнится вход в Консоль администратора ПБ и отобразится главная страница.

При нажатии кнопки «Отмена» текущие сессии останутся активными, отобразится окно входа в Консоль администратора ПБ.

В случае изменения списка ролей пользователя необходимо выйти из системы, а затем заново пройти аутентификацию и войти в систему!

Если после входа пользователь был неактивен более пяти минут, произойдет автоматический выход из нее и отобразится страница аутентификации. Для продолжения работы необходимо выполнить процедуру входа в ПБ, введя на странице аутентификации данные в поля «Email» и «Пароль» и нажав кнопку «Войти» (см. Рисунок 2).

Если пользователь был неактивен в течение 45 дней, то его учетная запись блокируется.

2.2. Описание интерфейса

Интерфейс Консоли администратора ПБ делится на следующие части:

- верхняя панель;
- рабочая область;

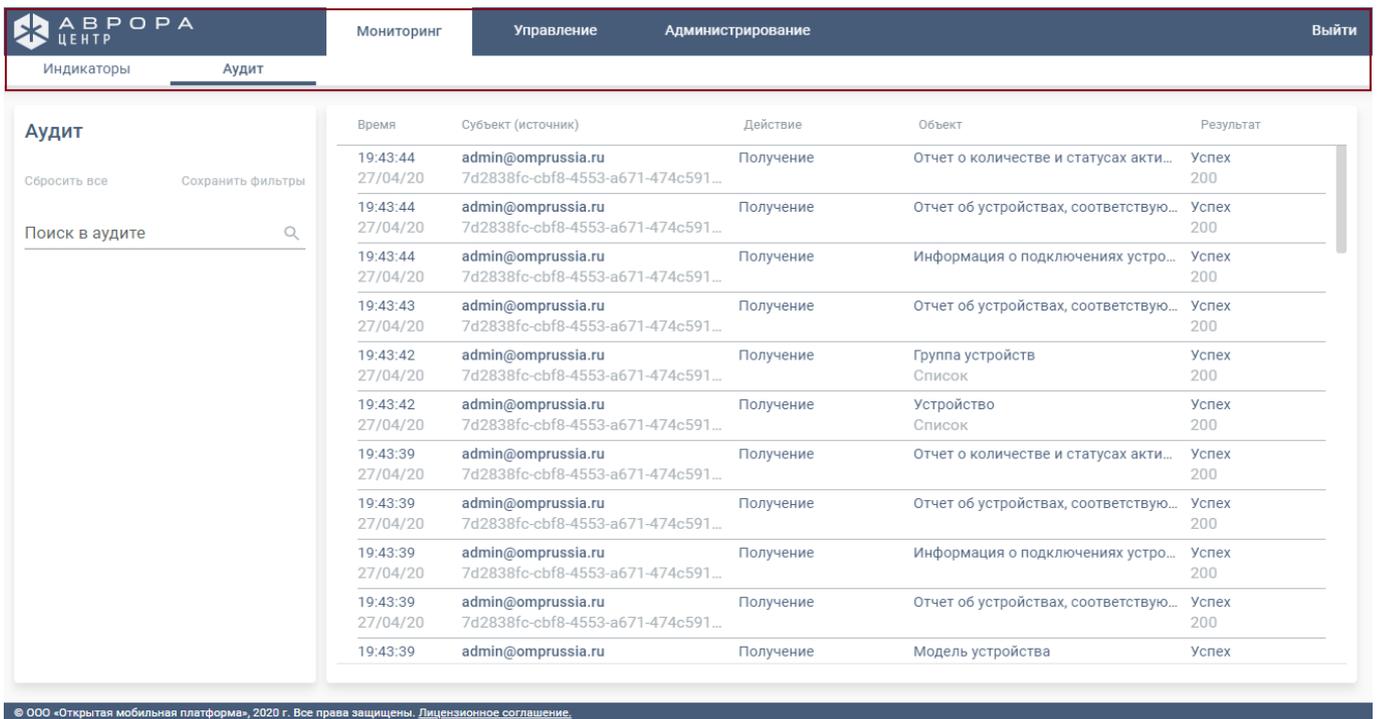
– область фильтров.

2.2.1. Верхняя панель

В верхней панели отображаются разделы и подразделы ППО (см. Таблица 2).

Верхняя панель ПБ состоит из следующих разделов:

- «Мониторинг». Включает подраздел «Аудит» (Рисунок 5);
- «Администрирование». Включает подраздел «Учетные записи» (Рисунок 6).



Время	Субъект (источник)	Действие	Объект	Результат
19:43:44 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет о количестве и статусах акти...	Успех 200
19:43:44 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет об устройствах, соответствую...	Успех 200
19:43:44 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Информация о подключениях устро...	Успех 200
19:43:43 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет об устройствах, соответствую...	Успех 200
19:43:42 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Группа устройств Список	Успех 200
19:43:42 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Устройство Список	Успех 200
19:43:39 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет о количестве и статусах акти...	Успех 200
19:43:39 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет об устройствах, соответствую...	Успех 200
19:43:39 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Информация о подключениях устро...	Успех 200
19:43:39 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет об устройствах, соответствую...	Успех 200
19:43:39	admin@omprussia.ru	Получение	Модель устройства	Успех

Рисунок 5

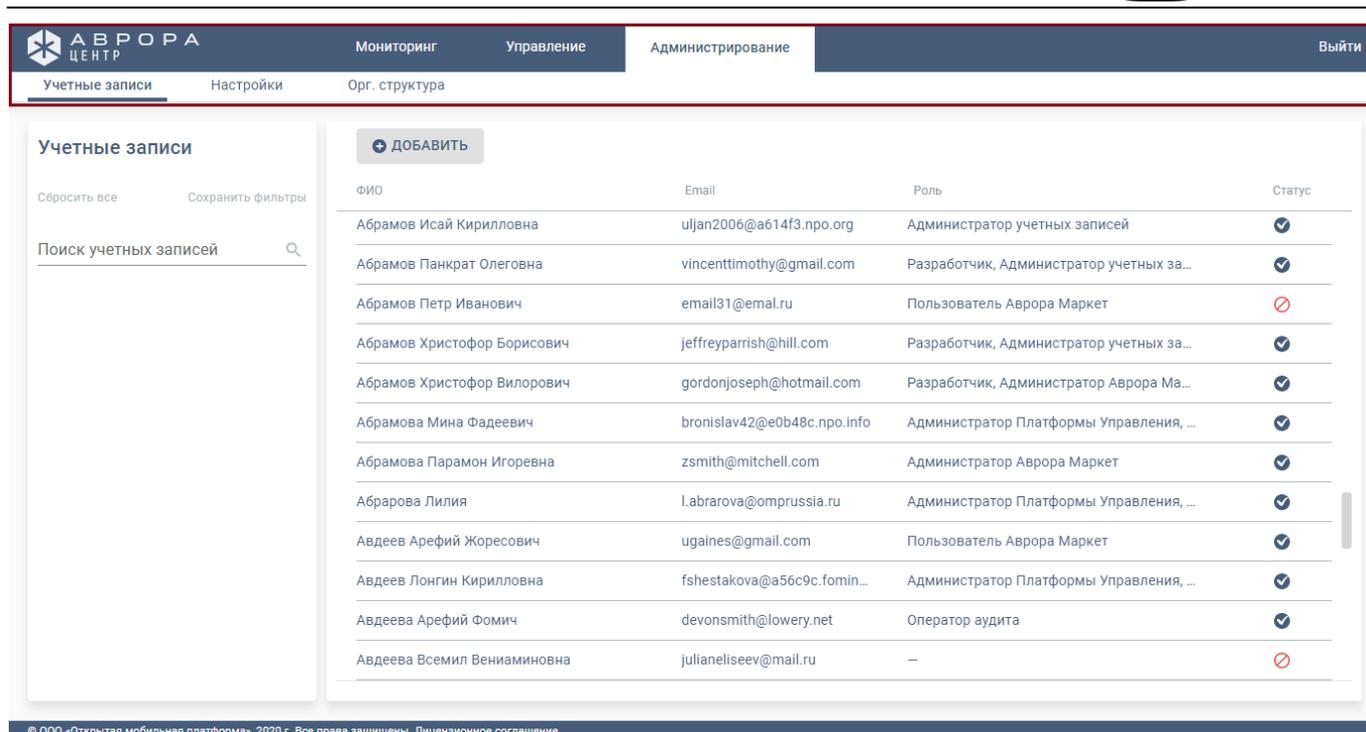


Рисунок 6

Работа в Консоли администратора ПБ осуществляется в подразделе «Учетные записи» раздела «Администрирование», а также в подразделе «Аудит» раздела «Мониторинг».

2.2.2. Рабочая область

В рабочей области ПБ осуществляется:

- создание учетных записей пользователей ППО и управления ими;
- просмотра событий аудита ППО.

Для упрощения взаимодействия с интерфейсом ПБ предусмотрены всплывающие подсказки. При наведении курсора на элемент отображается подсказка с информацией о назначении данного интерфейсного элемента (Рисунок 7).

Учетные записи

Сбросить все Сохранить фильтры

Поиск учетных записей

ФИО	Email	Роль	Статус
Абрамов Исай Кирилловна	uljan2006@a614f3.npo.org	Администратор учетных записей	✓
Абрамов Панкрат Олеговна	vincenttimothy@gmail.com	Разработчик, Администратор учетных записей, Оператор аудита, Администратор Платформы Управления, Пользователь Аврора Маркет	✓
Абрамов Петр Иванович	email31@emal.ru	Пользователь Аврора Маркет	✗
Абрамов Христофор Борисович	jeffreyparrish@hill.com	Разработчик, Администратор учетных записей	✓
Абрамов Христофор Вилорович	gordonjoseph@hotmail.com	Разработчик, Администратор Аврора Ма...	✓
Абрамова Мина Фадеевич	bronslav42@e0b48c.npo.info	Администратор Платформы Управления, ...	✓
Абрамова Парамон Игоревна	zsmith@mitchell.com	Администратор Аврора Маркет	✓
Абларова Лилия	l.ablarova@omprussia.ru	Администратор Платформы Управления, ...	✓
Авдеев Арефий Жоресович	ugaines@gmail.com	Пользователь Аврора Маркет	✓
Авдеев Лонгин Кирилловна	fshetakova@a56c9c.fomin...	Администратор Платформы Управления, ...	✓
Авдеева Арефий Фомич	devonsmith@lowery.net	Оператор аудита	✓
Авдеева Всемир Вениаминовна	julianeliseev@mail.ru	—	✗

© ООО «Открытая мобильная платформа», 2020 г. Все права защищены. Лицензионное соглашение.

Рисунок 7

2.2.3. Область фильтров

С помощью области фильтров возможно выполнить поиск в следующих разделах:

- «Мониторинг», подраздел «Аудит». Поиск субъектов мониторинга (Рисунок 8);
- «Администрирование», подраздел «Учетные записи». Поиск по учетным записям пользователей (Рисунок 9).

АВРОПА ЦЕНТР
Мониторинг Управление Администрирование
Выйти

Аудит

Сбросить все Сохранить фильтры

Поиск в аудите

Субъект:

Время с:

Время по:

Время	Субъект (источник)	Действие	Объект	Результат
16:42:39 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Отчет об устройствах, соответствующих политике	Успех 200
16:42:39 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Информация о подключениях устройств	Успех 200
16:42:39 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Отчет о количестве и статусах активации устройств	Успех 200
16:42:39 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Отчет об устройствах, соответствующих политике	Успех 200
16:42:39 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Модель устройства Список	Успех 200
16:42:29 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Роль Список	Успех 200
16:42:28 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Учетная запись Список	Успех 200
16:41:56 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Отчет об устройствах, соответствующих политике	Успех 200
16:41:56 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Отчет о количестве и статусах активации устройств	Успех 200
16:41:56 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Информация о подключениях устройств	Успех 200
16:41:56 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Отчет об устройствах, соответствующих политике	Успех 200
16:41:56 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Модель устройства Список	Успех 200

© ООО «Открытая мобильная платформа», 2020 г. Все права защищены. Лицензионное соглашение.

Рисунок 8

АВРОПА ЦЕНТР
Мониторинг Управление Администрирование
Выйти

Учетные записи

Сбросить все Сохранить фильтры

Поиск учетных записей

Имя:

Фамилия:

Отчество:

Email:

Роль:

Статус:

+ ДОБАВИТЬ

ФИО	Email	Роль	Статус
Абрамов Исай Кирилловна	uljan2006@ab14f3.npo.org	Администратор учетных записей	✓
Абрамов Панкрат Олеговна	vincenttimothy@gmail.com	Разработчик, Администратор учетных за...	✓
Абрамов Петр Иванович	email31@email.ru	Пользователь Аврора Маркет	✗
Абрамов Христофор Борисович	jeffreyparrish@hill.com	Разработчик, Администратор учетных за...	✓
Абрамов Христофор Вилорович	gordonjoseph@hotmail.com	Разработчик, Администратор Аврора Ма...	✓
Абрамова Мина Фадеевич	bronslav42@e0b48c.npo.info	Администратор Платформы Управления, ...	✓
Абрамова Парамон Игоревна	zsmith@mitchell.com	Администратор Аврора Маркет	✓
Абларова Лилия	l.ablarova@omprussia.ru	Администратор Платформы Управления, ...	✓
Авдеев Арефий Жоресович	ugaines@gmail.com	Пользователь Аврора Маркет	✓
Авдеев Лонгин Кирилловна	fshestakova@a56c9c.fomin...	Администратор Платформы Управления, ...	✓
Авдеева Арефий Фомич	devonsmith@lowery.net	Оператор аудита	✓
Авдеева Всемирл Вениаминовна	julianeliseev@mail.ru	—	✗

© ООО «Открытая мобильная платформа», 2020 г. Все права защищены. Лицензионное соглашение.

Рисунок 9

В сводной таблице приведены фильтры для поиска информации по каждому из подразделов (Таблица 6).

Таблица 6

Раздел	Фильтр	Описание
Поиск субъектов мониторинга		
Мониторинг	Субъект	Поиск по адресу электронной почты. Ввод значения с клавиатуры
	Время с	Поиск по времени события за выбранный период.
	Время по	Выбор значения в календаре и на циферблате
Поиск по учетным записям пользователей		
Администрирование	Имя	Поиск по имени. Ввод значения с клавиатуры
	Фамилия	Поиск по фамилии. Ввод значения с клавиатуры
	Отчество	Поиск по отчеству. Ввод значения с клавиатуры
	Email	Поиск по адресу электронной почты. Ввод значения с клавиатуры
	Роль	Поиск по роли. Выбор значения из списка: <ul style="list-style-type: none"> – «Администратор учетных записей»; – «Пользователь Аврора Маркет»; – «Администратор Платформы Управления»; – «Разработчик»; – «Администратор Аврора Маркет»; – «Оператор аудита». Из списка можно выбрать только одну роль
	Статус	Поиск по статусу. Выбор значения из списка: <ul style="list-style-type: none"> – «Активен»; – «Заблокирован»

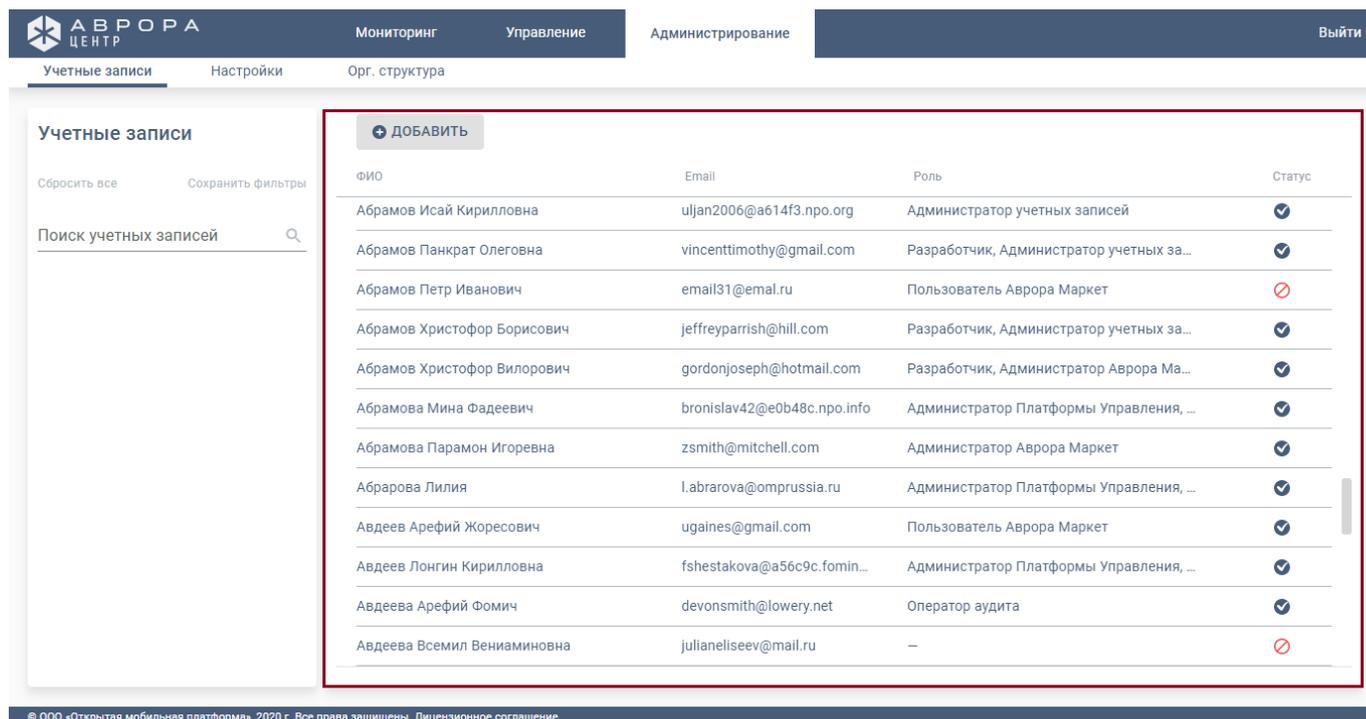
3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1. Консоль администратора ПБ. Раздел «Администрирование»

3.1.1. Работа в подразделе «Учетные записи»

В Консоли администратора ПБ в разделе «Администрирование» в подразделе «Учетные записи» отображается список учетных записей со следующей информацией (Рисунок 10):

- «ФИО»;
- «Email»;
- «Роль»;
- «Статус».



ФИО	Email	Роль	Статус
Абрамов Исая Кирилловна	uljan2006@a614f3.npo.org	Администратор учетных записей	✓
Абрамов Панкрат Олеговна	vincenttimothy@gmail.com	Разработчик, Администратор учетных за...	✓
Абрамов Петр Иванович	email31@emal.ru	Пользователь Аврора Маркет	✗
Абрамов Христофор Борисович	jeffreyparrish@hill.com	Разработчик, Администратор учетных за...	✓
Абрамов Христофор Вилорович	gordonjoseph@hotmail.com	Разработчик, Администратор Аврора Ма...	✓
Абрамова Мина Фадеевич	bronslav42@e0b48c.npo.info	Администратор Платформы Управления, ...	✓
Абрамова Парамон Игоревна	zsmith@mitchell.com	Администратор Аврора Маркет	✓
Абрарова Лилия	l.abrarova@omprussia.ru	Администратор Платформы Управления, ...	✓
Авдеев Арефий Жоресович	ugaines@gmail.com	Пользователь Аврора Маркет	✓
Авдеев Лонгин Кирилловна	fshestakova@a56c9c.fomin...	Администратор Платформы Управления, ...	✓
Авдеева Арефий Фомич	devonsmith@lowery.net	Оператор аудита	✓
Авдеева Всемир Вениаминовна	julianeliseev@mail.ru	—	✗

Рисунок 10

Возможные статусы учетных записей приведены в таблице (Таблица 7).

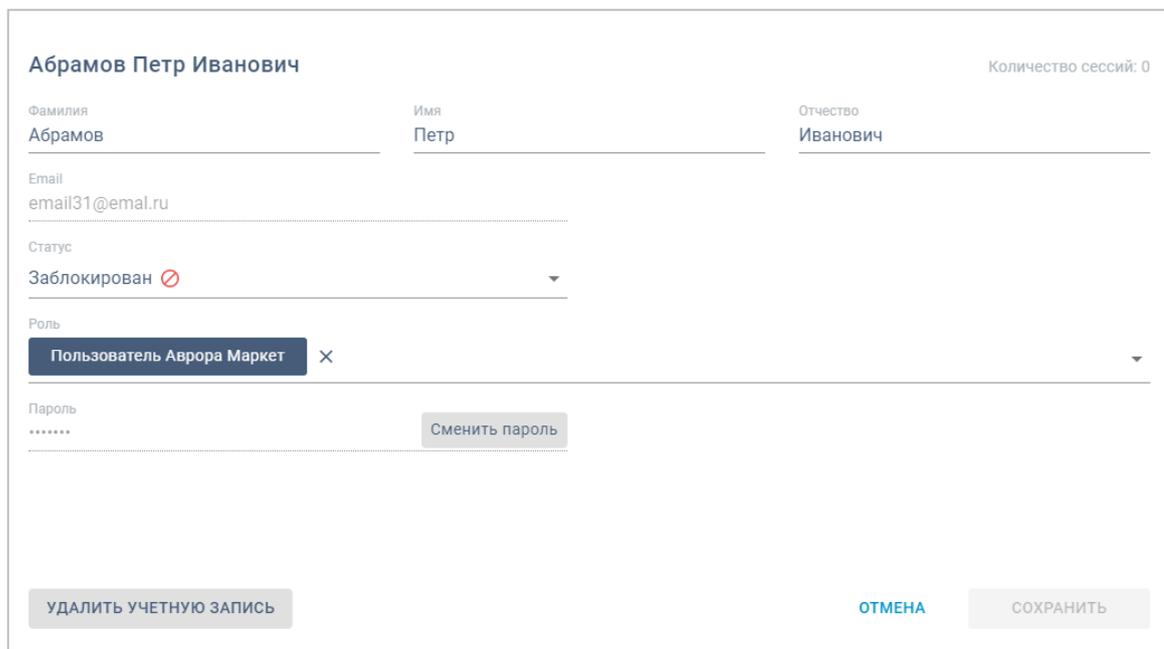
Таблица 7

Элемент	Наименование	Обозначение
	«Активен»	Учетная запись активна
	«Заблокирован»	Учетная запись заблокирована

Пользователи ППО могут иметь следующие роли:

- Администратор учетных записей;
- Пользователь Аврора Маркет;
- Администратор Платформы Управления;
- Разработчик;
- Администратор Аврора Маркет;
- Оператор аудита.

При нажатии на строку учетной записи пользователя ППО откроется карточка, в которой отображается количество активных сессий пользователя и основная информация (Рисунок 11).



Абрамов Петр Иванович Количество сессий: 0

Фамилия: Абрамов Имя: Петр Отчество: Иванович

Email: email31@emal.ru

Статус: **Заблокирован** 

Роль: **Пользователь Аврора Маркет** 

Пароль: Сменить пароль

УДАЛИТЬ УЧЕТНУЮ ЗАПИСЬ **ОТМЕНА** СОХРАНИТЬ

Рисунок 11

С помощью карточки учетной записи можно выполнить:

- редактирование данных учетной записи;
- смену пароля;
- удаление учетной записи.

Подробное описание приведено в пп. 3.1.1.2, 3.1.1.4, 3.1.1.5.

3.1.1.1. Создание учетной записи

Для создания учетной записи необходимо нажать кнопку «Добавить» (Рисунок 12).

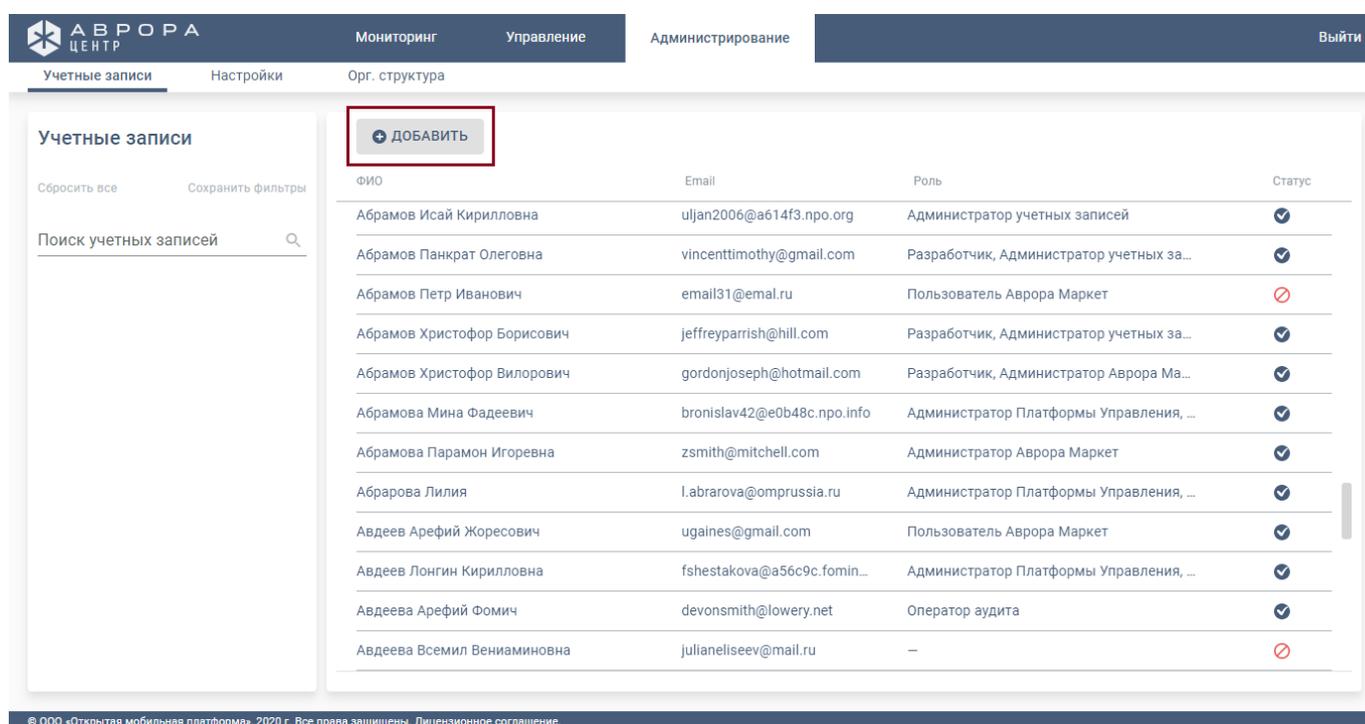


Рисунок 12

В открывшейся форме необходимо заполнить следующие поля (Рисунок 13):

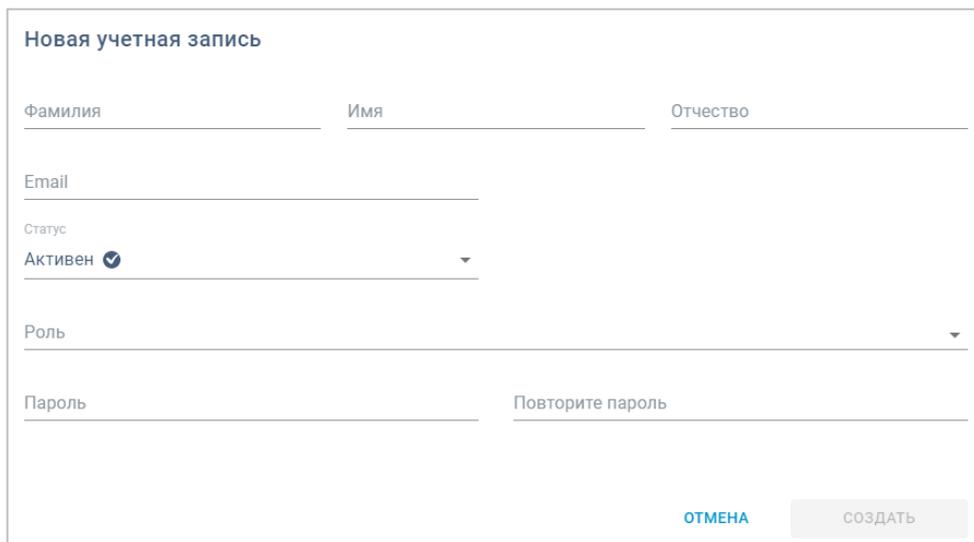
- «Фамилия» — ввести фамилию. Поля могут содержать до 255 символов;
- «Имя» — ввести имя. Поля могут содержать до 255;
- «Отчество» — ввести отчество. Поле может содержать до 255 символов;
- «Email» — ввести адрес электронной почты пользователя;
- «Статус» — выбрать из раскрывающегося списка статус учетной записи

пользователя;

– «Роль» — выбрать из раскрывающегося списка роль. Возможно назначение нескольких ролей;

– «Пароль», «Повторите пароль» — ввести и подтвердить пароль. Требования к сложности пароля приведены в подразделе 2.1 настоящего документа.

Поля «Фамилия», «Имя», «Email», «Пароль» и «Повторите пароль» обязательны для заполнения



Новая учетная запись

Фамилия _____ Имя _____ Отчество _____

Email _____

Статус
Активен

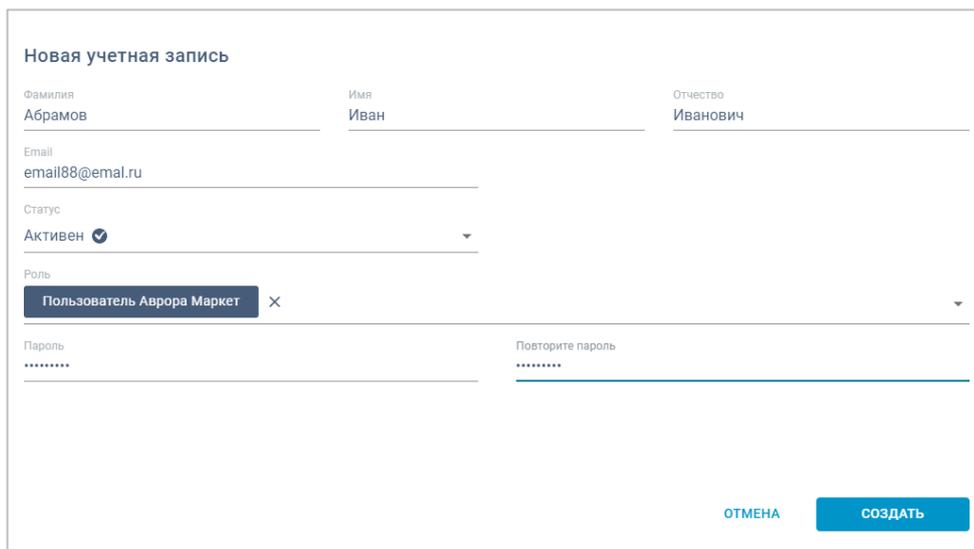
Роль _____

Пароль _____ Повторите пароль _____

ОТМЕНА СОЗДАТЬ

Рисунок 13

Для создания учетной записи необходимо нажать кнопку «Создать». Для отмены создания учетной записи необходимо нажать кнопку «Отмена» (Рисунок 14).



Новая учетная запись

Фамилия _____ Имя _____ Отчество _____
Абрамов Иван Иванович

Email _____
email88@emal.ru

Статус
Активен

Роль
Пользователь Аврора Маркет ×

Пароль _____ Повторите пароль _____
.....

ОТМЕНА СОЗДАТЬ

Рисунок 14

При успешном создании учетной записи отобразится сообщение «Учетная запись успешно создана». Добавленная учетная запись отобразится на странице «Учетные записи» в Консоли администратора ПБ. Сортировка осуществляется по ФИО пользователя в алфавитном порядке (Рисунок 15).

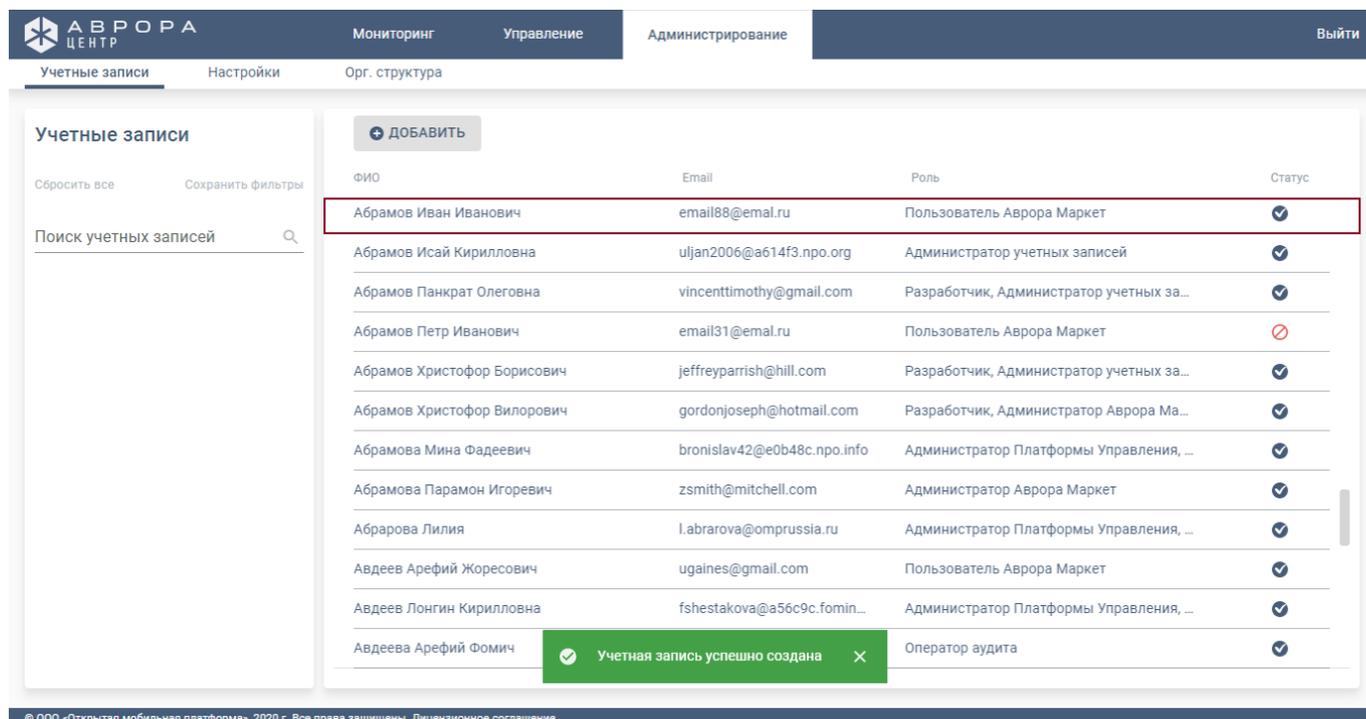


Рисунок 15

3.1.1.2. Редактирование данных учетной записи

Для редактирования данных учетной записи необходимо выполнить следующие действия:

- нажать на строку учетной записи (Рисунок 16);

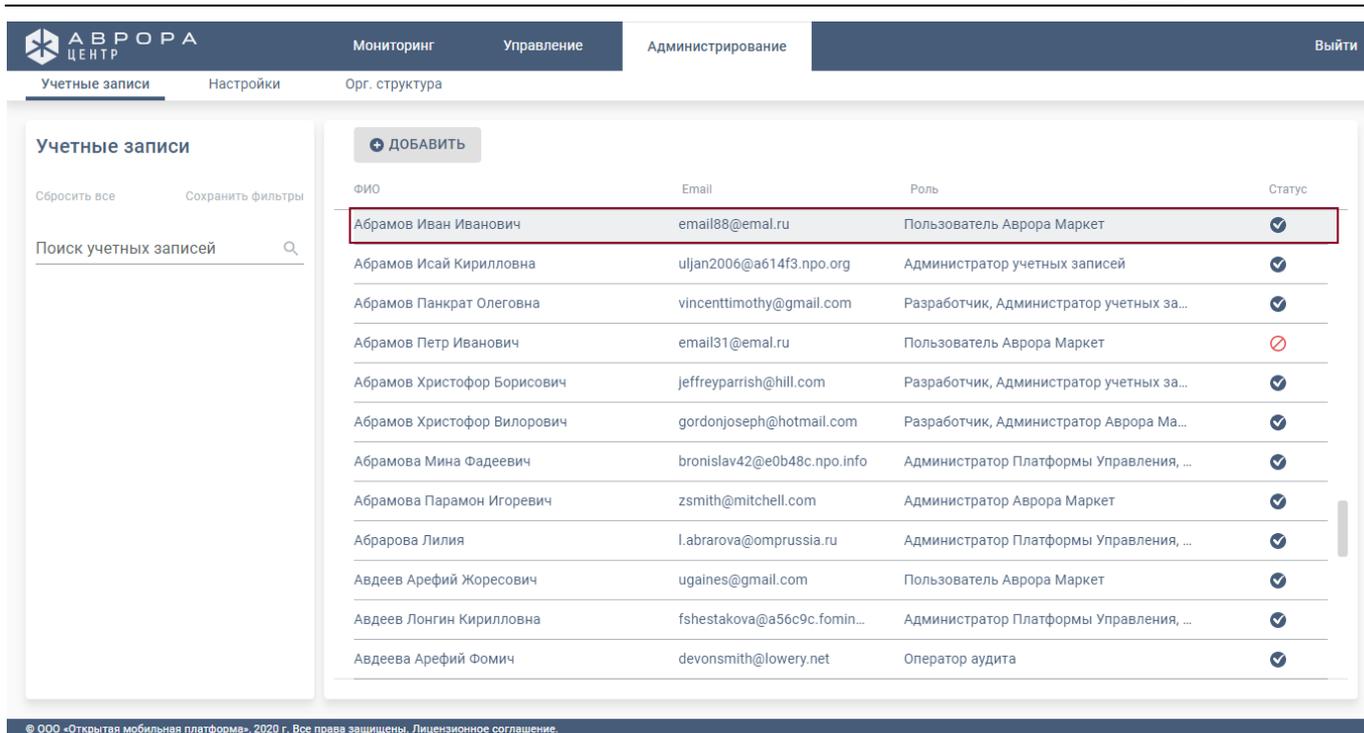
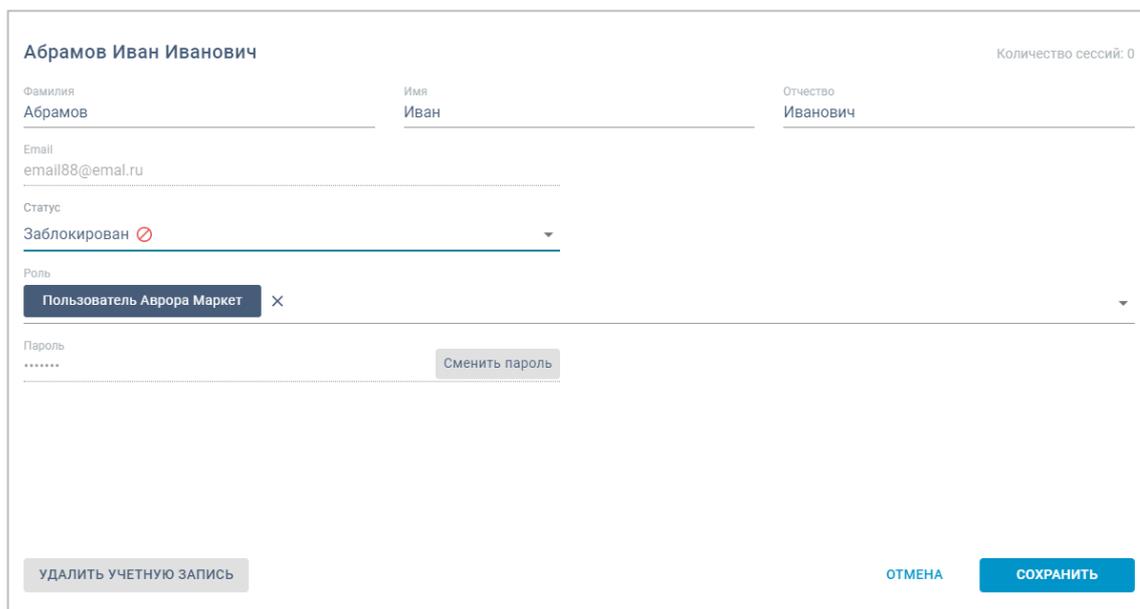


Рисунок 16

- в открывшейся форме внести необходимые изменения;
- нажать кнопку «Сохранить». Для отмены редактирования нажать кнопку «Отмена» (Рисунок 17);



Скриншот формы редактирования учетной записи «Абрамов Иван Иванович». В правом верхнем углу — «Количество сессий: 0». Поля: «Фамилия» (Абрамов), «Имя» (Иван), «Отчество» (Иванович), «Email» (email88@emal.ru), «Статус» (Заблокирован ✗), «Роль» (Пользователь Аврора Маркет ✗), «Пароль» (.....) с кнопкой «Сменить пароль». Внизу — кнопки «УДАЛИТЬ УЧЕТНУЮ ЗАПИСЬ», «ОТМЕНА», «СОХРАНИТЬ».

Рисунок 17

Поле «Email» недоступно для изменения

При успешном редактировании данных учетной записи отобразится сообщение «Учетная запись успешно обновлена» (Рисунок 18).

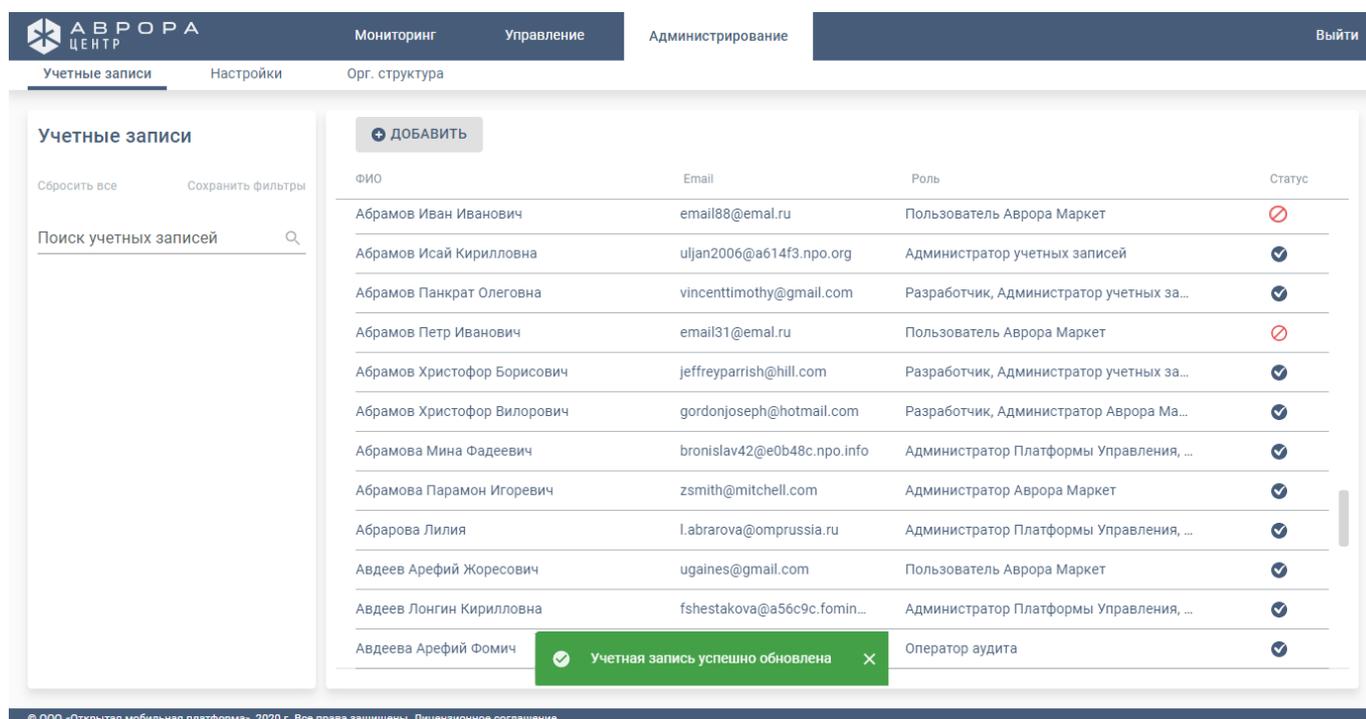


Рисунок 18

3.1.1.3. Работа с фильтрами

В Консоли администратора ПБ в области фильтров предусмотрена возможность поиска по заданным критериям.

Для поиска необходимо выполнить следующие действия (Рисунок 19):

- установить курсор в поле поиска;
- выбрать один из фильтров для поиска;
- ввести поисковый запрос;
- нажать на значок , для очистки поля нажать на значок .

Минимальная длина поискового запроса — три символа

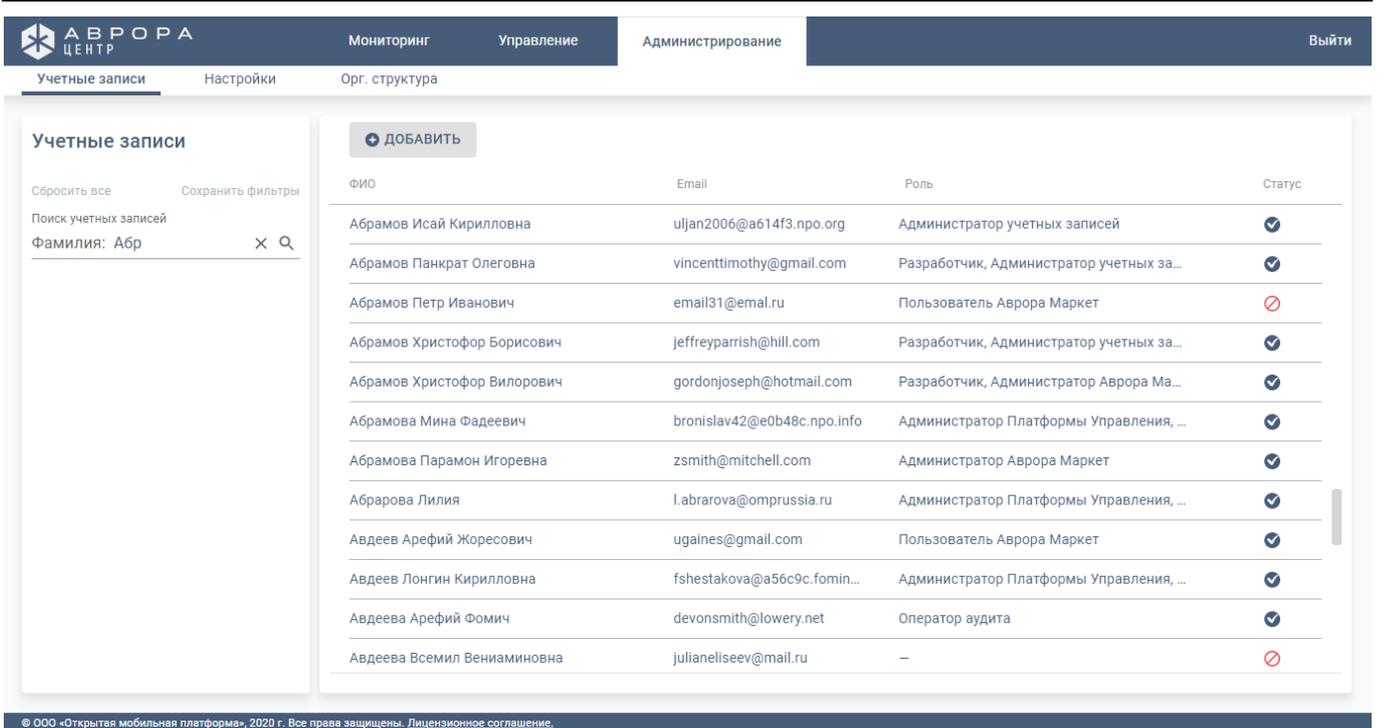


Рисунок 19

В результате выполнится поиск по выбранному фильтру (Рисунок 20).

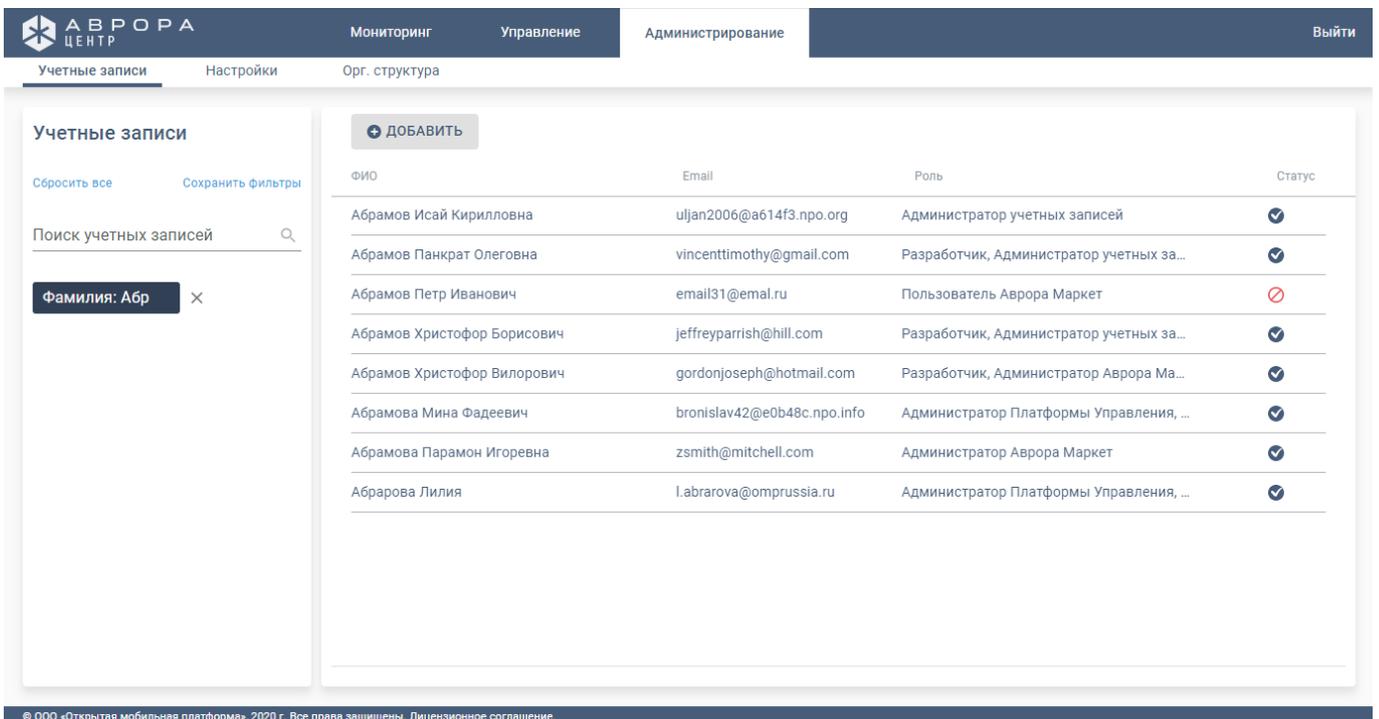
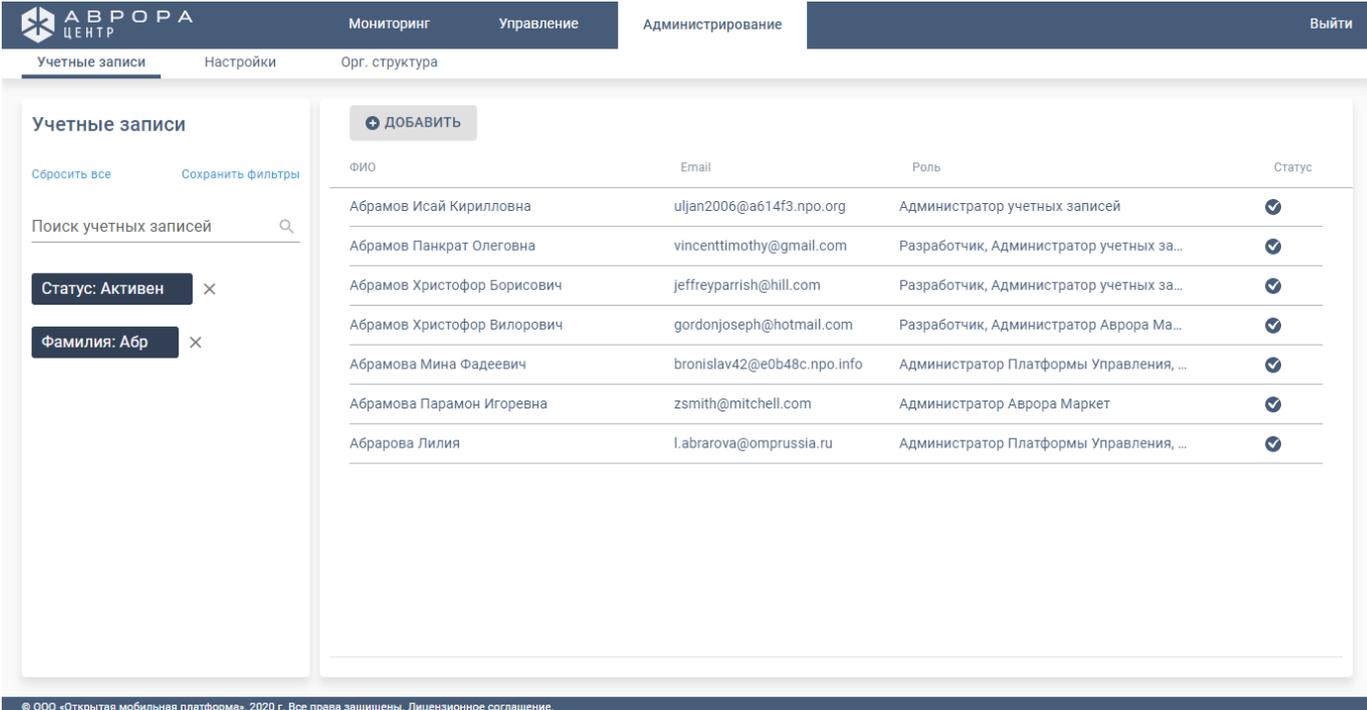


Рисунок 20

Для формирования детальной выборки можно комбинировать разные фильтры. Для этого необходимо добавить к текущим фильтрам дополнительный. Добавление производится в соответствии с описанием поиска выше.

В рабочей области отобразится перечень, сформированный с применением разных фильтров (Рисунок 21).



Учетные записи

Сбросить все Сохранить фильтры

Поиск учетных записей

Статус: Активен ×

Фамилия: Абр ×

ДОБАВИТЬ

ФИО	Email	Роль	Статус
Абрамов Исая Кирилловна	uljan2006@a614f3.npo.org	Администратор учетных записей	✓
Абрамов Панкрат Олеговна	vincenttimothy@gmail.com	Разработчик, Администратор учетных за...	✓
Абрамов Христофор Борисович	jeffreyparrish@hill.com	Разработчик, Администратор учетных за...	✓
Абрамов Христофор Вилорович	gordonjoseph@hotmail.com	Разработчик, Администратор Аврора Ма...	✓
Абрамова Мина Фадеевич	bronislav42@e0b48c.npo.info	Администратор Платформы Управления, ...	✓
Абрамова Парамон Игоревна	zsmith@mitchell.com	Администратор Аврора Маркет	✓
Абрарова Лилия	l.abrarova@omprussia.ru	Администратор Платформы Управления, ...	✓

© ООО «Открытая мобильная платформа», 2020 г. Все права защищены. Лицензионное соглашение.

Рисунок 21

Примененные фильтры можно сохранить в набор, выполнив следующие действия:

- нажать «Сохранить фильтры» (Рисунок 22);

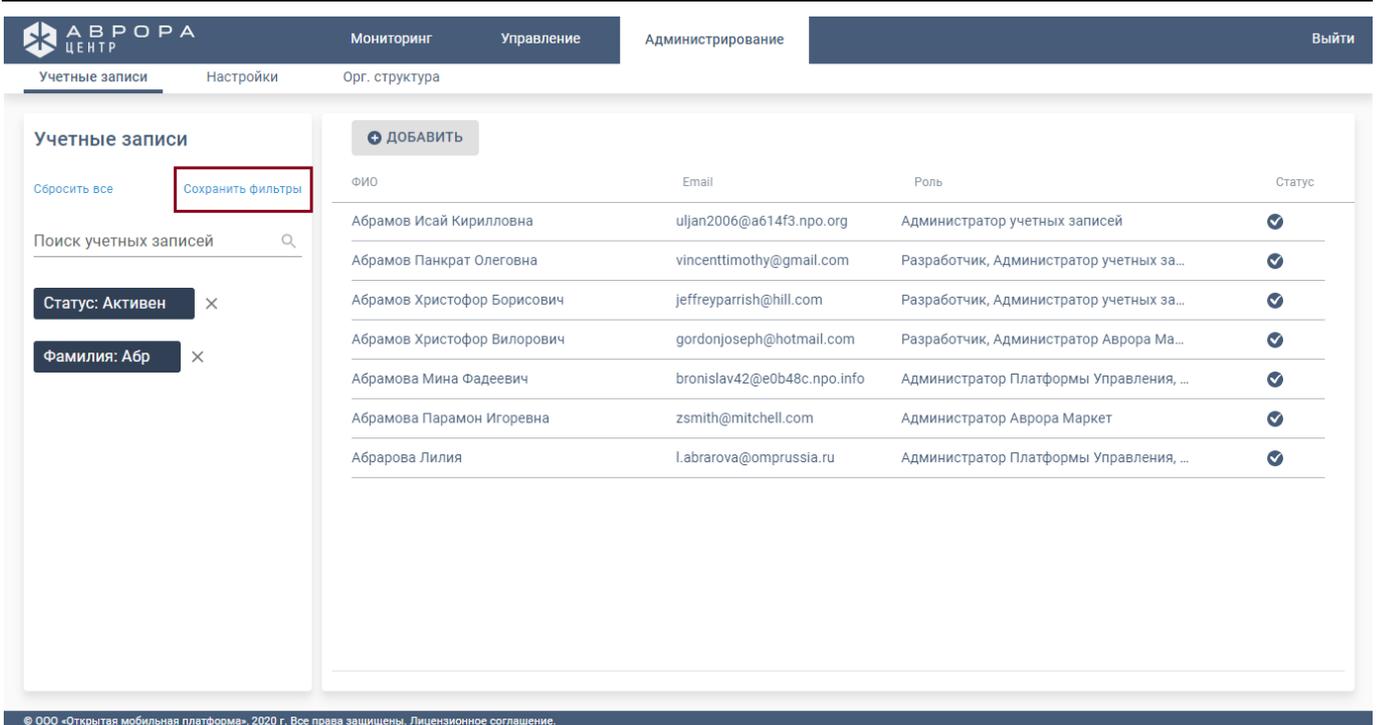


Рисунок 22

- ввести имя набора фильтров;
- нажать «Сохранить» (Рисунок 23).

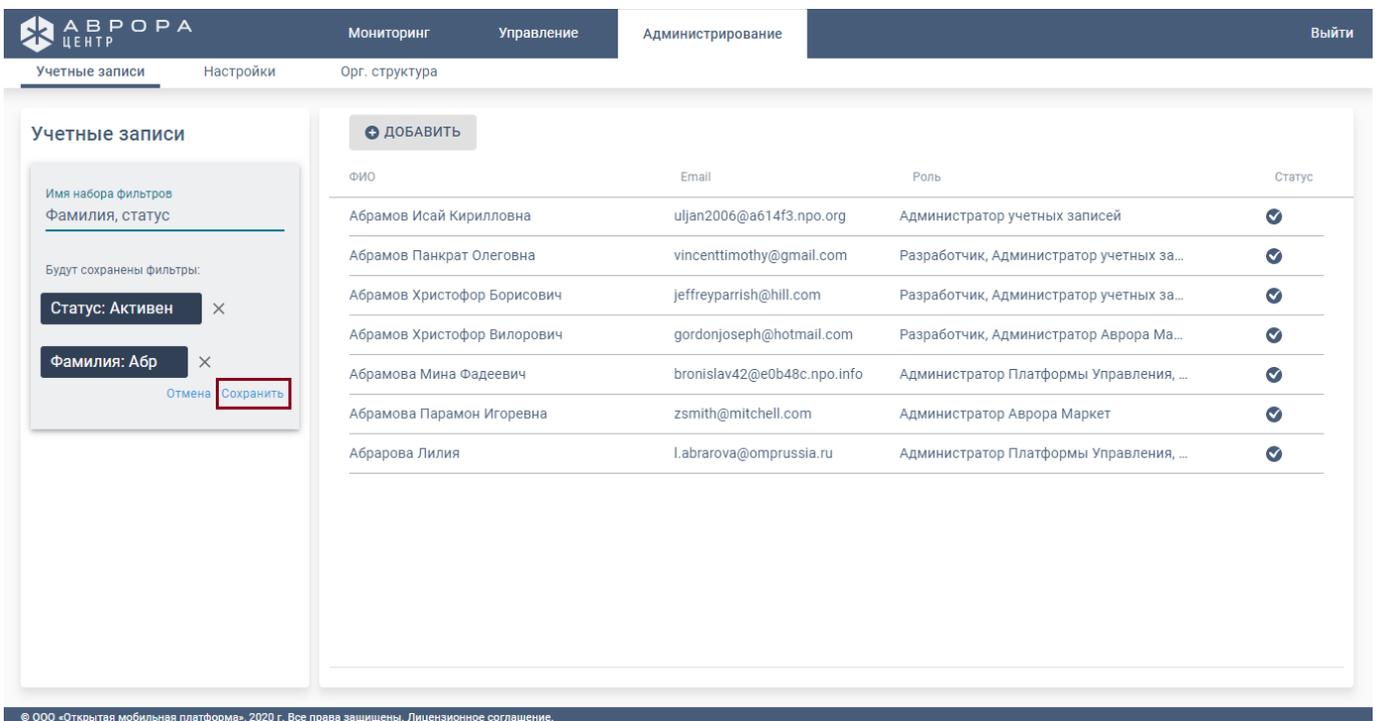
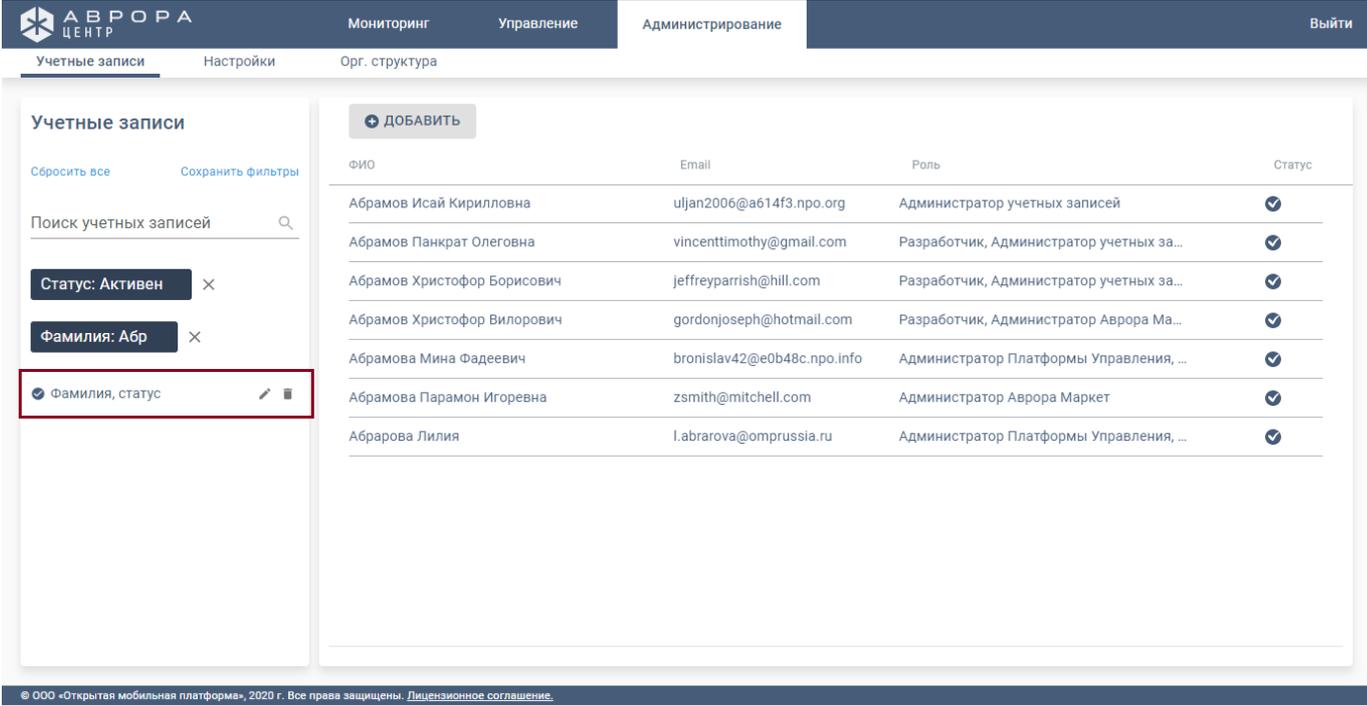


Рисунок 23

В результате выбранная комбинация фильтров сохранится в набор. При необходимости набор можно редактировать, нажав на значок , или удалить, нажав на значок  (Рисунок 24).



Учетные записи

Сбросить все Сохранить фильтры

Поиск учетных записей

Статус: Активен ×

Фамилия: Абр ×

Фамилия, статус  

ДОБАВИТЬ

ФИО	Email	Роль	Статус
Абрамов Исая Кирилловна	uljan2006@a614f3.npo.org	Администратор учетных записей	✓
Абрамов Панкрат Олеговна	vincenttimothy@gmail.com	Разработчик, Администратор учетных за...	✓
Абрамов Христофор Борисович	jeffreyparrish@hill.com	Разработчик, Администратор учетных за...	✓
Абрамов Христофор Вилорович	gordonjoseph@hotmail.com	Разработчик, Администратор Аврора Ма...	✓
Абрамова Мина Фадеевич	bronslav42@e0b48c.npo.info	Администратор Платформы Управления, ...	✓
Абрамова Парамон Игоревна	zsmith@mitchell.com	Администратор Аврора Маркет	✓
Абрарова Лилия	l.abrarova@omprussia.ru	Администратор Платформы Управления, ...	✓

© ООО «Открытая мобильная платформа», 2020 г. Все права защищены. Лицензионное соглашение.

Рисунок 24

Для применения сохраненного набора фильтров к списку учетных записей необходимо нажать на имя файла. В рабочей области отобразится перечень, сформированный с применением набора фильтров (Рисунок 25).

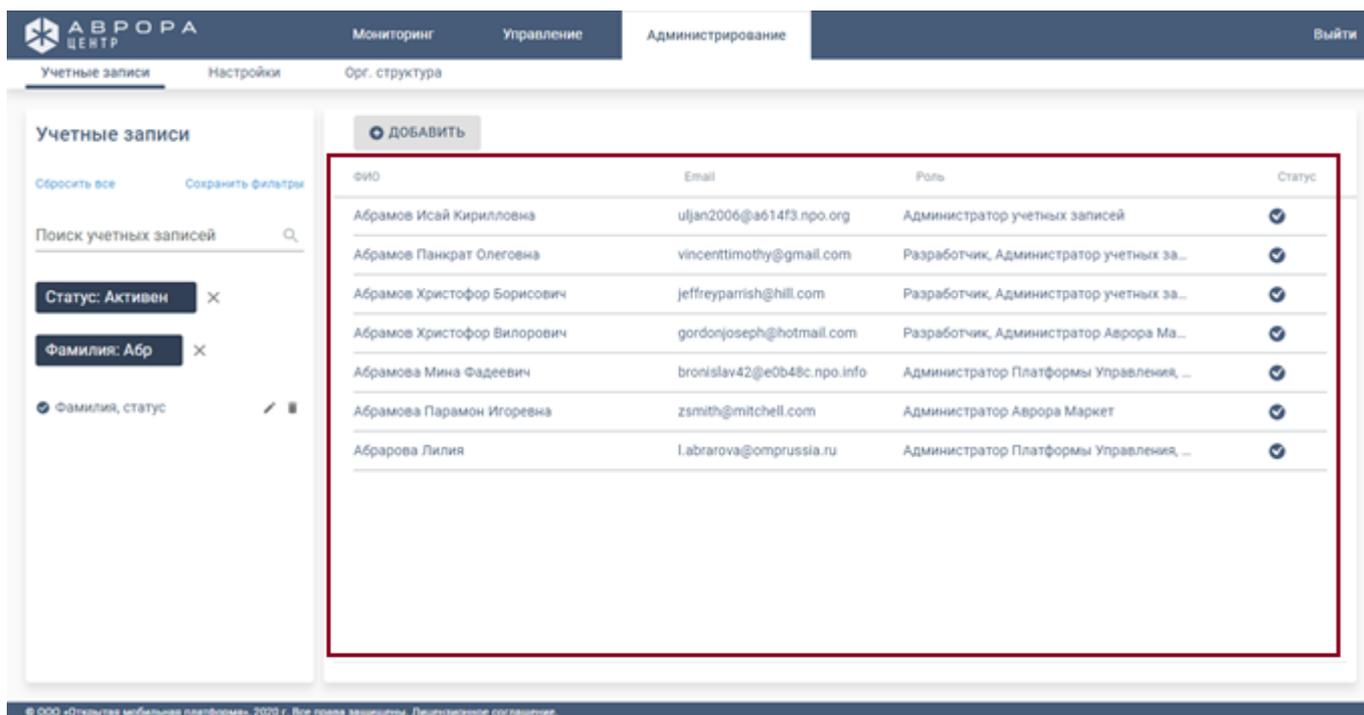


Рисунок 25

Для сброса всех фильтров необходимо нажать «Сбросить все» (Рисунок 26).

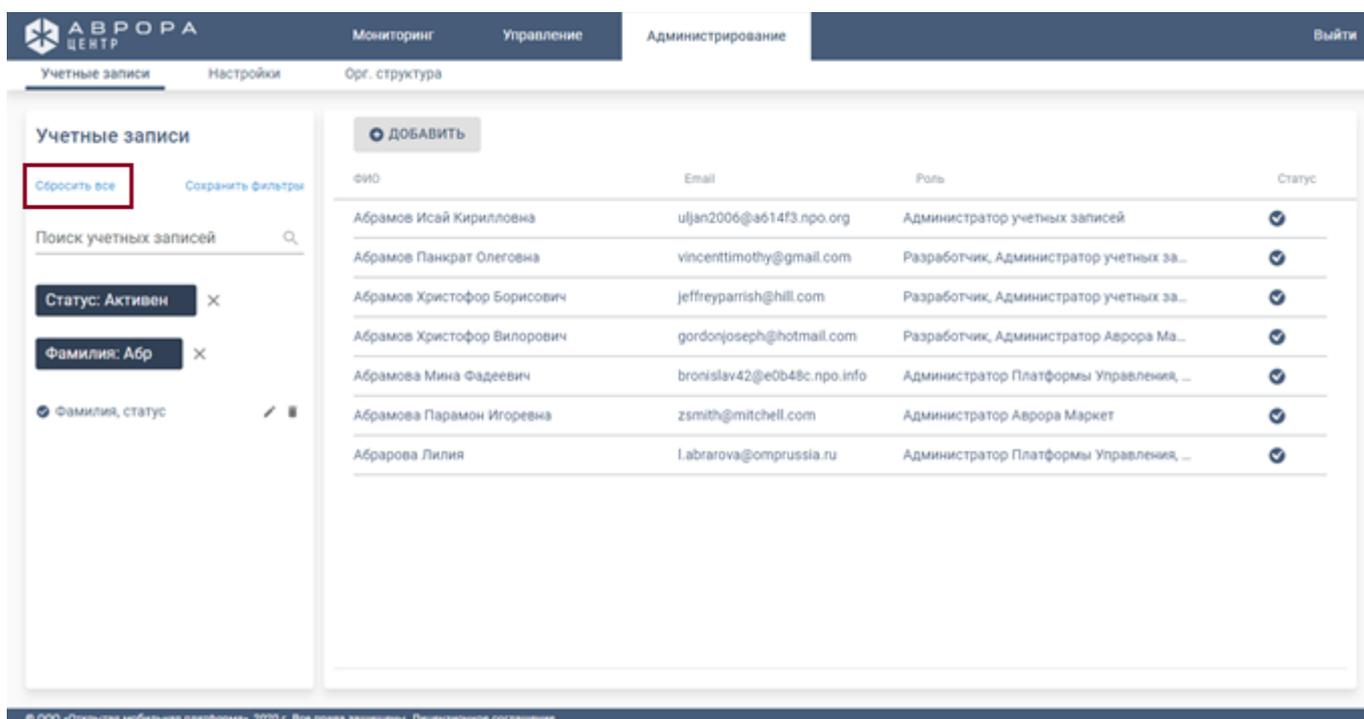
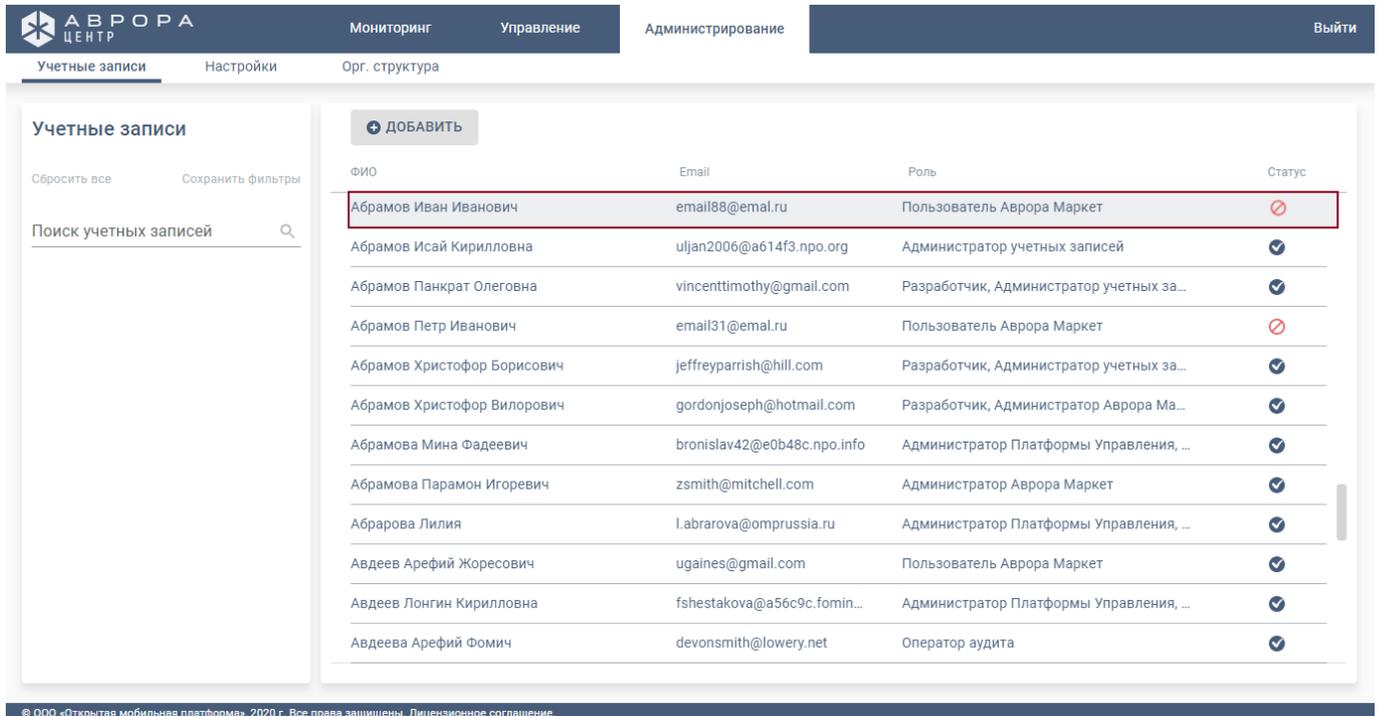


Рисунок 26

3.1.1.4. Смена пароля учетной записи

Для смены пароля учетной записи необходимо выполнить следующие действия:

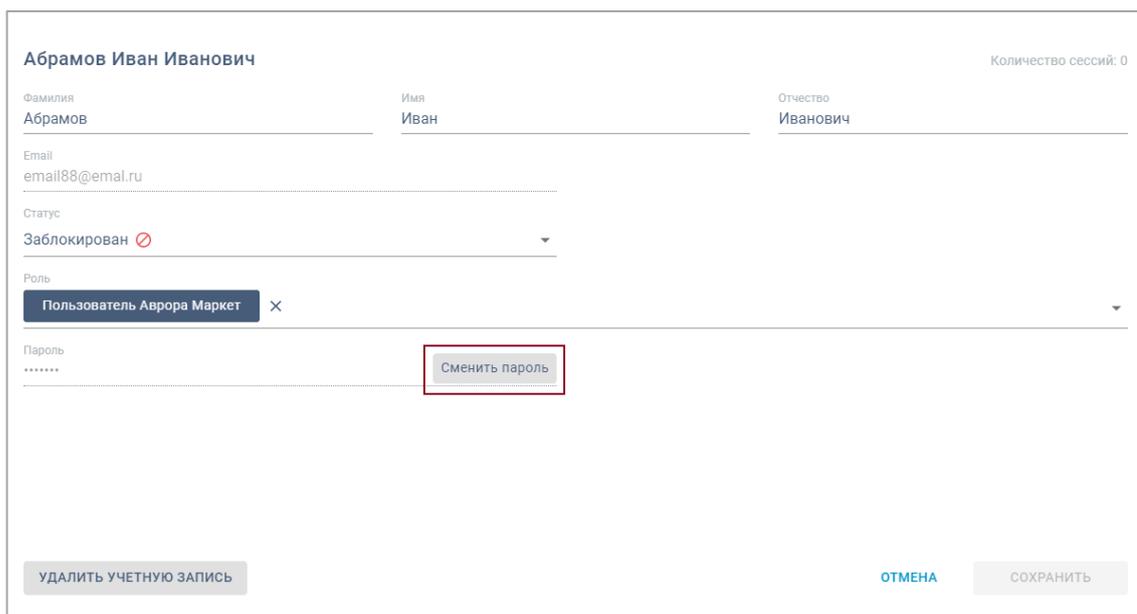
- нажать на строку учетной записи (Рисунок 27);



ФИО	Email	Роль	Статус
Абрамов Иван Иванович	email88@emal.ru	Пользователь Аврора Маркет	🚫
Абрамов Исай Кирилловна	uljan2006@a614f3.npo.org	Администратор учетных записей	✅
Абрамов Панкрат Олеговна	vincenttimothy@gmail.com	Разработчик, Администратор учетных за...	✅
Абрамов Петр Иванович	email31@emal.ru	Пользователь Аврора Маркет	🚫
Абрамов Христофор Борисович	jeffreyparrish@hill.com	Разработчик, Администратор учетных за...	✅
Абрамов Христофор Вилорович	gordonjoseph@hotmail.com	Разработчик, Администратор Аврора Ма...	✅
Абрамова Мина Фадеевич	bronislav42@e0b48c.npo.info	Администратор Платформы Управления, ...	✅
Абрамова Парамон Игоревич	zsmith@mitchell.com	Администратор Аврора Маркет	✅
Абларова Лилия	l.ablarova@omprussia.ru	Администратор Платформы Управления, ...	✅
Авдеев Арефий Жоресович	ugaines@gmail.com	Пользователь Аврора Маркет	✅
Авдеев Лонгин Кирилловна	fshestakova@a56c9c.fomin...	Администратор Платформы Управления, ...	✅
Авдеева Арефий Фомич	devonsmith@lowery.net	Оператор аудита	✅

Рисунок 27

- в открывшейся форме нажать кнопку «Сменить пароль» (Рисунок 28);



Абрамов Иван Иванович Количество сессий: 0

Фамилия: Абрамов | Имя: Иван | Отчество: Иванович

Email: email88@emal.ru

Статус: **Заблокирован** 🚫

Роль: **Пользователь Аврора Маркет** ✕

Пароль: **Сменить пароль**

УДАЛИТЬ УЧЕТНУЮ ЗАПИСЬ ОТМЕНА СОХРАНИТЬ

Рисунок 28

– в полях «Пароль», «Повторите пароль» ввести и подтвердить новый пароль (Рисунок 29). Требования к сложности пароля приведены в подразделе 2.1 настоящего документа;

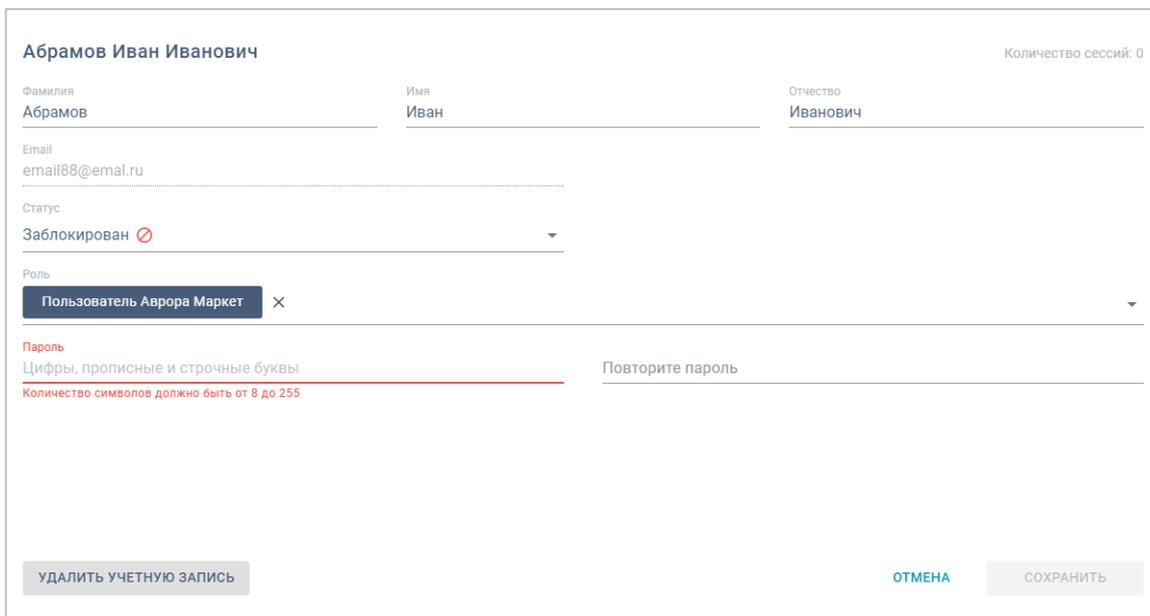


Рисунок 29

– нажать кнопку «Сохранить». Для отмены смены пароля нажать кнопку «Отмена» (Рисунок 30).

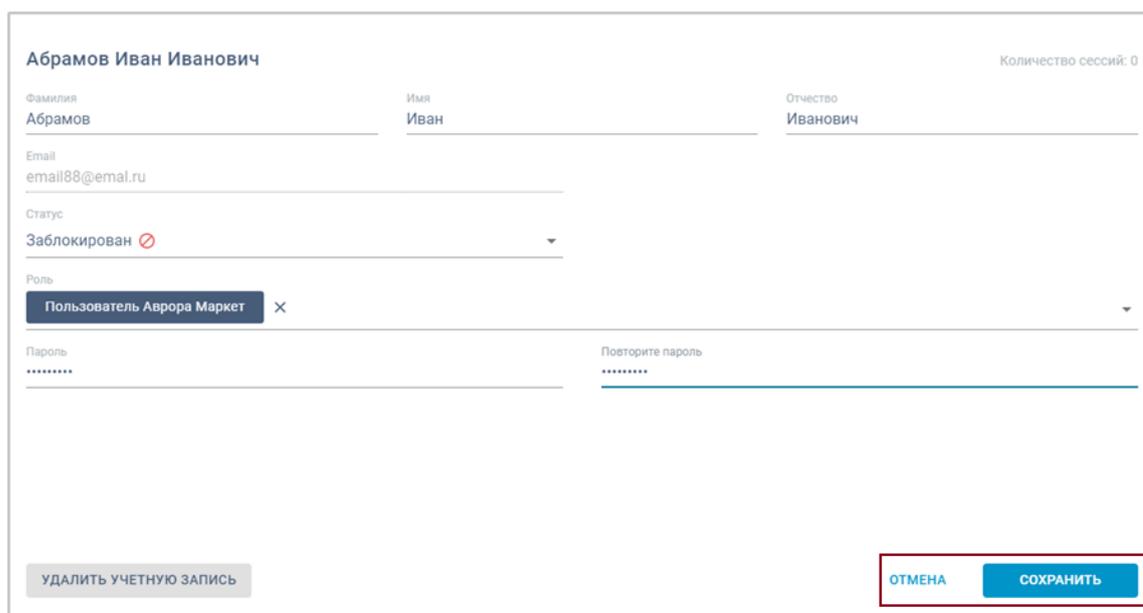


Рисунок 30

При успешном изменении пароля учетной записи отобразится сообщение «Учетная запись успешно обновлена» (Рисунок 31).

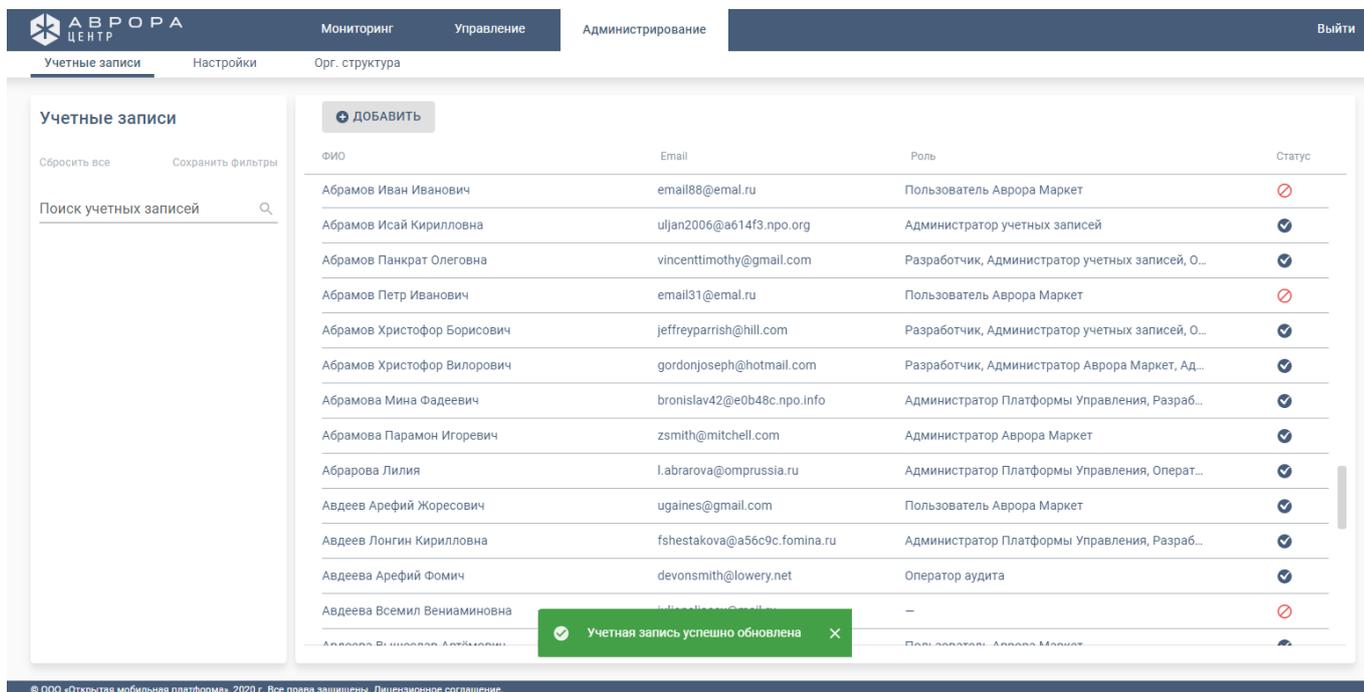


Рисунок 31

3.1.1.5. Удаление учетной записи

Для удаления данных учетной записи необходимо выполнить следующие действия:

- нажать на строку учетной записи (Рисунок 32);

ФИО	Email	Роль	Статус
Абрамов Иван Иванович	email88@emal.ru	Пользователь Аврора Маркет	
Абрамов Исai Кирилловна	uljan2006@a614f3.npo.org	Администратор учетных записей	
Абрамов Панкрат Олеговна	vincenttimothy@gmail.com	Разработчик, Администратор учетных записей, О...	
Абрамов Петр Иванович	email31@emal.ru	Пользователь Аврора Маркет	
Абрамов Христофор Борисович	jeffreyparrish@hill.com	Разработчик, Администратор учетных записей, О...	
Абрамов Христофор Вилорович	gordonjoseph@hotmail.com	Разработчик, Администратор Аврора Маркет, Ад...	
Абрамова Мина Фадеевич	bronislav42@e0b48c.npo.info	Администратор Платформы Управления, Разраб...	
Абрамова Парамон Игоревич	zsmith@mitchell.com	Администратор Аврора Маркет	
Абларова Лилия	l.ablarova@omprussia.ru	Администратор Платформы Управления, Операт...	
Авдеев Арeфий Жоресович	ugaines@gmail.com	Пользователь Аврора Маркет	
Авдеев Лонгин Кирилловна	fshestakova@a56c9c.fomina.ru	Администратор Платформы Управления, Разраб...	
Авдеева Арeфий Фомич	devonsmith@lowery.net	Оператор аудита	
Авдеева Всемил Вениаминовна	julianeliseev@mail.ru	—	
Авдеева Виктория Александровна	ifbaca@emal.ru	Пользователь Аврора Маркет	

Рисунок 32

— в открывшейся форме нажать кнопку «Удалить учетную запись» (Рисунок 33);

Абрамов Иван Иванович Количество сессий: 0

Фамилия: Абрамов Имя: Иван Отчество: Иванович

Email: email88@emal.ru

Статус: **Заблокирован**

Роль: **Пользователь Аврора Маркет** X

Пароль: Сменить пароль

УДАЛИТЬ УЧЕТНУЮ ЗАПИСЬ ОТМЕНА СОХРАНИТЬ

Рисунок 33

– нажать кнопку «Подтвердить». Для отмены удаления нажать кнопку «Отмена» (Рисунок 34).

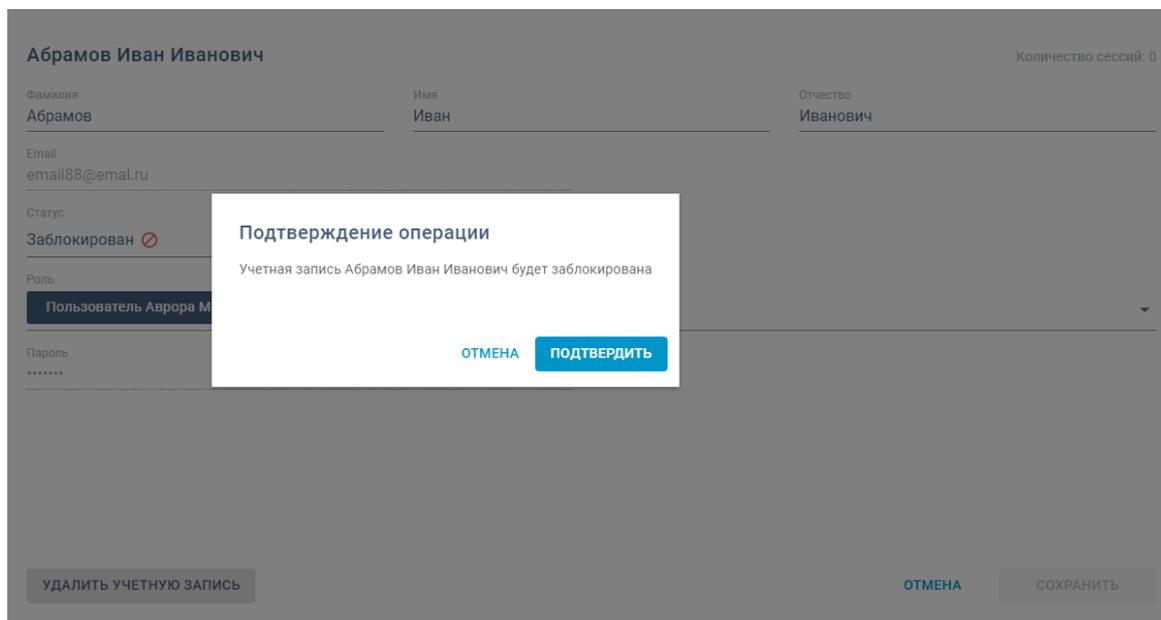


Рисунок 34

При успешном удалении учетной записи отобразится сообщение «Учетная запись успешно удалена» (Рисунок 35).

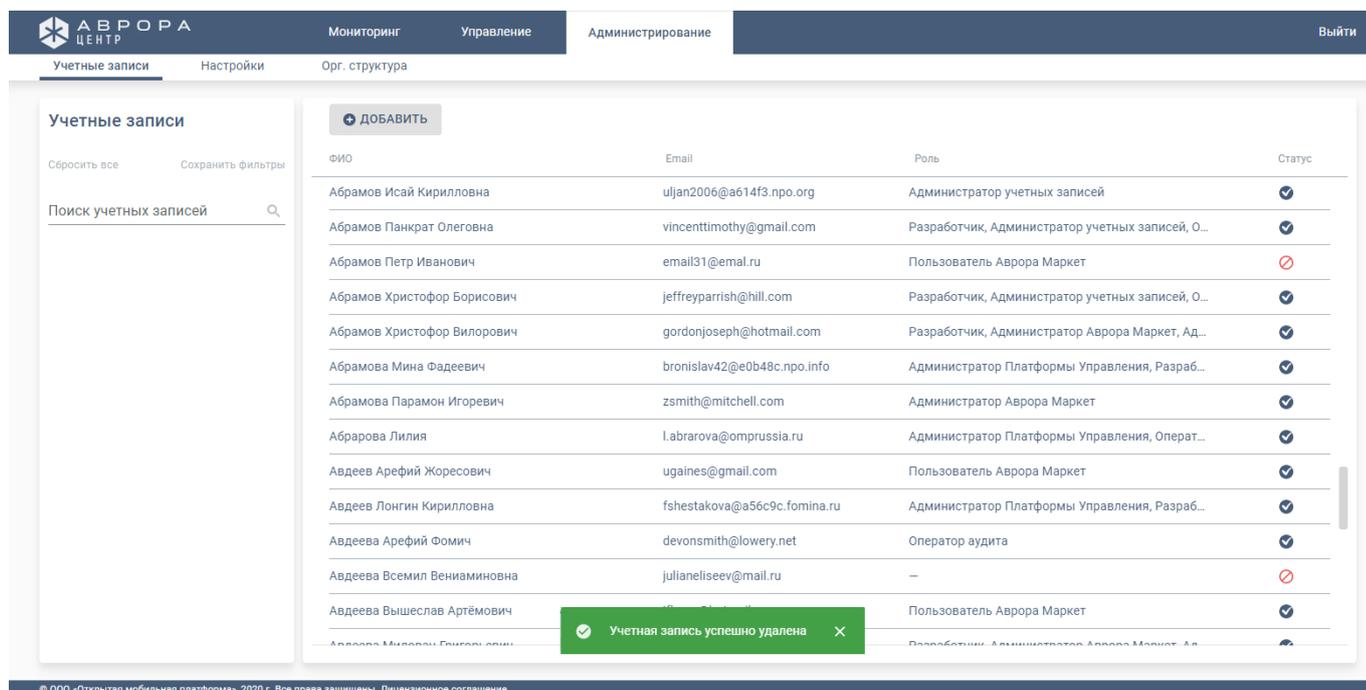


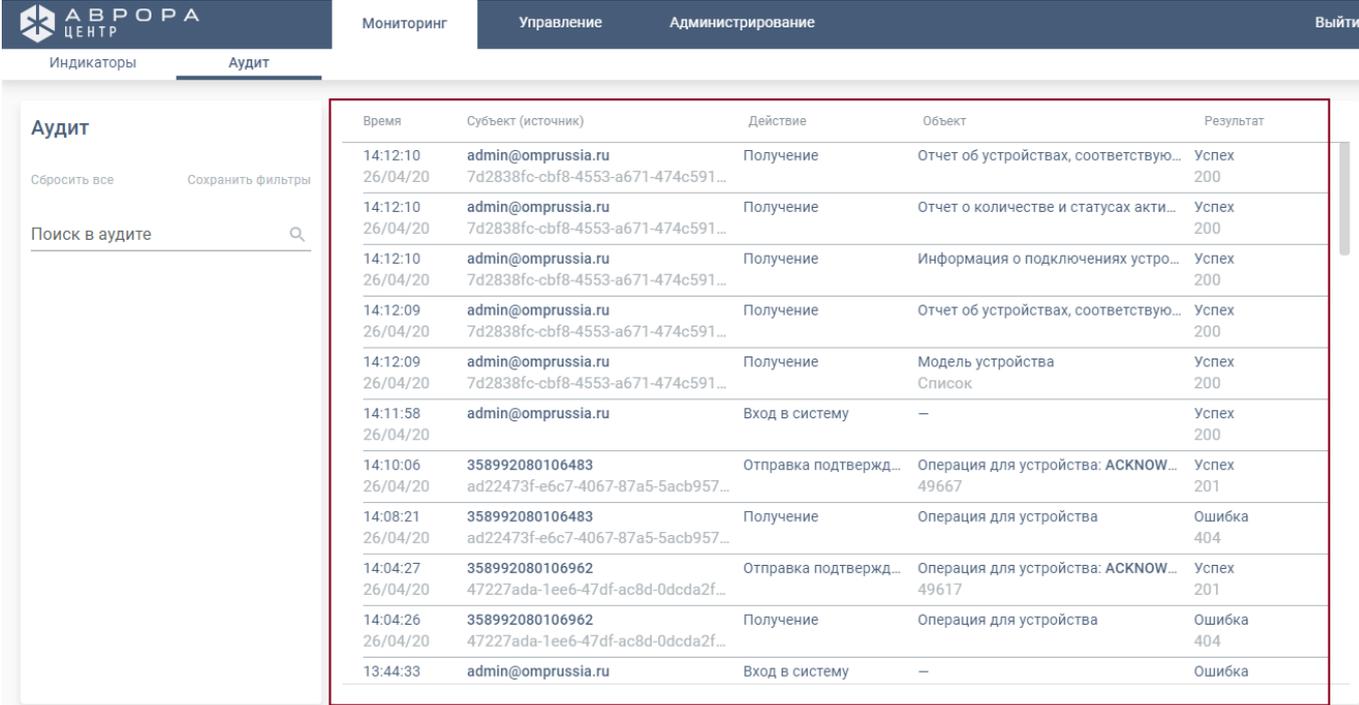
Рисунок 35

3.2. Консоль администратора ПБ. Раздел «Мониторинг»

3.2.1. Работа в подразделе «Аудит»

3.2.1.1. Рабочая область

В рабочей области Консоли администратора ПБ в разделе «Мониторинг» в подразделе «Аудит» отображается информация о событиях ППО (Рисунок 36).



Время	Субъект (источник)	Действие	Объект	Результат
14:12:10 26/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет об устройствах, соответствую...	Успех 200
14:12:10 26/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет о количестве и статусах акти...	Успех 200
14:12:10 26/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Информация о подключениях устро...	Успех 200
14:12:09 26/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет об устройствах, соответствую...	Успех 200
14:12:09 26/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Модель устройства Список	Успех 200
14:11:58 26/04/20	admin@omprussia.ru	Вход в систему	–	Успех 200
14:10:06 26/04/20	358992080106483 ad22473f-e6c7-4067-87a5-5acb957...	Отправка подтвержд...	Операция для устройства: ACKNOW... 49667	Успех 201
14:08:21 26/04/20	358992080106483 ad22473f-e6c7-4067-87a5-5acb957...	Получение	Операция для устройства	Ошибка 404
14:04:27 26/04/20	358992080106962 47227ada-1ee6-47df-ac8d-0dcda2f...	Отправка подтвержд...	Операция для устройства: ACKNOW... 49617	Успех 201
14:04:26 26/04/20	358992080106962 47227ada-1ee6-47df-ac8d-0dcda2f...	Получение	Операция для устройства	Ошибка 404
13:44:33	admin@omprussia.ru	Вход в систему	–	Ошибка

© ООО «Открытая мобильная платформа», 2020 г. Все права защищены. Лицензионное соглашение.

Рисунок 36

Подробное описание информации о событиях ППО приведено в таблице (Таблица 8).

Таблица 8

Элемент	Описание	Возможные значения
Время	Дата и время наступления события	– дата в формате DD/MM/YY; – время в формате HH:mm:ss
Субъект (источник)	Кто (что) совершил действие	– Логин инициатора; – ID объекта

Элемент	Описание	Возможные значения
Действие	Тип действия, совершенного над объектом	<ul style="list-style-type: none"> – «Создание»; – «Изменение»; – «Удаление»; – «Получение»; – «Отправка на ревью»; – «Согласование»; – «Отклонение»; – «Получение архива»; – «Получение релизов»; – «Получение ролей»; – «Добавление роли»; – «Удаление роли»; – «Блокировка»; – «Разблокировка»; – и т.д.
Объект	<ul style="list-style-type: none"> – название объекта, над которым произведено действие; – тип объекта, над которым произведено действие; – идентификатор объекта, над которым произведено действие 	<ul style="list-style-type: none"> – «Список»; – «Категория»; – «Приложение»; – «Релиз»; – «Иконка»; – «Билд»; – «Скриншот»; – «Учетная запись»; – «Роль»; – «Событие аудита»; – «Параметры доступа к серверу Аврора Маркет»; – «Связь»; – «Группа устройств»; – «Устройство»; – и т.д.

Элемент	Описание	Возможные значения
Результат	Ответ ППО	<ul style="list-style-type: none"> – Создано; – Обновлено; – Ошибка; – Успех

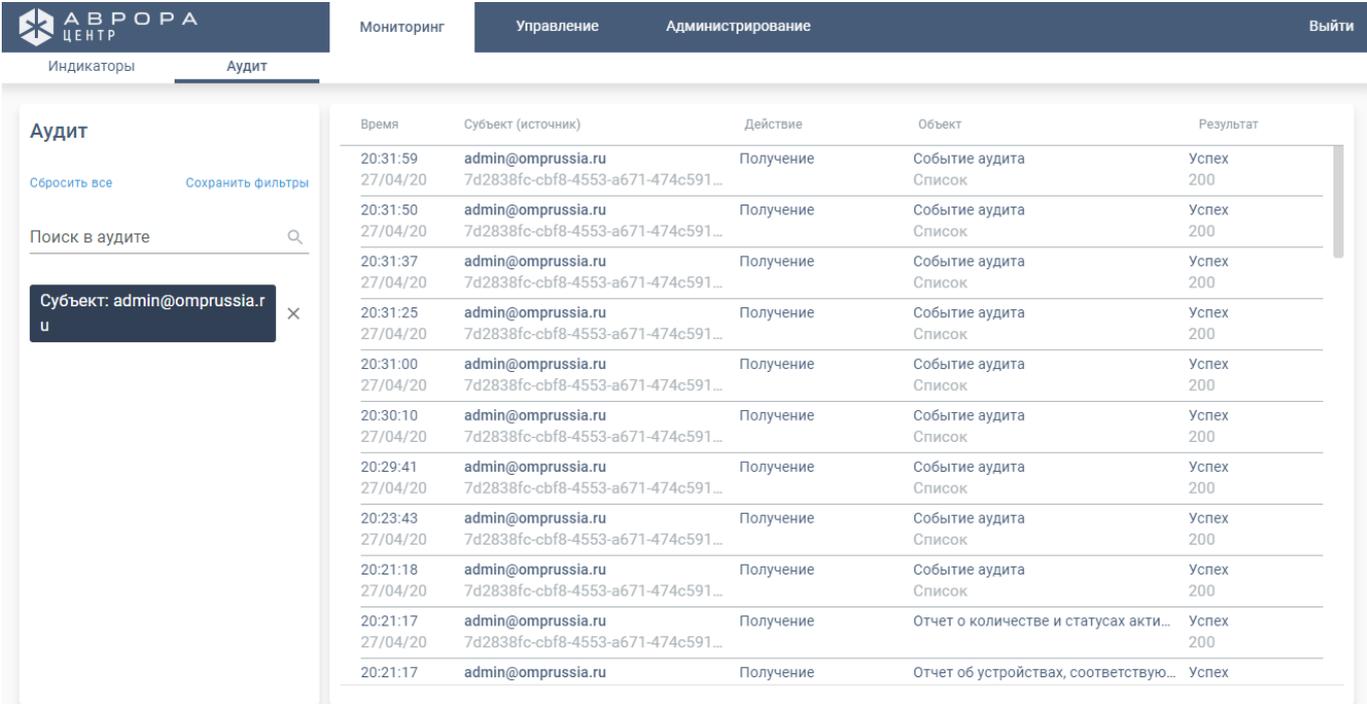
3.2.1.2. Работа с фильтрами

В области фильтров предусмотрена возможность поиска по заданным критериям (см. Таблица 6, Рисунок 8).

Для поиска необходимо выполнить следующие действия (см. Рисунок 8):

- установить курсор в поле поиска;
- выбрать один из фильтров для поиска;
- ввести поисковый запрос;
- нажать на значок , для очистки поля нажать на значок .

В результате выполнится поиск по выбранному фильтру (Рисунок 37).



The screenshot displays the 'Аудит' (Audit) section of the 'АВРОРА ЦЕНТР' system. The top navigation bar includes 'Мониторинг', 'Управление', 'Администрирование', and 'Выйти'. The main content area is divided into a left sidebar and a main table.

Left Sidebar (Аудит):

- Buttons: 'Сбросить все', 'Сохранить фильтры'
- Search field: 'Поиск в аудите' with a magnifying glass icon.
- Active filter: 'Субъект: admin@omprussia.ru' with a close icon (X).

Main Table:

Время	Субъект (источник)	Действие	Объект	Результат
20:31:59 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Событие аудита Список	Успех 200
20:31:50 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Событие аудита Список	Успех 200
20:31:37 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Событие аудита Список	Успех 200
20:31:25 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Событие аудита Список	Успех 200
20:31:00 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Событие аудита Список	Успех 200
20:30:10 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Событие аудита Список	Успех 200
20:29:41 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Событие аудита Список	Успех 200
20:23:43 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Событие аудита Список	Успех 200
20:21:18 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Событие аудита Список	Успех 200
20:21:17 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591...	Получение	Отчет о количестве и статусах акти...	Успех 200
20:21:17	admin@omprussia.ru	Получение	Отчет об устройствах, соответствующ...	Успех

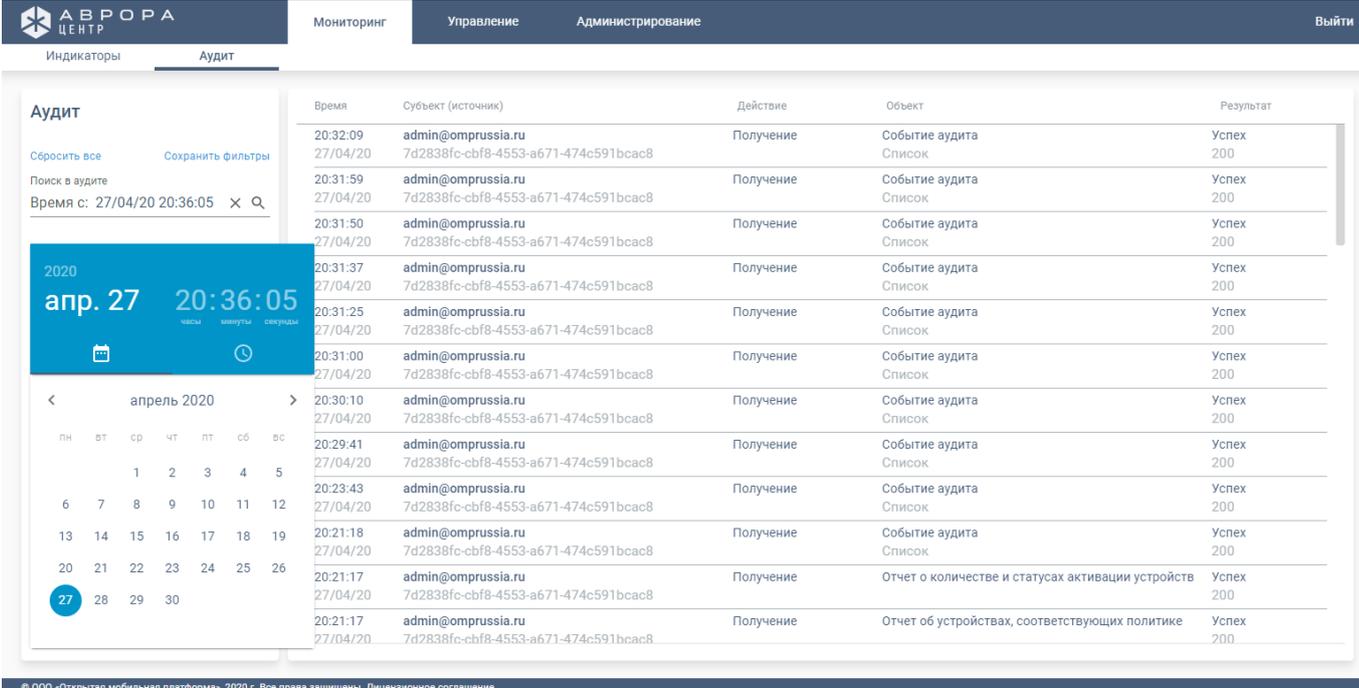
© ООО «Открытая мобильная платформа», 2020 г. Все права защищены. Лицензионное соглашение.

Рисунок 37

Для формирования детальной выборки необходимо произвести поиск по времени события за выбранный период (дате и времени). Для этого необходимо выполнить следующие действия:

- установить курсор в поле поиска;
- выбрать фильтр «Время с». В результате отобразится календарь, где необходимо выбрать дату начало периода события (Рисунок 38).

При открытии фильтра по времени по умолчанию будет отображаться текущие дата и время



Время	Субъект (источник)	Действие	Объект	Результат
20:32:09 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:31:59 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:31:50 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:31:37 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:31:25 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:31:00 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:30:10 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:29:41 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:23:43 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:21:18 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Событие аудита Список	Успех 200
20:21:17 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Отчет о количестве и статусах активации устройств	Успех 200
20:21:17 27/04/20	admin@omprussia.ru 7d2838fc-cbf8-4553-a671-474c591bcac8	Получение	Отчет об устройствах, соответствующих политике	Успех 200

Рисунок 38

– далее после выбора даты события необходимо выбрать время события, коснувшись значка . В результате отобразится циферблат, где необходимо выбрать время события (Рисунок 39);

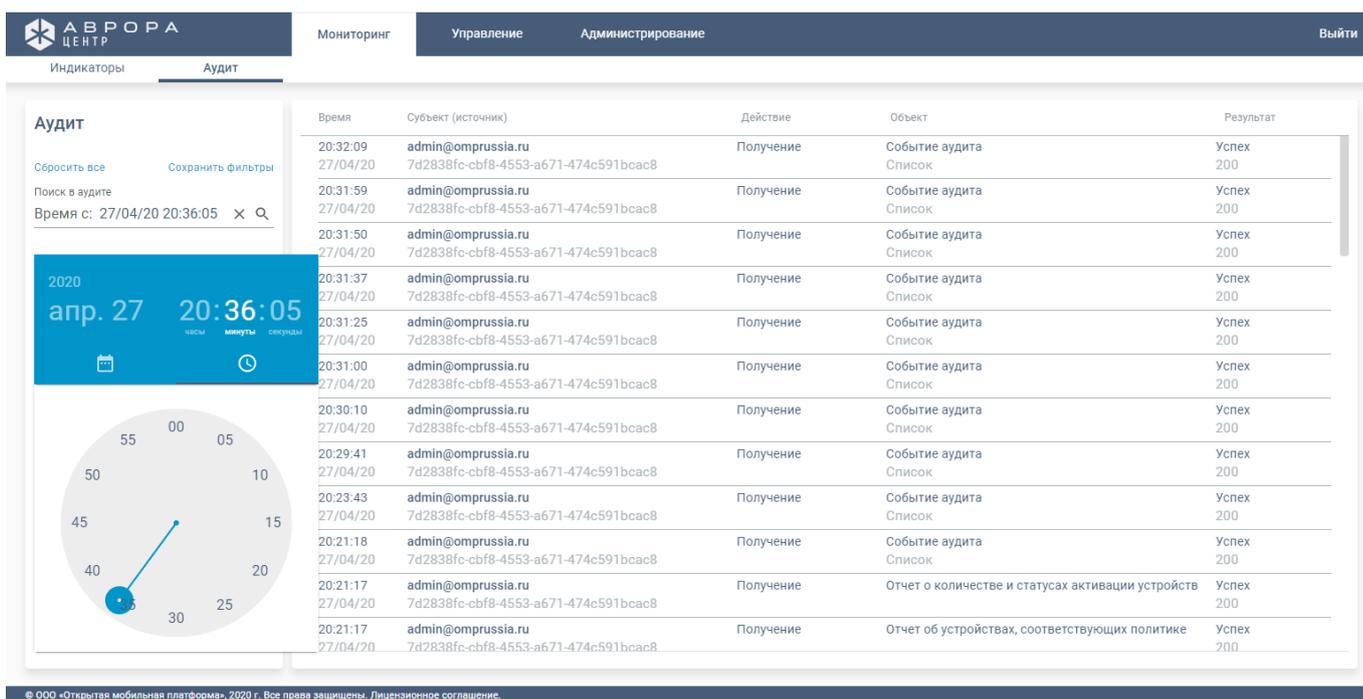


Рисунок 39

- нажать на значок , для очистки поля нажать на значок ;
- в рабочей области отобразится перечень, сформированный с применением выбранных фильтров (Рисунок 40).

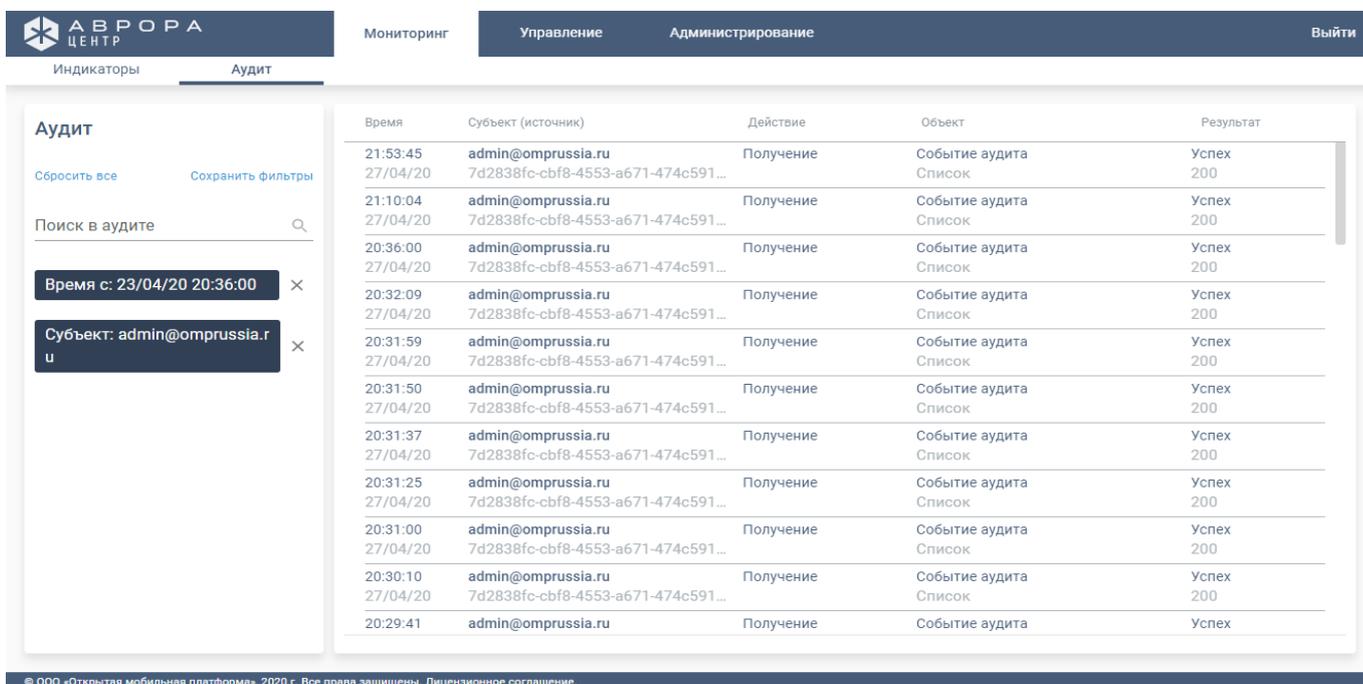


Рисунок 40

Для формирования более детальной выборки необходимо добавить несколько фильтров

3.3. Окончание сеанса работы

По окончании сеанса работы необходимо нажать кнопку «Выйти» в верхней панели (Рисунок 41).

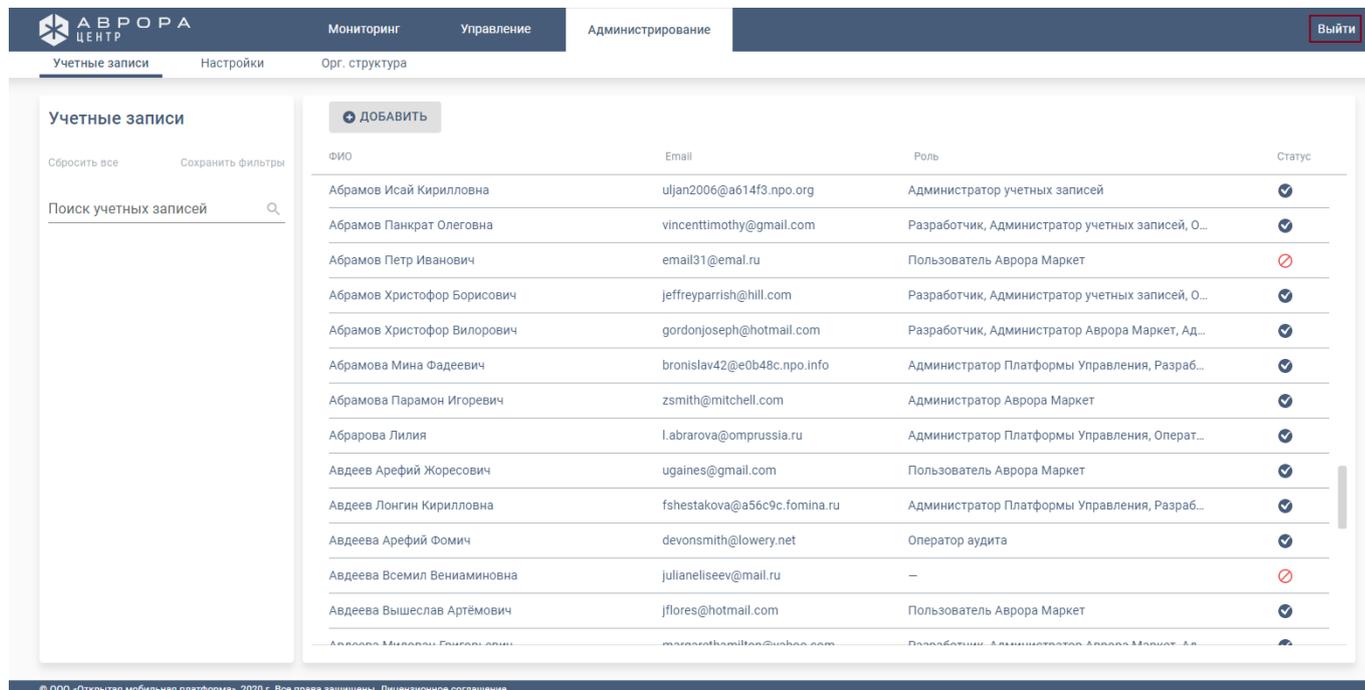


Рисунок 41

В результате откроется Консоль входа пользователей (см. Рисунок 2).

4. ОПИСАНИЕ УСТАНОВКИ ППО

ВНИМАНИЕ! При копировании команд в формате PDF из настоящего раздела будьте внимательны. Администратор/Разработчик должен проверять результаты выполнения команд на экране.

4.1. Общая информация

Установка ППО и компонентов среды функционирования ППО осуществляется с помощью сценариев установки ППО, выполняемых на управляющей ПЭВМ и написанных с использованием декларативного языка разметки для описания конфигураций Ansible. Сценарии установки ППО позволяют выполнить установку как локально (все компоненты на одной ПЭВМ), так и с удаленной ПЭВМ (управляющей ПЭВМ) (Рисунок 42).

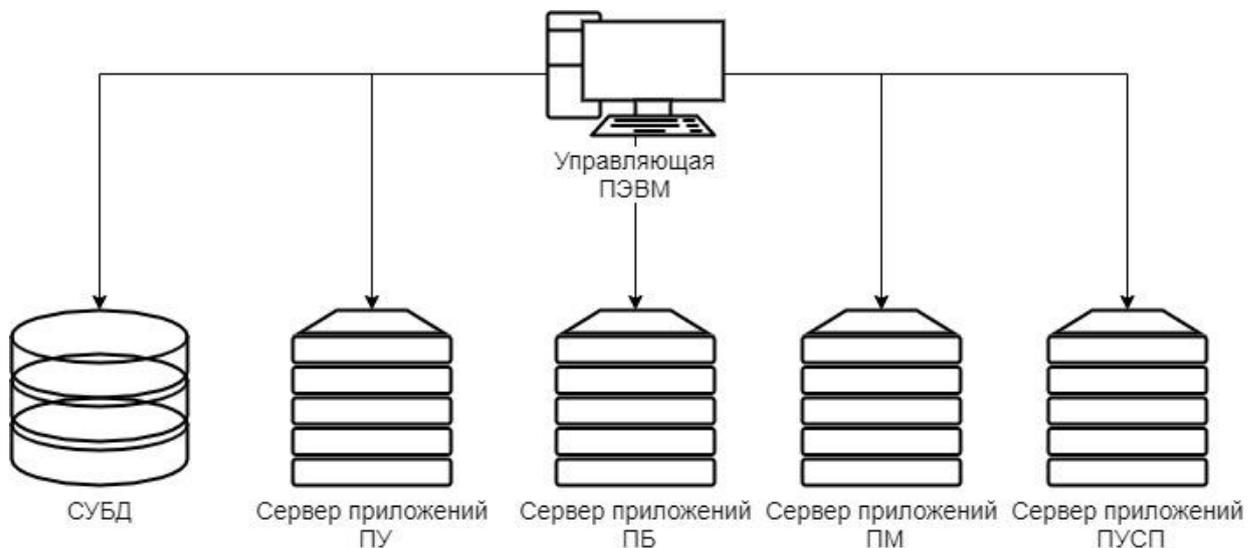


Рисунок 42

Управляющая ПЭВМ нужна только для установки ППО.

Установка ППО осуществляется в два этапа:

- 1) установка компонентов среды функционирования;
- 2) установка ППО.

Предусмотрены следующие типы конфигурационных файлов:

1) Конфигурационные файлы сценариев установки среды функционирования ППО. Описание параметров конфигурационных файлов и сценариев установки среды функционирования ППО приведено в подразделе 4.9 настоящего документа;

2) Конфигурационные файлы модулей ППО:

- ПБ;
- ПМ;
- ПУ;
- ПУСП.

Описание параметров конфигурационных файлов модулей ППО приведено в разделе 8 настоящего документа.

4.2. Порядок действий по приемке ППО

4.2.1. Проверка комплектности

4.2.1.1. Проверка проводится путем сравнения комплектности представленного ППО с комплектностью, указанной в соответствующем разделе «Формуляра».

4.2.1.2. ППО считается удовлетворяющим требованиям, если комплектность представленного ППО соответствует комплектности, указанной в соответствующем разделе «Формуляра».

4.2.2. Проверка контрольных сумм

4.2.2.1. Проверка ППО проводится путем сравнения КС загрузочного модуля ППО со значениями, указанными в соответствующем разделе «Формуляра» и на этикетке DVD с загрузочным модулем ППО.

4.2.2.2. КС файлов ПП рассчитаны с использованием программы «Средство фиксации и контроля целостности информации «ФИКС-Unix 1.0» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 680, действителен до 26 февраля 2021 г.).

4.2.2.3. ППО считается удовлетворяющим требованиям в случае совпадения КС, выданной программой, со значениями, указанными в «Формуляре» и на этикетке DVD.

4.2.3. Проверка качества изготовления

4.2.3.1. Проверка ППО проводится путем внешнего осмотра поверхности DVD ППО на предмет отсутствия видимых механических дефектов и вычисления КС записанной информации.

ППО считается удовлетворяющим требованиям, если DVD принят ОТК предприятия-изготовителя, не имеет видимых механических дефектов, установленный срок хранения DVD не превышал 12 месяцев, а значение КС записанной информации совпадает со значением, приведенным на DVD и в «Формуляре».

4.3. Порядок установки компонентов среды функционирования

4.3.1. Порядок установки и настройки ОС на управляющей ПЭВМ, серверах приложений и серверах БД

Для установки и настройки ОС на управляющей ПЭВМ, серверах приложений и серверах БД необходимо выполнить следующие действия:

4.3.1.1. Установить ОС CentOS версии 7 или ОС Альт 8 СП на управляющую ПЭВМ, сервера приложений и сервера БД.

ВНИМАНИЕ! Перед установкой указанной выше ОС необходимо ознакомиться с требованиями, приведенными в документации на СЗИ НСД.

ОС должна быть установлена в минимальной конфигурации без графического интерфейса. Для установки ОС CentOS версии 7 необходимо использовать iso-образ в названии которого содержится «Minimal». Например, CentOS-7-x86_64-Minimal-1810.iso.

Настройки сети ОС должны удовлетворять следующим требованиям:

1) для основного сетевого интерфейса должен присутствовать конфигурационный ifcfg файл:

– ОС CentOS: /etc/sysconfig/network-scripts/ifcfg-<имя интерфейса>

2) сетевой интерфейс должен автоматически запускаться при загрузке ОС

Для этого значение параметра ONBOOT в /etc/sysconfig/network-scripts/ifcfg<имя интерфейса> (для ОС CentOS) должно иметь значение «yes»:

```
ONBOOT=yes
```

3) приоритеты в конфигурационном файле /etc/nsswitch.conf файле должны выглядеть следующим образом (при использовании dnsmasq):

```
hosts: files dns ...
```

где `...` - остальные опции, если они используются.

4.3.1.2. Перейти в учетную запись пользователя root с помощью команды:

```
su -
```

4.3.1.3. Назначить пользователям ОС права на выполнение команд от имени суперпользователя root.

Для этого необходимо добавить пользователя в группу wheel, выполнив команду:

```
usermod -aG wheel username
```

Разрешить пользователям, входящим в группу wheel, выполнять команды без ввода пароля. Для чего в файле /etc/sudoers раскомментировать строку:

```
# %wheel    ALL=(ALL)    NOPASSWD: ALL
```

Открыть файл /etc/sudoers необходимо от имени суперпользователя root с помощью команды:

```
visudo
```

ВНИМАНИЕ! Права на выполнение команд от имени суперпользователя root должны быть назначены всем пользователям (на управляющей ПЭВМ, серверах приложений и серверах БД), которыми осуществляется установка компонентов среды функционирования, СУБД и ППО. В противном случае, в процессе установки возникнут ошибки.

4.3.1.4. Установить кодировку UTF-8 с помощью команды:

– ОС CentOS версии 7

```
localectl set-locale LANG=en_US.UTF-8
```

– ОС Альт 8 СП

В конфигурационном файле `/etc/sysconfig/i18n` задать следующее значение параметра LANG:

```
LANG=en_US.UTF-8
```

4.3.1.5. Задать имя хоста с помощью команды:

```
hostnamectl set-hostname "имя_хоста.имя_домена"
```

ВНИМАНИЕ! При задании имени хоста обязательно должно быть задано имя домена, которое отделяется точкой. Например:

```
hostnamectl set-hostname ocs-app.local
```

4.3.1.6. В настройках DNS-сервера или файлах `/etc/hosts` указать имена хостов (hostname) и полные имена доменов (FQDN) всех серверов кластера.

4.3.1.7. В ОС CentOS отключить SELinux. Для этого в конфигурационном файле `/etc/selinux/config` необходимо задать следующее значение параметра SELINUX:

```
SELINUX=disabled
```

4.3.1.8. Отключить в ОС межсетевой экран с помощью выполнения следующих команд:

```
systemctl stop firewalld  
systemctl disable firewalld
```

4.3.1.9. Перезагрузить управляющую ПЭВМ и сервера с помощью команды:

```
reboot
```

4.3.2. Порядок развертывания и настройки управляющей ПЭВМ

ВНИМАНИЕ! Перед развертыванием и настройкой управляющей ПЭВМ должны быть установлены и настроены ОС на управляющей ПЭВМ, серверах приложений и серверах БД в соответствии с п. 4.3.1.

Для развертывания и настройки управляющей ПЭВМ необходимо выполнить следующие действия:

4.3.2.1. Установить на управляющей ПЭВМ пакеты с помощью последовательного выполнения команд следующие пакеты:

– ОС CentOS версии 7 (управляющая ПЭВМ)

```
sudo yum -y install epel-release
sudo yum -y install jq
sudo yum -y install python-pip
sudo -H pip install ansible==2.9.2
sudo yum -y install sed
sudo yum -y install coreutils
```

– ОС Альт 8 СП (управляющая ПЭВМ)

```
sudo apt-get -y install jq
sudo apt-get -y install python-module-pip
sudo apt-get -y install python-module-psycopg2
sudo -H pip install ansible==2.9.2
sudo apt-get -y install coreutils
sudo pip install 'jinja2==2.10'
```

4.3.2.2. Настроить SSH доступ управляющей ПЭВМ к серверам приложений и серверам БД (даже в том случае, когда управляющая ПЭВМ и сервера установлены на одной ПЭВМ):

– сформировать ключевую пару на управляющем сервере:

```
ssh-keygen -t rsa
```

- скопировать открытый ключ на сервер приложений и БД:

```
ssh-copy-id <имя пользователя>@<сервер приложений>
```

```
ssh-copy-id <имя пользователя>@<сервер БД>
```

- проверить доступ с управляющей машины на сервера приложения и БД по

SSH ключу (при выполнении команд ниже ввод пароля не должен требоваться):

```
ssh <имя пользователя>@<сервер приложения>
```

```
ssh <имя пользователя>@<сервер БД>
```

Управляющие команды, формируемые сценариями установки ППО, передаются с использованием протокола SSH

4.3.3. Порядок установки и настройки компонентов среды функционирования серверов приложений

Для установки и настройки компонентов среды функционирования серверов приложений необходимо выполнить следующие действия:

4.3.3.1. Установить на сервера приложений с помощью последовательного выполнения команд следующие пакеты:

- ОС CentOS версии 7 (сервер приложений)

```
sudo yum -y install epel-release
```

```
sudo yum -y install jq
```

```
sudo yum -y install unzip
```

```
sudo yum -y install perl-libs
```

```
sudo yum -y install libxslt
```

```
sudo yum -y install postgresql-libs
```

```
sudo yum -y install libicu
```

```
sudo yum -y install dnsmasq
```

```
sudo yum -y install bind-utils
```

- ОС Альт 8 СП (сервер приложений)

```
sudo apt-get -y install glibc
```

```
sudo apt-get -y install libcrypt
```

```
sudo apt-get -y install jq
```

```
sudo apt-get -y install unzip
```

```
sudo apt-get -y install nginx
sudo apt-get -y install python-module-pkginfo
sudo apt-get -y install dnsmasq
sudo apt-get -y install bind-utils
```

4.3.3.2. Скопировать содержимое DVD с компонентами среды функционирования ППО на управляющую ПЭВМ. Например, в каталог `~/ocs-install-infra`.

Текущий пользователь на управляющей ПЭВМ, от имени которого проводится установка, должен быть владельцем папки и ее содержимого. В случае если у текущего пользователя на управляющей ПЭВМ отсутствуют данные полномочия, необходимо выполнить команду:

```
chown -R "пользователь:группа пользователя" ~/ocs-install-infra
```

4.3.3.3. В конфигурационном файле `inventories/hosts.yml` задать адреса серверов (имена хостов), на которые будут установлены компоненты среды функционирования ППО

Для отображения адреса ПЭВМ необходимо выполнить команду:

```
hostname
```

Конфигурационный файл сценария установки среды функционирования ППО на одной ПЭВМ с адресом `ocs-app.local` имеет следующий вид:

```
---
all:
  children:
    app:
      hosts:
        ocs-app.local:
    postgresql:
      children:
        postgresql_masters:
          hosts:
```

```
    ocs-app.local:
nginx:
  children:
    app:
consul:
  children:
    consul_servers:
      children:
        app:
    consul_agents:
consul-template:
  children:
    app:
nats_streaming_server:
  hosts:
    ocs-app.local:
redis:
  children:
    redis_masters:
      hosts:
        ocs-app.local:
    sentinel:
      hosts:
        ocs-app.local:
```

Описание параметров конфигурационного файла `inventories/hosts.yml` приведено в пп. 4.10.1.1 настоящего документа.

4.3.3.4. В конфигурационном файле сервиса гарантированной доставки сообщений Nats Streaming Server (файл: `inventories/group_vars/nats_streaming_servers/vars.yml`) задать токен доступа к Nats Streaming Server:

```
nats_token: FF12fddgdhFLL
```

Описание параметров конфигурационного файла

`inventories/group_vars/nats_streaming_servers/vars.yml` приведено в пп. 4.10.1.2 настоящего документа.

4.3.3.5. В конфигурационном файле СУБД Redis (файл: `inventories/group_vars/redis/vars.yml`) задать пароль доступа к СУБД Redis в параметре `redis_password`:

```
redis_password: "@rTT9089087fslk"
```

Описание параметров конфигурационного файла

`inventories/group_vars/redis/vars.yml` приведено в пп. 4.10.1.4 настоящего документа.

4.3.3.6. Отключить сокрытие ошибок в конвейере (pipeline) с помощью команды:

```
set -o pipefail
```

4.3.3.7. Выполнить установку компонентов среды функционирования ППО с помощью команды:

```
ansible-playbook -i inventories/hosts.yml play-  
{dnsmasq,nginx,consul,consul-template,nats-streaming-server,redis,ocs-  
user}.yml -vv --diff -u <имя пользователя> | tee -a install-infra.$(date  
'+%Y%m%d_%H%M%S').log
```

1) В параметре <имя пользователя> указывается имя привилегированного sudo-пользователя, под которым настроен SSH-доступ к серверам приложений и БД

2) Доступ по SSH к среде функционирования ППО может быть недоступен в соответствии с политиками компании. В данном случае необходимо во всех командах `ansible-playbook` в конце добавлять параметр `--ask-pass`

Также возможна раздельная установка компонентов среды функционирования ППО:

```
ansible-playbook -i inventories/hosts.yml play-dnsmasq.yml -vv --diff -u <ИМЯ пользователя> | tee -a install-infra-dnsmasq.$(date '+%Y%m%d_%H%M%S').log
```

```
ansible-playbook -i inventories/hosts.yml play-nginx.yml -vv --diff -u <ИМЯ пользователя> | tee -a install-infra-nginx.$(date '+%Y%m%d_%H%M%S').log
```

```
ansible-playbook -i inventories/hosts.yml play-consul.yml -vv --diff -u <ИМЯ пользователя> | tee -a install-infra-consul.$(date '+%Y%m%d_%H%M%S').log
```

```
ansible-playbook -i inventories/hosts.yml play-consul-template.yml -vv --diff -u <ИМЯ пользователя> | tee -a install-infra-consul-template.$(date '+%Y%m%d_%H%M%S').log
```

```
ansible-playbook -i inventories/hosts.yml play-nats-streaming-server.yml -vv --diff -u <ИМЯ пользователя> | tee -a install-infra-nats-streaming-server.$(date '+%Y%m%d_%H%M%S').log
```

```
ansible-playbook -i inventories/hosts.yml play-redis.yml -vv --diff -u <ИМЯ пользователя> | tee -a install-infra-redis.$(date '+%Y%m%d_%H%M%S').log
```

```
ansible-playbook -i inventories/hosts.yml play-ocs-user.yml -vv --diff -u <ИМЯ пользователя> | tee -a install-infra-ocs-user.$(date '+%Y%m%d_%H%M%S').log
```

4.3.4. Порядок установки и настройки СУБД PostgreSQL (Postgres Pro)

4.3.4.1. Порядок установки и настройки СУБД PostgreSQL 11 (ОС CentOS версии 7)

Для установки и настройки СУБД PostgreSQL 11 необходимо выполнить следующие действия:

4.3.4.1.1 Установить на сервера БД, работающие под управлением ОС CentOS версии 7 с помощью последовательного выполнения команд следующие пакеты:

```
sudo yum -y install epel-release  
sudo yum -y install jq
```

```
sudo yum -y install unzip
sudo yum -y install perl-libs
sudo yum -y install libxslt
sudo yum -y install postgresql-libs
sudo yum -y install libicu
sudo yum -y install python-psycopg2
```

4.3.4.1.2 В конфигурационном файле СУБД

inventories/group_vars/postgresql/vars.yml, находящимся в каталоге с компонентами среды функционирования ППО, задать следующие параметры:

- тип соединения, диапазон IP-адресов клиентов БД;
- имя БД, имя пользователя;
- способ аутентификации клиентов;
- пароль пользователя СУБД в параметре pg_superuser_password.

Описание параметров конфигурационного файла

inventories/group_vars/postgresql/vars.yml приведено в пп. 4.10.1.3 настоящего документа;

4.3.4.1.3 Установить СУБД PostgreSQL 11 с помощью команды:

```
ansible-playbook -i inventories/hosts.yml play-postgresql.yml
-vv --diff -u <имя пользователя> | tee -a install-infra-postgresql.$(date
'+%Y%m%d_%H%M%S').log
```

4.3.4.2. Порядок установки и настройки СУБД PostgreSQL 10 (ОС Альт 8 СП)

Для установки и настройки СУБД PostgreSQL 10 необходимо выполнить следующие действия:

4.3.4.2.1 Установить на сервера БД работающий под управлением ОС Альт 8 СП

с помощью последовательного выполнения команд следующие пакеты:

```
sudo apt-get -y install jq
sudo apt-get -y install unzip
sudo apt-get -y install postgresql10
sudo apt-get -y install postgresql10-server
sudo apt-get -y install postgresql10-contrib
sudo apt-get -y install python-module-pkginfo
```

4.3.4.2.2 В конфигурационных файлах СУБД `pg_hba.conf` и `postgresql.conf` задать следующие параметры:

- тип соединения, диапазон IP-адресов клиентов БД;
- имя БД, имя пользователя;
- способ аутентификации клиентов;
- пароль пользователя СУБД в параметре `pg_superuser_password`.

4.3.4.2.3 Инициализировать и запустить СУБД PostgreSQL 10 с помощью следующих команд:

```
sudo /etc/init.d/postgresql initdb
sudo systemctl enable postgresql
sudo systemctl start postgresql
```

4.3.4.3. Порядок установки и настройки СУБД Postgres Pro

Для установки и настройки СУБД Postgres Pro необходимо выполнить следующие действия:

4.3.4.3.1 Установить на сервера БД с помощью последовательного выполнения команд следующие пакеты:

- ОС CentOS версии 7 (сервер БД)

```
sudo yum -y install epel-release
sudo yum -y install jq
sudo yum -y install unzip
sudo yum -y install perl-libs
sudo yum -y install libxslt
sudo yum -y install postgresql-libs
sudo yum -y install libicu
sudo yum -y install python-psycopg2
```

- ОС Альт 8 СП (сервер БД)

```
sudo apt-get -y install jq
sudo apt-get -y install unzip
sudo apt-get -y install python-module-pkginfo
```

4.3.4.3.2 Установить и инициализировать СУБД Postgres Pro

Установка и инициализация СУБД Postgres Pro осуществляется в соответствии с эксплуатационной документацией на СУБД. После установки СУБД необходимо назначить пароль для пользователя postgres и создать на время установки символическую ссылку (symlink) для сокета PostgreSQL PRO с помощью следующих команд:

```
psql -U postgres
ALTER USER postgres with PASSWORD 'пароль';
exit
sudo ln -s /tmp /var/run/postgresql
```

4.3.4.3.3 В конфигурационных файлах СУБД pg_hba.conf и postgresql.conf задать следующие параметры:

- тип соединения, диапазон IP-адресов клиентов БД;
- имя БД, имя пользователя;
- способ аутентификации клиентов;
- пароль пользователя СУБД в параметре pg_superuser_password.

4.3.4.3.4 Установить расширение pg_partman с помощью команды:

- ОС CentOS версии 7

```
sudo rpm -ivh pg_partman11-v4.3.0-1.el7.x86_64.rpm
```

- ОС Альт 8 СП

```
sudo rpm -ivh pg_partman11-v4.3.0-1.alt.x86_64.rpm
```

Указанные rpm-пакеты находятся на DVD с компонентами среды функционирования ППО в каталоге /binary/postgresql/.

4.3.4.3.5 Перезапустить сервис СУБД Postgres Pro с помощью команды:

```
sudo systemctl restart postgrespro-std-11
```

4.4. Порядок установки ППО

Для установки ППО необходимо выполнить следующие действия:

4.4.1. Скопировать файл `installer_variant<номер варианта поставки>.sh` (`installer_variant1.sh`, или `installer_variant2.sh`, или `installer_variant3.sh`), из каталога `/server` на DVD с загрузочными модулями ППО, на ПЭВМ (сервер приложений или управляющую ПЭВМ).

4.4.2. Назначить пользователю право на исполнение файла `installer_variant<номер варианта поставки>.sh` с помощью команды:

```
chmod +x installer_variant<номер варианта поставки>.sh
```

Например,

```
chmod +x installer_variant1.sh
```

4.4.3. Запустить `installer.sh` с помощью команды:

```
./installer.sh
```

4.4.4. Ознакомиться с лицензионным соглашением и принять его (Рисунок 43)

```
[omp@ocs-app ~]$ ./installer_variant1.sh
```

```
ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ  
ВАЖНО! ПЕРЕД ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, К КОТОРОМУ  
ПРИЛАГАЕТСЯ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ  
(ДАЛЕЕ ПО ТЕКСТУ – «ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ» ИЛИ «ЛИЦЕНЗИЯ»),  
ПОЖАЛУЙСТА, ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ НИЖЕСЛЕДУЮЩИЕ УСЛОВИЯ. ЕСЛИ ВЫ  
НЕ СОГЛАШАЕТЕСЬ С УСЛОВИЯМИ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ, ТО  
ВЫ НЕ ИМЕЕТЕ ПРАВА ИСПОЛЬЗОВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ В КАКИХ-ЛИБО  
ЦЕЛЯХ.
```

1. ОПРЕДЕЛЕНИЯ

```
«Правообладатель» – общество с ограниченной ответственностью «Открытая мобильная платформа»  
(ООО «Открытая мобильная платформа»), 420500, Республика Татарстан, Верхнеуслонский район, г.  
Иннополис, ул. Университетская, д. 7, офис 59, ОГРН 1161690087020.  
«ПО» – прикладное программное обеспечение «Аврора Центр», состоящее из прикладного программного  
обеспечения «Аврора Центр: Маркет» и прикладного программного обеспечения «Аврора Центр: Платформа  
управления», подробное описание функциональных возможностей которого содержатся в Документации.  
«Документация» – относящиеся к ПО сопроводительные материалы, в том числе Руководство  
Пользователя, Руководство Администратора, которые принадлежат Правообладателю.  
«Устройство» – это аппаратная система (физическая или виртуальная) со встроенным запоминающим  
устройством, на которых может быть запущено ПО.
```

Рисунок 43

⁹ Варианты поставки ППО описаны в пункте 5.1.1 «Формуляра».

Для того чтобы принять лицензионное соглашение, необходимо после вопроса «Вы принимаете условия лицензии (y/n)?» ввести «y».

В результате в каталоге с файлом `installer.sh` будет создан каталог `install-<версия ППО>`. Например, `install-2.2.1`.

4.4.5. Выполнить настройку ППО (подсистем ППО)

Для настройки ППО необходимо выполнить следующие действия:

4.4.5.1. Перейти в созданный каталог (каталог: `/install-<версия ППО>/install-apps/`) и отредактировать конфигурационные файлы `hosts.yml` для каждой из подсистем ППО, указав адреса серверов (имена хостов), на которые будут установлены подсистемы ППО.

Конфигурационный файл `inventories-auth/deploy/hosts.yml` может иметь следующий вид:

```
---
  all:
    children:
      app:
        hosts:
          ocs-app.local:
      postgresql:
        children:
          postgresql_masters:
            hosts:
              ocs-app.local:
      nginx:
        children:
          app:
      consul:
        children:
          consul_servers:
```

```
    children:
      app:
        consul_agents:
consul-template:
  children:
    app:
nats_streaming_server:
  hosts:
    ocs-app.local:
redis:
  children:
    redis_masters:
      hosts:
        ocs-app.local:
    sentinel:
      hosts:
        ocs-app.local:
```

Описание параметров конфигурационного файла `inventories-auth/deploy/hosts.yml` приведено в пп. 4.10.2.1 настоящего документа.

Конфигурационный файл `inventories-appstore/deploy/hosts.yml` может иметь следующий вид:

```
---
all:
  children:
    app:
      hosts:
        ocs-app.local:
  postgresql:
    children:
      postgresql_masters:
```

```
        hosts:
            ocs-app.local:
nginx:
    children:
        app:
consul:
    children:
        consul_servers:
            children:
                app:
        consul_agents:
consul-template:
    children:
        app:
nats_streaming_server:
    hosts:
        ocs-app.local:
redis:
    children:
        redis_masters:
            hosts:
                ocs-app.local:
        sentinel:
            hosts:
                ocs-app.local:
```

Описание параметров конфигурационного файла `inventories-appstore/deploy/hosts.yml` приведено в пп. 4.10.2.3 настоящего документа.

Конфигурационный файл `inventories-emm/deploy/hosts.yml` может иметь следующий вид:

```
---
    all:
```

```
children:
  app:
    hosts:
      ocs-app.local:
postgresql:
  children:
    postgresql_masters:
      hosts:
        ocs-app.local:
nginx:
  children:
    app:
consul:
  children:
    consul_servers:
      children:
        app:
    consul_agents:
consul-template:
  children:
    app:
nats_streaming_server:
  hosts:
    ocs-app.local:
redis:
  children:
    redis_masters:
      hosts:
        ocs-app.local:
    sentinel:
      hosts:
        ocs-app.local:
```

Описание параметров конфигурационного файла `inventories-
emm/deploy/hosts.yml` приведено в пп. 4.10.2.6 настоящего документа.

Конфигурационный файл `inventories-pkgrepo/deploy/hosts.yml` может иметь следующий вид:

```
---  
all:  
  children:  
    app:  
      hosts:  
        ocs-app.local:  
    postgresql:  
      children:  
        postgresql_masters:  
          hosts:  
            ocs-app.local:  
    nginx:  
      children:  
        app:  
    consul:  
      children:  
        consul_servers:  
          children:  
            app:  
        consul_agents:  
    consul-template:  
      children:  
        app:  
    nats_streaming_server:  
      hosts:  
        ocs-app.local:  
    redis:
```

```
children:
  redis_masters:
    hosts:
      ocs-app.local:
  sentinel:
    hosts:
      ocs-app.local:
```

Описание параметров конфигурационного файла `inventories-pkgrepo/deploy/hosts.yml` приведено в пп. 4.10.2.8 настоящего документа.

4.4.5.2. Отредактировать конфигурационные файлы `/deploy/group_vars/all/vars.yml` каждой подсистемы ППО:

- для ПБ: `inventories-auth/deploy/group_vars/all/vars.yml`;
- для ПМ: `inventories-appstore/deploy/group_vars/all/vars.yml`;
- для ПУ: `inventories-emm/deploy/group_vars/all/vars.yml`;
- для ПУСП: `inventories-pkgrepo/deploy/group_vars/all/vars.yml`.

В данных конфигурационных файлах необходимо задать, либо поменять предустановленные значения:

- доменное имя для межсервисного взаимодействия в рамках одной ноды (узла сервера) должно иметь значение `local` (`domain: local`);
- параметры подключения подсистем ППО к БД;
- пароль суперпользователя СУБД `Postgresql`, который был задан при установке СУБД;
- токен авторизации, заданный при установке сервиса гарантированной доставки сообщений `Nats Streaming Server`;
- пароль доступа к СУБД `Redis`, заданный при ее установке.
- `*_client_secret` – секретные ключи клиентов (сервисов).

При использовании СУБД PostgreSQL 10 необходимо удалить расширение `pg_partman_bgw` в секции `postgresql.extensions`.

Конфигурационные файлы `/deploy/group_vars/all/vars.yml` могут иметь следующий вид:

```
project_name: "appstore"

logger_level: "error"
gateway_gin_log_enabled: true

download_mode: "httplocal"
repository_dir: "{{ playbook_dir }}/repository"

insecure_uri: false

postgresql:
  dbname: appstore
  port: 5432
  user: appstore
  password: ocs
  extensions: ["pg_partman_bgw", "pg_trgm", "pg_stat_statements"]
postgres_password: "postgres"

nats:
  auth_token: FF12fddgdhFLL

redis_password: "@rTT9089087fslk"
domain: local

session_remember_for: "1h"
session_renew_timeout: "1m"

auth_public_address: "https://demo-ocs.ompccloud.ru"
```

```
auth_admin_address: "https://demo-ocs.ompcloud.ru"  
aps_admin_address: "https://demo-ocs.ompcloud.ru"  
aps_dev_address: "https://demo-ocs.ompcloud.ru"  
emm_admin_address: "https://demo-ocs.ompcloud.ru"
```

```
auth_public_basepath: "/auth/public"  
auth_admin_basepath: "/auth/admin"  
aps_admin_basepath: "/appstore/admin"  
aps_dev_basepath: "/appstore/dev"  
emm_admin_basepath: "/emm/admin"
```

```
auth_public_uri: "{{ auth_public_address }}{{ auth_public_basepath  
}}"
```

```
auth_admin_uri: "{{ auth_admin_address }}{{ auth_admin_basepath }}"  
aps_admin_uri: "{{ aps_admin_address }}{{ aps_admin_basepath }}"  
aps_dev_uri: "{{ aps_dev_address }}{{ aps_dev_basepath }}"  
emm_admin_uri: "{{ emm_admin_address }}{{ emm_admin_basepath }}"  
insecure_uri: true
```

```
aps_client_cdn_uri: "{{ aps_client_uri }}"
```

```
aps_admin_cdn_uri: "{{ aps_admin_uri }}"
```

```
aps_dev_cdn_uri: "{{ aps_dev_uri }}"
```

```
aps_dev_console_client_secret: "nevertellanyone"
```

```
aps_admin_console_client_secret: "nevertellanyone"
```

```
aurora_market_client_secret: "nevertellanyone"
```

```
appstore_integration_account_client_secret: "nevertellanyone"
```

Описание параметров конфигурационных файлов

/deploy/group_vars/all/vars.yml приведено в пп. 4.10.2.2, 4.10.2.4, 4.10.2.7, 4.10.2.9.

4.4.5.3. В случае если каналы связи защищаются с использованием СКЗИ (используется протокол HTTPS), в секции `config.extra_config.git_omprussia_ru/auth/krakendrp` шаблонов конфигурационных файлах шлюзов доступа `ocs-appstore-admin-api-gw`, `ocs-appstore-dev-api-gw`, `ocs-auth-admin-api-gw`, `ocs-emm-admin-api-gw` (файлы: `inventories-auth/config/gateways/ocs-auth-admin-api-gw/ocs-auth-admin-api-gw.json.j2`, `inventories-appstore/config/gateways/ocs-appstore-admin-api-gw/ocs-appstore-admin-api-gw.json.j2`, `inventories-appstore/config/gateways/ocs-appstore-dev-api-gw/ocs-appstore-dev-api-gw.json.j2`, `inventories-emm/config/gateways/ocs-emm-admin-api-gw/ocs-emm-admin-api-gw.json.j2`) задать для параметра `same_site_mode` значение `none`:

```
"same_site_mode": "none"
```

В данном пункте приведен перечень модулей (конфигурационных файлов) ППО для варианта поставки №1. Для других вариантов поставки часть модулей (конфигурационных файлов) ППО будет отсутствовать

4.4.5.4. В секциях `system` и `cookie` конфигурационных файлов `inventories-auth\config\services\ocs-auth-server-admin\ocs-auth-server-admin.yml.j2` и `inventories-auth\config\services\ocs-auth-server-public\ocs-auth-server-public.yml.j2` поменять предустановленные значения паролей, используемых для защиты критичной информации (например, `cookie` сессии).

4.4.6. Установить Сервер приложений ПБ

Для установки Сервера приложений ПБ необходимо выполнить следующие действия:

4.4.6.1. Создать БД, схемы БД и назначить права доступа БД ПБ, выполнив следующую команду:

– СУБД PostgreSQL

```
ansible-playbook -i inventories-auth/deploy/hosts.yml play-  
postgres-configure.yml -vv --extra-vars "apps=all" -u <имя пользователя>  
| tee -a install-apps-auth-postgres-configure.$(date  
'+%Y%m%d_%H%M%S').log
```

– СУБД Postgres Pro

```
ansible-playbook -i inventories-auth/deploy/hosts.yml play-
postgres-configure.yml -vv --diff --extra-vars "apps=all
postgresql_service=postgrespro-std-11
postgresql_data_dir=/var/lib/pgpro/std-11/data" -u <имя пользователя> |
tee -a install-apps-auth-postgres-configure.$(date '+%Y%m%d_%H%M%S').log
```

4.4.6.2. Установить сервисы (модули) Сервера приложений ПБ и выполнить миграцию БД ПБ с помощью следующей команды:

```
ansible-playbook -i inventories-auth/deploy/hosts.yml play-
systemd-deploy.yml -vv --extra-vars "apps=all" -u <имя пользователя> |
tee -a install-apps-auth-systemd-deploy.$(date '+%Y%m%d_%H%M%S').log
```

4.4.6.3. Зарегистрировать OIDC-клиентов, выполнив следующую команду:

```
ansible-playbook -i inventories-auth/deploy/hosts.yml play-
register-clients.yml -vv --extra-vars "clients=all" -u <имя пользователя>
| tee -a install-apps-auth-register-clients.$(date '+%Y%m%d_%H%M%S').log
```

OIDC-клиентами являются шлюзы доступа и МП

4.4.7. Установить Сервер приложений ПМ

Для установки Сервера приложений ПМ необходимо выполнить следующие действия:

4.4.7.1. Создать БД, схемы БД и назначить права доступа БД ПМ, выполнив следующую команду:

– СУБД PostgreSQL

```
ansible-playbook -i inventories-appstore/deploy/hosts.yml play-
postgres-configure.yml -vv --extra-vars "apps=all" -u <имя пользователя>
| tee -a install-apps-appstore-postgres-configure.$(date
'+%Y%m%d_%H%M%S').log
```

– СУБД Postgres Pro

```
ansible-playbook -i inventories-appstore/deploy/hosts.yml play-  
postgres-configure.yml -vv --diff --extra-vars "apps=all  
postgresql_service=postgrespro-std-11  
postgresql_data_dir=/var/lib/pgpro/std-11/data" -u <имя пользователя> |  
tee -a install-apps-appstore-postgres-configure.$(date  
'+%Y%m%d_%H%M%S').log
```

4.4.7.2. Установить сервисы (модули) Сервера приложений ПМ и выполнить миграцию БД ПМ с помощью следующей команды:

```
ansible-playbook -i inventories-appstore/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=all" -u <имя пользователя> |  
tee -a install-apps-appstore-systemd-deploy.$(date '+%Y%m%d_%H%M%S').log
```

4.4.7.3. Зарегистрировать OIDC-клиентов, выполнив следующую команду:

```
ansible-playbook -i inventories-appstore/deploy/hosts.yml play-  
register-clients.yml -vv --extra-vars "clients=all" -u <имя пользователя>  
| tee -a install-apps-appstore-register-clients.$(date  
'+%Y%m%d_%H%M%S').log
```

4.4.7.4. На Сервере приложений ПМ создать каталог, в котором будут храниться файлы МП (иконки, скриншоты, грм-пакеты), загружаемые разработчиками, либо каталог, к которому будет монтироваться единое файловое хранилище.

В первом случае нужно создать каталог в соответствии с параметром `rootFolderPath` конфигурационного файла `inventories-appstore/config/services/config.yml.j2` ПМ и сделать владельцем данного каталога пользователя `ocs`, под которым работают сервисы ПМ:

```
sudo mkdir -p /ocs/appstore/applications-api  
sudo chown ocs:ocs /ocs/appstore/applications-api
```

Параметры конфигурационного файла inventories-appstore/config/services/config.yml.j2 могут иметь следующий вид:

```
filestorage:
  rootFolderPath: "/ocs/appstore/applications-api"
```

Описание параметров конфигурационного файла inventories-appstore/config/services/config.yml.j2 приведено в пп. 4.10.2.5 настоящего документа.

При использовании единого файлового хранилища для хранения файлов МП на сервере приложений ПМ необходимо создать каталог /ocs и сделать владельцем данного каталога пользователя ocs, под которым работают сервисы ПМ:

```
sudo mkdir -p /ocs
sudo chown ocs:ocs /ocs
```

ВНИМАНИЕ! При эксплуатации ППО в кластерной конфигурации все ноды Сервера приложений ПМ должны иметь доступ к единому файлового хранилищу. Соответственно все ноды Сервера приложений ПМ должны быть настроены на работу с данным файлового хранилищем.

Пример настройки единого файлового хранилища и работы Сервера приложений ПМ (ноды Сервера приложений ПМ) приведен в подразделе 4.6.

4.4.8. Установить Сервер приложений ПУ

Для установки Сервера приложений ПУ необходимо выполнить следующие действия:

4.4.8.1. Создать БД, схемы БД и назначить права доступа БД ПУ, выполнив следующую команду:

– СУБД PostgreSQL

```
ansible-playbook -i inventories-emm/deploy/hosts.yml play-
postgres-configure.yml -vv --extra-vars "apps=all" -u <имя пользователя>
| tee -a install-apps-emm-postgres-configure.$(date
'+%Y%m%d_%H%M%S').log
```

– СУБД Postgres Pro

```
ansible-playbook -i inventories-emm/deploy/hosts.yml play-  
postgres-configure.yml -vv --diff --extra-vars "apps=all  
postgresql_service=postgrespro-std-11  
postgresql_data_dir=/var/lib/pgpro/std-11/data" -u <имя пользователя> |  
tee -a install-apps-emm-postgres-configure.$(date '+%Y%m%d_%H%M%S').log
```

4.4.8.2. Установить сервисы (модули) Сервера приложений ПУ и выполнить миграцию БД ПУ с помощью следующей команды:

```
ansible-playbook -i inventories-emm/deploy/hosts.yml play-systemd-  
deploy.yml -vv --extra-vars "apps=all" -u <имя пользователя> | tee -a  
install-apps-emm-systemd-deploy.$(date '+%Y%m%d_%H%M%S').log
```

4.4.8.3. Зарегистрировать OIDC-клиентов, выполнив следующую команду:

```
ansible-playbook -i inventories-emm/deploy/hosts.yml play-  
register-clients.yml -vv --extra-vars "clients=all" -u <имя пользователя>  
| tee -a install-apps-emm-register-clients.$(date '+%Y%m%d_%H%M%S').log
```

4.4.8.4. Настроить взаимодействие с SMTP-сервером

Для работоспособности функционала по отправке QR-кодов и лог-файлов мобильных устройств на электронную почту, должен быть настроен доступ ПУ к SMTP-серверу. Взаимодействие ПУ с SMTP-сервером может осуществляться с использованием протоколов аутентификации CRAM-MD5 или PLAIN, либо без аутентификации.

Для настройки взаимодействия ППО с SMTP-сервером необходимо в секции smtp конфигурационного файла ПУ (файл: /var/ocs/emm/config.yml) задать требуемые значения.

4.4.9. Установить Сервер приложений ПУСП

Для установки Сервера приложений ПУСП необходимо выполнить следующие действия:

4.4.9.1. Отредактировать конфигурационный файл inventories-pkgrepo/deploy/group_vars/all/vars.yml задав следующее значение параметров pkgrepo_mobile_basepath и pkgrepo_mobile_address:

```
pkgrepo_mobile_basepath: "/pkgrepo/mobile"
```

```
pkgrepo_mobile_address: "http://{{ groups['app'] | first }}"
```

4.4.9.2. Создать БД, схемы БД и назначить права доступа БД ПУСП, выполнив следующую команду:

– СУБД PostgreSQL

```
ansible-playbook -i inventories-pkgrepo/deploy/hosts.yml play-  
postgres-configure.yml -vv --extra-vars "apps=all" -u <имя пользователя>  
| tee -a install-apps-pkgrepo-postgres-configure.$(date  
'+%Y%m%d_%H%M%S').log
```

– СУБД Postgres Pro

```
ansible-playbook -i inventories-pkgrepo/deploy/hosts.yml play-  
postgres-configure.yml -vv --diff --extra-vars "apps=all  
postgresql_service=postgrespro-std-11  
postgresql_data_dir=/var/lib/pgpro/std-11/data" -u <имя пользователя> |  
tee -a install-apps-pkgrepo-postgres-configure.$(date  
'+%Y%m%d_%H%M%S').log
```

4.4.9.3. Установить сервисы (модули) Сервера приложений ПУСП и выполнить миграцию БД ПУСП с помощью следующей команды:

```
ansible-playbook -i inventories-pkgrepo/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=all" -u <имя пользователя> |  
tee -a install-apps-pkgrepo-systemd-deploy.$(date '+%Y%m%d_%H%M%S').log
```

4.4.9.4. Зарегистрировать OIDC-клиентов, выполнив следующую команду:

```
ansible-playbook -i inventories-pkgrepo/deploy/hosts.yml play-  
register-clients.yml -vv --extra-vars "clients=all" -u <имя пользователя>  
| tee -a install-apps-pkgrepo-register-clients.$(date  
'+%Y%m%d_%H%M%S').log
```

4.4.10. Проверить корректность установки и функционирования ППО

Проверка осуществляется в соответствии с подразделом 4.9.

4.5. Адреса веб-консолей

Первоначальный вход в ППО осуществляется с помощью Консоли администратора ПБ и предустановленной учетной записи с ролью Администратор учетных записей:

- логин: admin@omprussia.ru;
- пароль: admin.

При первом входе в ППО необходимо сменить пароль

В таблице (Таблица 9) приведены адреса веб-консолей.

Таблица 9

Веб-консоль	URL-адрес веб-консоли
Консоль администратора ПБ	http://<сервер приложения>:8019
Консоль администратора ПМ	http://<сервер приложения>:8015
Консоль разработчика ПМ	http://<сервер приложения>:8014
Консоль администратора ПУ	http://<сервер приложения>:8011

4.6. Пример настройки единого файлового хранилища

4.6.1. Установить NFS сервер в соответствии с официальной документацией на ОС RedHat приведенной на следующей странице: [https://access.redhat.com/documentation/en-](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/nfs-serverconfig)

[us/red_hat_enterprise_linux/7/html/storage_administration_guide/nfs-serverconfig](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/nfs-serverconfig)

4.6.2. Выполнить монтирование файловой системы NFS к каталогу /ocs с помощью команды:

```
mount example.com:/export/ocsfs /ocs
```

где,

- example.com – имя узла файлового сервера NFS;
- /export/ocsfs – каталог, который экспортирует example.com;
- /ocs – каталог, к которому осуществляется монтирование.

Для проверки корректности монтирования необходимо выполнить команду

```
ls /ocs
```

и убедиться, что полученный список файлов соответствует списку файлов в каталоге `/export/ocsfs` на компьютере `example.com`.

Также выполнить монтирование файловой системы NFS можно путем редактирования файла `/etc/fstab`. Для этого в данный файл необходимо добавить запись следующего вида:

```
example.com:/export/ocsfs /ocs nfs defaults 0 0
```

Редактирование файла `/etc/fstab` должно осуществляться пользователем с правами `root`.

4.6.3. В файловом хранилище создать каталог, в котором будут храниться файлы МП (иконки, скриншоты, rpm-пакеты), загружаемые разработчиками

Каталог нужно создать в соответствии с параметром `rootFolderPath` конфигурационного файла `inventories-appstore/config/services/config.yml.j2` ПМ:

```
mkdir -p /ocs/appstore/applications-api
```

Параметры конфигурационного файла `inventories-appstore/config/services/config.yml.j2` могут иметь следующий вид:

```
config:
  ocs-appstore-applications-api:
    filestorage:
      rootFolderPath: "/ocs/appstore/applications-api"
```

Описание параметров конфигурационного файла `inventories-appstore/config/services/config.yml.j2` приведено в пп. 4.10.2.5 настоящего документа.

4.6.4. В файловом хранилище создать каталог, в котором будут храниться системные пакеты ПУСП:

```
mkdir -p /ocs/pkgrepo
```

Создаваемый каталог должен соответствовать параметрам, заданным в конфигурационном файле `pkgrepo.nginx.conf` веб-сервера `Nginx Web Server`.

4.7. Действия по безопасной установке и настройке средства

Установка, настройка и эксплуатация ППО должна осуществляться в соответствии с эксплуатационной документацией на ППО.

При использовании ППО в государственных информационных системах, не содержащих информации, составляющей государственной тайны 1 класса защищенности, в информационных системах персональных данных 1 уровня защищенности и в автоматизированных системах управления 1 класса защищенности должны быть установлены значения параметров приведенные в таблице (Таблица 10).

Таблица 10

Параметр	Значение
Конфигурационный файл ПБ: /var/ocs/auth/config.yml	
Период времени неиспользования идентификатора (учетной записи) пользователя через которое происходит его блокирование: config.maxAccountInactivityPeriod	не более 45 дней maxAccountInactivityPeriod: 1080h
Минимальная длина пароля: config.passwordSettings.minLength	не менее 8 символов config.passwordSettings.minLength: 8
Алфавит пароля: config.passwordSettings.minDigits config.passwordSettings.minUpperLetters config.passwordSettings.minLowerLetters config.passwordSettings.minSpecialChars	не менее 70 символов minDigits: 1 minUpperLetters: 1 minLowerLetters: 1 minSpecialChars: 1
Максимальное время действия пароля: config.passwordExpirationTime	не более 60 дней passwordExpirationTime: "1440h"
Число последних использованных паролей, которые запрещено использовать пользователями при создании новых паролей:	passwordHistoryDepth: 3

Параметр	Значение
<code>config.passwordHistoryDepth</code>	
Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки: <code>config.failedLoginTries</code>	не более 3 <code>failedLoginTries: 3</code>
Время блокировки учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации: <code>config.failedLoginBlockTime</code>	не менее 15 минут <code>failedLoginBlockTime: "15m"</code>
Количество одновременных сессий для привилегированных учетных записей: <code>config.privilegedSessionsLimit</code>	не более 2-х <code>privilegedSessionsLimit: 2</code>
Время бездействия (неактивности) пользователя через которое осуществляется завершение сеанса пользователя: <code>config.session.rememberFor</code>	не более 5 минут <code>rememberFor: 5m</code>
Конфигурационные файлы ПМ и ПУ: <code>/var/ocs/appstore/config.yml</code> <code>/var/ocs/emm/config.yml</code>	
Время бездействия (неактивности) пользователя через которое осуществляется завершение сеанса пользователя: <code>config.session.rememberFor</code>	не более 5 минут <code>rememberFor: 5m</code>

Более подробное описание параметров конфигурационных файлов `/var/ocs/auth/config.yml`, `/var/ocs/appstore/config.yml` и `/var/ocs/auth/config.yml` приведено в разделе 7 настоящего документа.

4.8. Действия по реализации функций безопасности среды функционирования ППО

4.8.1. Установка, настройка и эксплуатация СЗИ НСД

Эксплуатация ППО и СУБД должна осуществляться в одной из следующих ОС:

- CentOS версии 7 с установленными СЗИ НСД «Dallas Lock Linux», или СЗИ «Secret Net LSP», или СЗИ НСД «Аккорд-Х К»;
- Альт 8 СП.

Установка СЗИ НСД должна осуществляться после установки ППО. После установки СЗИ НСД необходимо повторно назначить пользователям ОС права на выполнение команд от имени суперпользователя root в соответствии с подразделом 4.3.

Установка, настройка и эксплуатация СЗИ НСД и ОС Альт 8 СП должна осуществляться в соответствии с эксплуатационной документацией на СЗИ (ОС).

4.8.2. Меры по межсетевому экранированию

В информационной системе должна осуществляться защита периметра (физических и (или) логических границ) информационной системы с использованием межсетевого экрана требуемого класса защиты.

Межсетевой экран должен пропускать трафик только на внешние порты ППО, приведенные в таблице (Таблица 11), остальной трафик должен быть запрещен.

Таблица 11

Сервис (модуль)	Порт
Auth public API gateway	http://<сервер приложения>:8018
Auth admin API gateway	http://<сервер приложения>:8019
AMM device API gateway	http://<сервер приложения>:8012
AMM admin API gateway	http://<сервер приложения>:8011
Aurora market admin API gateway	http://<сервер приложения>:8015
Aurora market development API gateway	http://<сервер приложения>:8014
Aurora market client API gateway	http://<сервер приложения>:8016
Файловый сервер ПУСП	http://<сервер приложения>:8030

Рекомендуется запретить доступ к ППО привилегированных пользователей из-за пределов контролируемой зоны, запретив доступ к Консоли администратора ПБ. Так же при необходимости можно запретить доступ к остальным веб-консолям. Для этого необходимо запретить трафик на требуемых портах в соответствии с таблицей (Таблица 9)

4.9. Проверка корректности установки и функционирования ППО

Для проверки корректности установки и функционирования ППО, а также среды функционирования ППО в состав поставки компонентов среды функционирования (каталог: install-infra) включена утилита для формирования диагностического отчета.

Диагностический отчет формируется в виде файла в формате HTML и содержит следующие разделы:

- общая информация о статусе сервисов ППО (Рисунок 44);

Diagnostic Report		
Generated on 2020-04-22 22:35:53		
		ocs-app.local
Services Status		
Service name	State	Status
OCS Services		
ocs-appstore-admin-api-gw	running	enabled
ocs-appstore-adminconsole-ui	running	enabled
ocs-appstore-applications-api	running	enabled
ocs-appstore-client-api-gw	running	enabled
ocs-appstore-dev-api-gw	running	enabled
ocs-appstore-devconsole-ui	running	enabled
ocs-appstore-egress-api-gw	running	enabled
ocs-auth-accounts-devices-api	running	enabled
ocs-auth-accounts-users-api	running	enabled
ocs-auth-admin-api-gw	running	enabled
ocs-auth-adminconsole-ui	running	enabled
ocs-auth-audit-api	running	enabled

Рисунок 44

– общая информация о статусе компонентов среды функционирования (Рисунок 45);

System environment		
consul-template.service	running	enabled
consul.service	running	enabled
nats-streaming-server.service	running	enabled
nginx.service	running	enabled
postgresql-11.service	running	enabled
postgresql.service	missed	

Рисунок 45

– разделы, содержащие детальную информацию об отдельных сервисах ППО и компонентах среды функционирования (Рисунок 46).

Nginx Service Proxy

Service name	Upstreams	Virtual server
ocs-appstore-devconsole-ui	1	OK
ocs-appstore-egress-api-gw	1	OK
ocs-appstore-client-api-gw	1	OK
ocs-auth-server-admin	1	OK
ocs-emm-admin-api-gw	1	OK
ocs-appstore-dev-api-gw	1	OK
ocs-auth-server-public-proxy	1	OK
ocs-emm-enrollments-api	1	OK

Рисунок 46

Для формирования диагностического отчета необходимо перейти в каталог с компонентами среды функционирования (каталог: install-infra) и выполнить команду:

```
ansible-playbook play-diagnostic-report.yml -i
inventories/hosts.yml -vv --user <имя пользователя>
```

В результате выполнения команды в каталоге report будет сформирован файл в report.html.

4.10. Описание параметров конфигурационных файлов сценариев установки среды функционирования и ППО

4.10.1. Конфигурационные файлы сценариев установки среды функционирования

4.10.1.1. Инвентарный файл inventories/hosts.yml

В инвентарном файле inventories/hosts.yml задаются адреса серверов приложений и серверов БД, на которые будут установлены компоненты среды функционирования. Описание секций инвентарного файла inventories/hosts.yml приведено в таблице (Таблица 12).

Таблица 12

Секция конфигурационного файла	Описание
all.children.app	Сервера приложений ППО
all.children.postgresql.children.postgresql_masters	СУБД Postgres
all.children.nginx	Балансировщик микросервисов «Nginx Web Server»
all.children.consul	Система обнаружения сервисов «Consul»
all.children.consul-template	Средство управления конфигурациями микросервисов «Consul Template»
all.children.nats_streaming_server	Сервис гарантированной доставки сообщений «Nats Streaming Server»
all.children.redis.children.redis_masters	СУБД Redis для хранения сессий
all.children.redis.children.sentinel	Redis Sentinel обеспечивает высокую доступность СУБД Redis

Файл сценария установки для установки среды функционирования ППО на одном сервере с адресом "ocs-app.local", имеет следующий вид:

```

---
all:
  children:
    app:
      hosts:
        ocs-app.local:
    postgresql:
      children:
        postgresql_masters:
          hosts:
            ocs-app.local:

```

```

nginx:
  children:
    app:
consul:
  children:
    consul_servers:
      children:
        app:
    consul_agents:
consul-template:
  children:
    app:
nats_streaming_server:
  hosts:
    ocs-app.local:
redis:
  children:
    redis_masters:
      hosts:
        ocs-app.local:
    sentinel:
      hosts:
        ocs-app.local:

```

4.10.1.2. Конфигурационный файл установки Nats Streaming Server (файл: [inventories/group_vars/nats_streaming_servers/vars.yml](#))

Описание секций конфигурационного файла приведено в таблице (Таблица 13).

Таблица 13

Секция конфигурационного файла	Описание
nats_token	Токен доступа к Nats Streaming Server

Конфигурационный файл `inventories/group_vars/nats_streaming_server/vars.yml` может иметь следующий вид:

```
nats_token: FF12fddgdhFLL
```

4.10.1.3. Конфигурационный файл СУБД PostgreSQL (файл: [inventories/group_vars/postgresql/vars.yml](#))

Описание секций конфигурационного файла приведено в таблице (Таблица 14).

Таблица 14

Секция конфигурационного файла	Описание
<code>pg_hba_settings.type</code>	Тип подключения
<code>pg_hba_settings.name</code>	Имя подключения
<code>pg_hba_settings.database</code>	Имя БД
<code>pg_hba_settings.address</code>	IP-адрес для подключения
<code>pg_hba_settings.method</code>	Метод аутентификации
<code>pg_superuser_password</code>	Пароль суперпользователя СУБД Postges

Конфигурационный файл `inventories/group_vars/postgresql/vars.yml` может иметь следующий вид:

```
pg_hba_settings:
  - type: local
    name: all
    database: all
    method: trust
  - type: host # Local access
    name: all
    database: all
    address: 127.0.0.1/32
    method: trust
  - type: host # Local access
    name: all
    database: all
    address: ::1/128
    method: trust
  - type: host
    name: all
```

```
database: all
address: <подсеть серверов приложений>
method: md5
```

```
pg_superuser_password: postgres
```

4.10.1.4. Конфигурационный файл СУБД Redis (файл: inventories/group_vars/redis/vars.yml)

Описание секций конфигурационного файла приведено в таблице (Таблица 15).

Таблица 15

Секция конфигурационного файла	Описание
redis_password	Пароль доступа к СУБД Redis

Конфигурационный файл inventories/group_vars/redis/vars.yml может иметь следующий вид:

```
redis_password:"@rTT9089087fs1k"
```

4.10.2. Конфигурационные файлы сценариев установки подсистем ППО

4.10.2.1. Конфигурационный файл ПБ inventories-auth/deploy/hosts.yml

В данном конфигурационном файле задаются адреса компонентов ПБ. Описание секций конфигурационного файла приведено в таблице (Таблица 16).

Таблица 16

Секция конфигурационного файла	Описание
all.children.app	Сервера приложений ППО
all.children.postgresql.children.postgresql_masters	СУБД Postgres
all.children.nginx	Балансировщик микросервисов «Nginx Web Server»
all.children.consul	Система обнаружения сервисов «Consul»

Секция конфигурационного файла	Описание
all.children.consul-template	Средство управления конфигурациями микросервисов «Consul Template»
all.children.nats_streaming_server	Сервис гарантированной доставки сообщений «Nats Streaming Server»
all.children.redis.children.redis_masters	СУБД Redis для хранения сессий
all.children.redis.children.sentinel	Redis Sentinel обеспечивает высокую доступность СУБД Redis

Конфигурационный файл `inventories-auth/deploy/hosts.yml` может иметь следующий вид:

```

---
all:
  children:
    app:
      hosts:
        ocs-app.local:
    postgresql:
      children:
        postgresql_masters:
          hosts:
            ocs-app.local:
    nginx:
      children:
        app:
    consul:
      children:
        consul_servers:
          children:
            app:

```

```

    consul_agents:
consul-template:
  children:
    app:
nats_streaming_server:
  hosts:
    ocs-app.local:
redis:
  children:
    redis_masters:
      hosts:
        ocs-app.local:
    sentinel:
      hosts:
        ocs-app.local:

```

4.10.2.2. Конфигурационный файл ПБ inventories-auth/deploy/group_vars/all/vars.yml

В данном конфигурационном файле задаются параметры взаимодействия ПБ с СУБД PostgreSQL, СУБД Redis и Nats Streaming Server. Описание секций конфигурационного файла приведено в таблице (Таблица 17).

Таблица 17

Секция конфигурационного файла	Описание
project_name	Имя подсистемы
logger_level	Уровень логирования
gateway_gin_log_enabled	Включение логирования запросов на шлюзах доступа (true – логирование включено, false – логирование выключено)
download_mode	Режим получения бинарных файлов подсистемы при развертывании ППО. Возможные значения: http, httplocal, local

Секция конфигурационного файла	Описание
repository_dir	Локальный репозиторий с бинарными файлами ППО для режимов httplocal и local
postgresql.dbname	Имя БД
postgresql.port	Порт
postgresql.user	Имя пользователя
postgresql.password	Пароль
postgresql.extensions	Расширения
postgres_password	Пароль суперпользователя СУБД PostgreSQL
nats.auth_token	Токен доступа, установленный при развертывании Nats Streaming Server
redis_password	Пароль от СУБД Redis
session_remember_for	Время бездействия (неактивности) пользователя через которое осуществляется завершение сеанса пользователя
session_renew_timeout	Время, через которое происходит продление сессии пользователя между двумя активностями
auth_public_address	Адрес Консоли входа пользователей
auth_admin_address	Адрес Консоли администратора ПБ
aps_admin_address	Адрес Консоли администратора ПМ
aps_dev_address	Адрес Консоли разработчика ПМ
emm_admin_address	Адрес Консоли администратора ПУ
auth_public_basepath	basepath Консоли входа пользователей
auth_admin_basepath	basepath Консоли администратора ПБ
aps_admin_basepath	basepath Консоли администратора ПМ
aps_dev_basepath	basepath Консоли разработчика ПМ
emm_admin_basepath	basepath Консоли администратора ПУ
auth_public_url	Адрес Консоли входа пользователей с учетом basepath
auth_admin_url	Адрес Консоли администратора ПБ с учетом basepath
aps_admin_url	Адрес Консоли администратора ПМ с учетом basepath

Секция конфигурационного файла	Описание
aps_dev_url	Адрес Консоли разработчика ПМ с учетом basepath
emm_admin_url	Адрес Консоли администратора ПУ с учетом basepath
insecure_uri	Протокол взаимодействия с модулями OIDC provider public API и OIDC provider admin API
allow_termination_from	Адреса подсетей (или хостов), из которых разрешен трафик в формате: x.x.x.x/x. Например, 10.189.200.0/24 (для подсетей); 10.189.200.1/32 (для хостов).
auth_admin_console_client_secret	Секретный ключ OIDC-клиента (Auth admin API gateway)
domain	Служебный домен для межсервисного взаимодействия
install_dir	Путь к каталогу с бинарными файлами ПБ в локальном репозитории

Конфигурационный файл inventories-auth/deploy/group_vars/all/vars.yml может иметь следующий вид:

```
project_name: "auth"

logger_level: "debug"
gateway_gin_log_enabled: true

download_mode: "httplocal"
repository_dir: "{{ playbook_dir }}/repository"

postgresql:
  dbname: auth
  port: 5432
  user: auth
  password: ocs
  extensions: ["pg_partman_bgw", "pg_trgm", "pg_stat_statements"]
postgresql_password: "postgres"
```

```
nats:
  auth_token: "FF12fddgdhFLL"

redis_password: "@rTT9089087fslk"

session_remember_for: "24h"
session_renew_timeout: "1m"

auth_public_address: "http://{{ groups['app'] | first }}:8018"
auth_admin_address: "http://{{ groups['app'] | first }}:8019"
aps_admin_address: "http://{{ groups['app'] | first }}:8015"
aps_dev_address: "http://{{ groups['app'] | first }}:8014"
emm_admin_address: "http://{{ groups['app'] | first }}:8011"

auth_public_basepath: ""
auth_admin_basepath: ""
aps_admin_basepath: ""
aps_dev_basepath: ""
emm_admin_basepath: ""

auth_public_uri: "{{ auth_public_address }}{{ auth_public_basepath
}}"
auth_admin_uri: "{{ auth_admin_address }}{{ auth_admin_basepath }}"
aps_admin_uri: "{{ aps_admin_address }}{{ aps_admin_basepath }}"
aps_dev_uri: "{{ aps_dev_address }}{{ aps_dev_basepath }}"
emm_admin_uri: "{{ emm_admin_address }}{{ emm_admin_basepath }}"

insecure_uri: true

allow_termination_from:
- 10.189.200.0/24
- 10.189.20.0/24
```

```
auth_admin_console_client_secret:
"7dd7c204aa4f6192e70fad5642d3755"
```

```
download_mode: "local"
domain: "local"
install_dir: "binary/auth"
```

4.10.2.3. Конфигурационный файл ПМ [inventories-appstore/deploy/hosts.yml](#)

В данном конфигурационном файле задаются адреса компонентов ПМ. Описание секций конфигурационного файла приведено в таблице (Таблица 18).

Таблица 18

Секция конфигурационного файла	Описание
all.children.app	Сервера приложений ППО
all.children.postgresql.children.postgresql_masters	СУБД Postgres
all.children.nginx	Балансировщик микросервисов «Nginx Web Server»
all.children.consul	Система обнаружения сервисов «Consul»
all.children.consul-template	Средство управления конфигурациями микросервисов «Consul Template»
all.children.nats_streaming_server	Сервис гарантированной доставки сообщений «Nats Streaming Server»
all.children.redis.children.redis_masters	СУБД Redis для хранения сессий
all.children.redis.children.sentinel	Redis Sentinel обеспечивает высокую доступность СУБД Redis

Конфигурационный файл `inventories-appstore/deploy/hosts.yml` может иметь следующий вид:

```
---
  all:
    children:
      app:
        hosts:
          ocs-app.local:
      postgresql:
        children:
          postgresql_masters:
            hosts:
              ocs-app.local:
      nginx:
        children:
          app:
      consul:
        children:
          consul_servers:
            children:
              app:
          consul_agents:
      consul-template:
        children:
          app:
      nats_streaming_server:
        hosts:
          ocs-app.local:
      redis:
        children:
          redis_masters:
```

```

hosts:
  ocs-app.local:
sentinel:
  hosts:
    ocs-app.local:

```

4.10.2.4. Конфигурационный файл ПМ inventories-appstore/deploy/group_vars/all/vars.yml

В данном конфигурационном файле задаются параметры взаимодействия ПМ с СУБД PostgreSQL, СУБД Redis и Nats Streaming Server. Описание секций конфигурационного файла приведено в таблице (Таблица 19).

Таблица 19

Секция конфигурационного файла	Описание
project_name	Имя подсистемы
logger_level	Уровень логирования
gateway_gin_log_enabled	Включение логирования запросов на шлюзах доступа (true – логирование включено, false – логирование выключено)
download_mode	Режим получения бинарных файлов подсистемы при развертывании ППО. Возможные значения: http, httplocal, local
repository_dir	Локальный репозиторий с бинарными файлами ППО для режимов httplocal и local
postgresql.dbname	Имя БД
postgresql.port	Порт
postgresql.user	Имя пользователя
postgresql.password	Пароль
postgresql.extensions	Расширения
postgres_password	Пароль суперпользователя СУБД PostgreSQL
nats.auth_token	Токен доступа, установленный при развертывании Nats Streaming Server

Секция конфигурационного файла	Описание
redis_password	Пароль от СУБД Redis
session_remember_for	Время бездействия (неактивности) пользователя через которое осуществляется завершение сеанса пользователя
session_renew_timeout	Время, через которое происходит продление сессии пользователя между двумя активностями
auth_public_address	Адрес Консоли входа пользователей
auth_admin_address	Адрес Консоли администратора ПБ
aps_admin_address	Адрес Консоли администратора ПМ
aps_dev_address	Адрес Консоли разработчика ПМ
aps_client_address	Адрес шлюза доступа для обработки запросов МП «Аврора Маркет»
emm_admin_address	Адрес Консоли администратора ПУ
auth_public_basepath	basepath Консоли входа пользователей
auth_admin_basepath	basepath Консоли администратора ПБ
aps_admin_basepath	basepath Консоли администратора ПМ
aps_dev_basepath	basepath Консоли разработчика ПМ
aps_client_basepath	basepath шлюза доступа для обработки запросов МП «Аврора Маркет»
emm_admin_basepath	basepath Консоли администратора ПУ
auth_public_url	Адрес Консоли входа пользователей с учетом basepath
auth_admin_url	Адрес Консоли администратора ПБ с учетом basepath
aps_admin_url	Адрес Консоли администратора ПМ с учетом basepath
aps_dev_url	Адрес Консоли разработчика ПМ с учетом basepath
aps_client_uri	Адрес шлюза доступа для обработки запросов МП Аврора Маркет с учетом basepath
emm_admin_url	Адрес Консоли администратора ПУ с учетом basepath

Секция конфигурационного файла	Описание
<code>insecure_uri</code>	Протокол взаимодействия с модулями OIDC provider public API и OIDC provider admin API
<code>aps_dev_console_client_secret</code>	Секретный ключ OIDC-клиента (Aurora market development API gateway)
<code>aps_admin_console_client_secret</code>	Секретный ключ OIDC-клиента (Aurora market admin API gateway)
<code>aurora_market_client_secret</code>	Секретный ключ OIDC-клиента (МП «Аврора Маркет»)
<code>appstore_integration_account_client_secret</code>	Секретный ключ OIDC-клиента (Aurora market egress API gateway)
<code>domain</code>	Служебный домен для межсервисного взаимодействия
<code>install_dir</code>	Путь к каталогу с бинарными файлами ПБ в локальном репозитории

Конфигурационный файл `inventories-appstore/deploy/group_vars/all/vars.yml` может иметь следующий вид:

```
project_name: "appstore"

logger_level: "debug"
gateway_gin_log_enabled: true

download_mode: "httplocal"
repository_dir: "{{ playbook_dir }}/repository"

insecure_uri: true

postgresql:
  dbname: appstore
  port: 5432
  user: appstore
  password: ocs
```

```
extensions: ["pg_partman_bgw", "pg_trgm", "pg_stat_statements"]
postgres_password: "postgres"

nats:
  auth_token: FF12fddgdhFLL

redis_password: "@rTT9089087fslk"

session_remember_for: "24h"
session_renew_timeout: "1m"

auth_public_address: "http://{{ groups['app'] | first }}:8018"
auth_admin_address: "http://{{ groups['app'] | first }}:8019"
aps_admin_address: "http://{{ groups['app'] | first }}:8015"
aps_dev_address: "http://{{ groups['app'] | first }}:8014"
aps_client_address: "http://{{ groups['app'] | first }}:8016"
emm_admin_address: "http://{{ groups['app'] | first }}:8011"

auth_public_basepath: ""
auth_admin_basepath: ""
aps_admin_basepath: ""
aps_dev_basepath: ""
aps_client_basepath: ""
emm_admin_basepath: ""

auth_public_uri: "{{ auth_public_address }}{{ auth_public_basepath
}}"
auth_admin_uri: "{{ auth_admin_address }}{{ auth_admin_basepath }}"
aps_admin_uri: "{{ aps_admin_address }}{{ aps_admin_basepath }}"
aps_dev_uri: "{{ aps_dev_address }}{{ aps_dev_basepath }}"
aps_client_uri: "{{ aps_client_address }}{{ aps_client_basepath }}"
emm_admin_uri: "{{ emm_admin_address }}{{ emm_admin_basepath }}"

aps_client_cdn_uri: "{{ aps_client_uri }}"
aps_admin_cdn_uri: "{{ aps_admin_uri }}"
```

```
aps_dev_cdn_uri: "{{ aps_dev_uri }}"

aps_dev_console_client_secret: "nevertellanyone"
aps_admin_console_client_secret: "nevertellanyone"
aurora_market_client_secret: "nevertellanyone"
appstore_integration_account_client_secret: "nevertellanyone"

download_mode: "local"
domain: "local"
install_dir: "binary/appstore"
```

4.10.2.5. Конфигурационный файл ПМ [inventories-appstore/config/services/config.yml.j2](#)

В данном конфигурационном файле необходимо задать путь к каталогу, в котором будут храниться файлы МП, загружаемые разработчиками:

- иконки;
- скриншоты;
- загрузочные модули (rpm-пакеты).

Путь к каталогу задается в секции `config.ocs-appstore-applications-api.filestorage.rootFolderPath`.

Секция `config.ocs-appstore-applications-api.filestorage.rootFolderPath` может иметь следующий вид:

```
config:
  ocs-appstore-applications-api:
    filestorage:
      rootFolderPath: "/ocs/appstore/applications-api"
```

4.10.2.6. Конфигурационный файл ПУ [inventories-emm/deploy/hosts.yml](#)

В данном конфигурационном файле задаются адреса компонентов подсистемы ПУ. Описание секций конфигурационного файла приведено в таблице (Таблица 20).

Таблица 20

Секция конфигурационного файла	Описание
all.children.app	Сервера приложений ППО
all.children.postgresql.children.postgresql_masters	СУБД Postgres
all.children.nginx	Балансировщик микросервисов «Nginx Web Server»
all.children.consul	Система обнаружения сервисов «Consul»
all.children.consul-template	Средство управления конфигурациями микросервисов «Consul Template»
all.children.nats_streaming_server	Сервис гарантированной доставки сообщений «Nats Streaming Server»
all.children.redis.children.redis_masters	СУБД Redis для хранения сессий
all.children.redis.children.sentinel	Redis Sentinel обеспечивает высокую доступность СУБД Redis

Конфигурационный файл `inventories-emm/deploy/hosts.yml` может иметь следующий вид:

```

---
all:
  children:
    app:
      hosts:
        ocs-app.local:
    postgresql:
      children:
        postgresql_masters:
          hosts:
            ocs-app.local:

```

```
nginx:
  children:
    app:
consul:
  children:
    consul_servers:
      children:
        app:
    consul_agents:
consul-template:
  children:
    app:
nats_streaming_server:
  hosts:
    ocs-app.local:
redis:
  children:
    redis_masters:
      hosts:
        ocs-app.local:
    sentinel:
      hosts:
        ocs-app.local:
```

4.10.2.7. Конфигурационный файл ПУ `inventories- emm/deploy/group_vars/all/vars.yml`

В данном конфигурационном файле задаются параметры взаимодействия ПУ с СУБД PostgreSQL, СУБД Redis и Nats Streaming Server. Описание секций конфигурационного файла приведено в таблице (Таблица 21).

Таблица 21

Секция конфигурационного файла	Описание
<code>project_name</code>	Имя подсистемы
<code>logger_level</code>	Уровень логирования
<code>gateway_gin_log_enabled</code>	Включение логирования запросов на шлюзах доступа (<code>true</code> – логирование включено, <code>false</code> – логирование выключено)
<code>download_mode</code>	Режим получения бинарных файлов подсистемы при развертывании ППО. Возможные значения: <code>http</code> , <code>httplocal</code> , <code>local</code>
<code>repository_dir</code>	Локальный репозиторий с бинарными файлами ППО для режимов <code>httplocal</code> и <code>local</code>
<code>postgresql.dbname</code>	Имя БД
<code>postgresql.port</code>	Порт
<code>postgresql.user</code>	Имя пользователя
<code>postgresql.password</code>	Пароль
<code>postgresql.extensions</code>	Расширения
<code>postgres_password</code>	Пароль суперпользователя СУБД PostgreSQL
<code>nats.auth_token</code>	Токен доступа, установленный при развертывании Nats Streaming Server
<code>redis_password</code>	Пароль от СУБД Redis
<code>session_remember_for</code>	Время бездействия (неактивности) пользователя через которое осуществляется завершение сеанса пользователя
<code>session_renew_timeout</code>	Время, через которое происходит продление сессии пользователя между двумя активностями

Секция конфигурационного файла	Описание
auth_public_address	Адрес Консоли входа пользователей
auth_admin_address	Адрес Консоли администратора ПБ
aps_admin_address	Адрес Консоли администратора ПМ
aps_market_address	Адрес шлюза доступа для обработки запросов МП «Аврора Маркет»
emm_admin_address	Адрес Консоли администратора ПУ
emm_mobile_address	Адрес шлюза доступа для обработки запросов МП «Аврора Центр»
pkgrepo_admin_address	Адрес ПУСП
auth_public_basepath	basepath Консоли входа пользователей
auth_admin_basepath	basepath Консоли администратора ПБ
aps_admin_basepath	basepath Консоли администратора ПМ
aps_market_basepath	basepath шлюза доступа для обработки запросов МП «Аврора Маркет»
emm_admin_basepath	basepath Консоли администратора ПУ
emm_mobile_basepath	basepath шлюза доступа для обработки запросов МП «Аврора Центр»
pkgrepo_admin_basepath	basepath ПУСП
auth_public_url	Адрес Консоли входа пользователей с учетом basepath
auth_admin_url	Адрес Консоли администратора ПБ с учетом basepath
aps_admin_url	Адрес Консоли администратора ПМ с учетом basepath
aps_market_uri	Адрес шлюза доступа для обработки запросов МП «Аврора Маркет» с учетом basepath
emm_admin_url	Адрес Консоли администратора ПУ с учетом basepath
emm_mobile_uri	Адрес шлюза доступа для обработки запросов МП «Аврора Центр» с учетом basepath
emm_admin_cdn_uri	Путь к статическому контенту (файлам МП, системным пакетам) при использовании cdn

Секция конфигурационного файла	Описание
emm_mobile_cdn_uri	Путь к статическому контенту (файлам МП, системным пакетам) при использовании cdn
insecure_uri	Протокол взаимодействия с модулями OIDC provider public API и OIDC provider admin API
emm_admin_console_client_secret	Секретный ключ OIDC-клиента (AMM admin API gateway)
aurora_mobility_management_client_secret	Секретный ключ OIDC-клиента (МП «Аврора Центр»)
emm_integration_account_client_secret	Секретный ключ OIDC-клиента (AMM egress API gateway)
domain	Служебный домен для межсервисного взаимодействия
install_dir	Путь к каталогу с бинарными файлами ПБ в локальном репозитории

Конфигурационный файл `inventories-emm/deploy/group_vars/all/vars.yml`

может иметь следующий вид:

```
project_name: "emm"

logger_level: "debug"
gateway_gin_log_enabled: true

download_mode: "httplocal"
repository_dir: "{{ playbook_dir }}/repository"

postgresql:
  dbname: emm
  port: 5432
  user: emm
  password: ocs
  extensions: ["pg_partman_bgw", "pg_stat_statements"]
  postgres_password: "postgres"
```

```
nats:
  auth_token: FF12fddgdhFLL

redis_password: "@rTT9089087fslk"

session_remember_for: "24h"
session_renew_timeout: "1m"

auth_public_address: "http://{{ groups['app'] | first }}:8018"
auth_admin_address: "http://{{ groups['app'] | first }}:8019"
aps_admin_address: "http://{{ groups['app'] | first }}:8015"
aps_market_address: "http://{{ groups['app'] | first }}:8016"
emm_admin_address: "http://{{ groups['app'] | first }}:8011"
emm_mobile_address: "http://{{ groups['app'] | first }}:8012"
pkgrepo_admin_address: "http://{{ groups['app'] | first }}:8022"

auth_public_basepath: ""
auth_admin_basepath: ""
emm_admin_basepath: ""
emm_mobile_basepath: ""
aps_admin_basepath: ""
aps_market_basepath: ""
pkgrepo_admin_basepath: ""

auth_public_uri: "{{ auth_public_address }}{{ auth_public_basepath
}}}"
auth_admin_uri: "{{ auth_admin_address }}{{ auth_admin_basepath }}"
aps_admin_uri: "{{ aps_admin_address }}{{ aps_admin_basepath }}"
aps_market_uri: "{{ aps_market_address }}{{ aps_market_basepath }}"
emm_admin_uri: "{{ emm_admin_address }}{{ emm_admin_basepath }}"
emm_mobile_uri: "{{ emm_mobile_address }}{{ emm_mobile_basepath }}"

emm_admin_cdn_uri: "{{ emm_admin_uri }}"
emm_mobile_cdn_uri: "{{ emm_mobile_uri }}"
```

```

insecure_uri: true
same_site_mode: "strict"
krakendcsrf_enabled: false

emm_admin_console_client_secret: "nevertellanyone"
aurora_mobility_management_client_secret: "nevertellanyone"
emm_integration_account_client_secret: "nevertellanyone"

download_mode: "local"
domain: "local"
install_dir: "binary/emm"

```

4.10.2.8. Конфигурационный файл ПУСП `inventories-pkgrepo/deploy/hosts.yml`

В данном конфигурационном файле задаются адреса компонентов подсистемы ПУСП. Описание секций конфигурационного файла приведено в таблице (Таблица 22).

Таблица 22

Секция конфигурационного файла	Описание
<code>all.children.app</code>	Сервера приложений ППО
<code>all.children.postgresql.children.postgresql_masters</code>	СУБД Postgres
<code>all.children.nginx</code>	Балансировщик микросервисов «Nginx Web Server»
<code>all.children.consul</code>	Система обнаружения сервисов «Consul»
<code>all.children.consul-template</code>	Средство управления конфигурациями микросервисов «Consul Template»
<code>all.children.nats_streaming_server</code>	Сервис гарантированной доставки сообщений «Nats Streaming Server»
<code>all.children.redis.children.redis_masters</code>	СУБД Redis для хранения сессий
<code>all.children.redis.children.sentinel</code>	Redis Sentinel обеспечивает высокую доступность СУБД Redis

Конфигурационный файл `inventories-pkgrepo/deploy/hosts.yml` может иметь следующий вид:

```
---
all:
  children:
    app:
      hosts:
        ocs-app.local:
    postgresql:
      children:
        postgresql_masters:
          hosts:
            ocs-app.local:
    nginx:
      children:
        app:
    consul:
      children:
        consul_servers:
          children:
            app:
        consul_agents:
    consul-template:
      children:
        app:
    nats_streaming_server:
      hosts:
        ocs-app.local:
    redis:
      children:
```

```

redis_masters:
  hosts:
    ocs-app.local:
sentinel:
  hosts:
    ocs-app.local:

```

4.10.2.9. Конфигурационный файл ПУСП inventories-pkgrepo/deploy/group_vars/all/vars.yml

В данном конфигурационном файле задаются параметры взаимодействия ПУСП с СУБД PostgreSQL, СУБД Redis и Nats Streaming Server. Описание секций конфигурационного файла приведено в таблице (Таблица 23).

Таблица 23

Секция конфигурационного файла	Описание
project_name	Имя подсистемы
logger_level	Уровень логирования
gateway_gin_log_enabled	Включение логирования запросов на шлюзах доступа (true – логирование включено, false – логирование выключено)
download_mode	Режим получения бинарных файлов подсистемы при развертывании ППО. Возможные значения: http, httplocal, local
repository_dir	Локальный репозиторий с бинарными файлами ППО для режимов httplocal и local
postgresql.dbname	Имя БД
postgresql.port	Порт
postgresql.user	Имя пользователя
postgresql.password	Пароль
postgresql.extensions	Расширения
postgres_password	Пароль суперпользователя СУБД PostgreSQL

Секция конфигурационного файла	Описание
nats.auth_token	Токен доступа, установленный при развертывании Nats Streaming Server
redis_password	Пароль от СУБД Redis
session_remember_for	Время бездействия (неактивности) пользователя через которое осуществляется завершение сеанса пользователя
session_renew_timeout	Время, через которое происходит продление сессии пользователя между двумя активностями
auth_public_address	Адрес Консоли входа пользователей
auth_admin_address	Адрес Консоли администратора ПБ
auth_public_basepath	basepath Консоли входа пользователей
auth_admin_basepath	basepath Консоли администратора ПБ
auth_public_url	Адрес Консоли входа пользователей с учетом basepath
auth_admin_url	Адрес Консоли администратора ПБ с учетом basepath
pkgrepo_integration_account_client_secret	Секретный ключ OIDC-клиента (Package repository egress API gateway)
pkgrepo_mobile_uri	Путь к файловому серверу (Nginx) ПУСП
domain	Служебный домен для межсервисного взаимодействия
install_dir	Путь к каталогу с бинарными файлами ПБ в локальном репозитории

Конфигурационный файл `inventories-pkgrepo/deploy/group_vars/all/vars.yml` может иметь следующий вид:

```
project_name: "pkgrepo"

logger_level: "debug"
gateway_gin_log_enabled: true

download_mode: "httplocal"
repository_dir: "{{ playbook_dir }}/repository"
```

```
postgresql:
  dbname: pkgrepo
  port: 5432
  user: pkgrepo
  password: ocs
  extensions: ["pg_partman_bgw", "pg_stat_statements"]
postgres_password: "postgres"

nats:
  auth_token: FF12fddgdhFLL

redis_password: "@rTT9089087fslk"

auth_public_address: "http://{{ groups['app'] | first }}:8018"
auth_admin_address: "http://{{ groups['app'] | first }}:8019"

auth_public_basepath: ""
auth_admin_basepath: ""

auth_public_uri: "{{ auth_public_address }}{{ auth_public_basepath
}}"
auth_admin_uri: "{{ auth_admin_address }}{{ auth_admin_basepath }}"

pkgrepo_integration_account_client_secret: "nevertellanyone"
pkgrepo_mobile_uri: "http://{{ groups['app'] | first
}}:8030/pkgrepo/mobile"

download_mode: "local"
domain: "local"
install_dir: "binary/pkgrepo"

"
```

5. РЕЗЕРВНОЕ КОПИРОВАНИЕ

ВНИМАНИЕ! Приведенные ниже имена файлов и каталогов характерны для типового варианта установки ППО и среды функционирования ППО.

5.1. Резервное копирование после установки (обновления) ППО

После успешной установки (обновления) ППО необходимо создать резервные копии каталога с компонентами среды функционирования (install-infra) и каталога с загрузочными модулями ППО (install-apps).

5.2. Периодическое резервное копирование и резервное копирование перед установкой обновлений

Периодичность резервного копирования определяется регламентами эксплуатирующей организации.

Периодическое резервное копирование и резервное копирование перед установкой обновлений выполняется в следующей последовательности:

5.2.1. Резервное копирование данных

5.2.1.1. Создать резервные копии баз данных ПБ (auth), ПМ (appstore), ПУ (emm) и ПУСП (pkgrepo).

Резервная копия БД выполняется в соответствии с эксплуатационной документацией на используемую СУБД, либо в соответствии с регламентами эксплуатирующей организации.

5.2.1.2. Создать резервную копию каталога с файлами МП подсистемы «Маркет».

Для этого необходимо создать резервную копию каталога /ocs/appstore/applications-api на сервере приложений ПМ, либо в едином файловом хранилище, в зависимости от того какой вариант хранения файлов используется.

5.2.1.3. Создать резервную копию каталога с файлами системных пакетов ПУСП.

Для этого необходимо создать резервную копию каталога `/ocs/pkgrepo` на сервере приложений ПУСП, либо в едином файловом хранилище, в зависимости от того какой вариант хранения файлов используется.

5.2.2. Резервное копирование ППО

5.2.2.1. Создать резервную копию каталога с конфигурационными файлами подсистем и сервисов ППО (каталог: `/var/ocs/`).

5.2.2.2. Создать резервную копию сервисов ППО.

5.2.2.3. Для этого необходимо создать резервную копию файлов `*.target` и `*.service` по маске `ocs-*`, находящихся в каталоге `/etc/systemd/system/`, а так же бинарных файлов сервисов по маске `ocs-*`, находящихся в каталоге `/usr/bin/`.

5.2.3. Резервное копирование компонентов среды функционирования

5.2.3.1. Создать резервную копию Nginx Web Server (каталог: `/etc/nginx/`).

5.2.3.2. Создать резервную копию Consul (каталог: `/opt/consul/`).

5.2.3.3. Создать резервную копию Consul Template (каталог: `/etc/consul-template/`).

5.2.3.4. Создать резервную копию Nats Streaming Server (каталог: `/data/nats/`).

5.2.3.5. Создать резервную копию конфигурационных файлов Redis (файлы: `/etc/redis.conf /etc/redis-sentinel.conf`).

5.2.3.6. Создать резервную копию конфигурационных файлов PostgreSQL (файлы: `/var/lib/pgsql/11/data/postgresql.conf /var/lib/pgsql/11/data/pg_hba.conf` для ОС CentOS и `/var/lib/pgsql/data/postgresql.conf /var/lib/pgsql/data/pg_hba.conf` для ОС Альт 8 СП).

5.2.3.7. Создать резервную копию конфигурационных файлов PostgresPro (файлы: `/opt/pgpro/std-11/data/postgresql.conf /opt/pgpro/std-11/data/pg_hba.conf`).

5.2.3.8. Создать резервную копию сетевых настроек.

Для этого необходимо создать резервные копии следующих файлов:

- /etc/hosts
- /etc/hostname
- конфигурационные файлы DNS-сервера.

6. ОБНОВЛЕНИЕ ППО

Внимание! Для установки обновления ППО количество свободного места на жестком диске сервера БД ПБ должно быть не меньше, чем размер самой БД ПБ. При недостаточном количестве свободного места на жестком диске его необходимо увеличить. Время обновления ППО зависит от размера БД и может занять длительное время.

Обновление ППО выполняется в следующей последовательности:

6.1. Создать резервную копию данных, ППО и компонентов среды функционирования в соответствии с подразделом 4.10.

6.2. Выполнить перенос лог-файлов Nats Streaming Server в каталог с данными.

Для этого необходимо перейти в каталог `install-infra` новой версии ППО и выполнить команду:

```
ansible-playbook -i inventories/hosts.yml -u <имя пользователя>  
release_upgrade/play-upgrade_to_release_2.2.2.yml -vv --diff
```

6.3. Установить компоненты среды функционирования в соответствии с подразделом 4.3.

Устанавливать необходимо только те компоненты среды функционирования, у которых изменилась версия. Для этого необходимо выполнить сравнение версий компонентов среды функционирования в новом и предыдущем дистрибутивах. Информация о версиях компонентов среды функционирования приведена в третьем столбце файла `versions`. Файл `versions` находится в корневом каталоге дистрибутива с компонентами среды функционирования.

Пример, файла versions:

consul	master	4698dcd2fa0ad1a29a846c2a475046d5e572f66a
consul-template	master	1dd681d509a1c5e3aa1882aeb53ebeb504faeef
nginx	master	420ad871296855752ed3bb31e9958ecf0d68ad52
postgresql	master	e7d2e67da97955d2440723a58dfb4510db3907b4
nats-streaming-server	master	fb4a9b55308f29c8bcda3fc1804da92db84e90d6
server-provision-scripts	master	cdcb455e074dd6bc2bcc519ebd842d36c3a29726
redis	master	f4c6c300e7f9533652bb02008575ff009f8ef985
openssl	master	7ac23c1d67a6671e20785a9e1cc84d7d8b46103d
cert-distr-infra	branch	1ac040b2fff85ce3c9fbca42a914b34679303acc

6.4. Установить ППО в соответствии с пунктом 4.4.

7. УПРАВЛЕНИЕ СЕРВИСАМИ И НАСТРОЙКАМИ СЕРВИСОВ (ПОДСИСТЕМ) ППО

7.1. Управление сервисами ППО

Управление сервисами ППО заключается в их установке, удалении, запуске, остановке, перезапуске, проверке статуса, изменении настроек и осуществляется с помощью скриптов из каталога `install-<версия ППО>`, созданного на этапе установки ППО п. 4.4.4.

Формат команды управления сервисами имеет следующий вид:

```
ansible-playbook -i <inventory-file> play-systemd-deploy.yml -vv -  
-extra-vars "apps=<перечень сервисов подсистемы> action=<действие>" -u  
<имя пользователя>
```

Описание параметров команды управления:

1) Параметр "-i"

Данный параметр задает путь к инвентарному файлу (конфигурационному файл `hosts.yml`) подсистемы ППО и может принимать значения, приведенные в таблице (Таблица 24).

2) Параметр "-u"

Данный параметр задает пользователя ОС от имени которого будут выполняться действия (осуществляться управление).

3) Параметр "apps"

Данный параметр задает перечень сервисов, для которых будет выполнена команда управления. Если необходимо выполнить команду сразу для всех сервисов подсистемы, то необходимо перечислить через запятую все сервисы подсистемы, либо задать значение параметра `"apps=all"`.

В параметре “apps” могут задаваться только сервисы той подсистемы ППО, которая соответствует инвентарному файлу, указанному в параметре “-i”. При этом управление шлюзами доступа (сервисами шлюзов доступа) осуществляется в рамках той подсистемы, для которой они предназначены

Таблица 24

Значение параметра "-i"	Сервисы (значение параметра "apps")
ПБ	
inventories-auth/deploy/hosts.yml	ocs-auth-admin-api-gw
	ocs-auth-public-api-gw
	ocs-auth-server-public-proxy
	ocs-auth-idp-api
	ocs-auth-accounts-devices-api
	ocs-auth-accounts-users-api
	ocs-auth-server-admin
	ocs-auth-server-public
	ocs-auth-audit-api
	ocs-auth-adminconsole-ui
ocs-auth-idp-ui	
ПМ	
inventories-appstore/deploy/hosts.yml	ocs-appstore-applications-api
	ocs-appstore-adminconsole
	ocs-appstore-devconsole-ui
	ocs-appstore-admin-api-gw
	ocs-appstore-client-api-gw
	ocs-appstore-dev-api-gw
ocs-appstore-egress-api-gw	
ПУ	
inventories-emm/deploy/hosts.yml	ocs-emm-applications-api
	ocs-emm-dispatcher-api
	ocs-emm-devices-api
	ocs-emm-state-manager-api
	ocs-emm-enrollments-api
	ocs-emm-policies-api
ocs-emm-reports-api	

Значение параметра "-i"	Сервисы (значение параметра "apps")
	ocs-emm-users-api
	ocs-emm-journal-api
	ocs-emm-adminconsole-ui
	ocs-emm-admin-api-gw
	ocs-emm-device-api-gw
	ocs-emm-egress-api-gw
ПУСП	
inventories- pkgrepo/deploy/hosts.yml	ocs-pkgrepo-pkg-repo-api
	ocs-pkgrepo-device-api-gw
	ocs-pkgrepo-admin-api-gw
	ocs-pkgrepo-egress-api-gw

4) Параметр "action"

Данный параметр действие, которое необходимо выполнить. Перечень допустимых действий и соответствующие им значения параметра приведены в таблице (Таблица 25).

Таблица 25

Значение параметра "apps"	Действие
deploy	Установка
flush_all	Удаление
start	Запуск
stop	Остановка
restart	Перезапуск
config	Изменение настроек (переустановка конфигурационного файла)

Примеры команд управления:

1) Остановка всех сервисов ПМ:

```
ansible-playbook -i inventories-appstore/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=all action=stop" -u ivanov
```

2) Запуск сервисов ocs-appstore-applications-api и ocs-appstore-adminconsole

ПМ:

```
ansible-playbook -i inventories-appstore/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=ocs-appstore-applications-  
api,ocs-appstore-adminconsole action=start" -u ivanov
```

3) Удаление сервиса ocs-appstore-devconsole-ui ПМ:

```
ansible-playbook -i inventories-appstore/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=ocs-appstore-devconsole-ui  
action=flush_all" -u ivanov
```

7.2. Управление настройками сервисов и подсистем ППО

Управление настройками сервисов и подсистем ППО может осуществляться двумя способами.

7.2.1. Способ 1 (рекомендуемый)

Для изменения настроек сервисов и подсистем ППО данным способом необходимо выполнить следующие действия:

7.2.1.1. Задать требуемые значения параметров в конфигурационных файлах сценариев установки подсистем ППО. Описание параметров конфигурационных файлов сценариев установки подсистем ППО приведены в п. 4.10.2.

7.2.1.2. Переустановить конфигурационные файлы с помощью следующей команды:

– ПБ

```
ansible-playbook -i inventories-auth/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=all action=config" -u <имя  
пользователя>
```

– ПМ

```
ansible-playbook -i inventories-appstore/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=all action=config" -u <имя  
пользователя>
```

– ПУ

```
ansible-playbook -i inventories-emm/deploy/hosts.yml play-systemd-  
deploy.yml -vv --extra-vars "apps=all action=config" -u <имя  
пользователя>
```

– ПУСП

```
ansible-playbook -i inventories-pkgrepo/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=all action=config" -u <имя  
пользователя>
```

7.2.2. Способ 2

Для изменения настроек сервисов и подсистем ППО данным способом необходимо выполнить следующие действия:

7.2.2.1. Задать требуемые значения параметров в конфигурационных файлах сервисов и подсистем ППО. Описание параметров конфигурационных файлов сценариев установки подсистем ППО приведены в п. 8.

7.2.2.2. Перезапустить требуемые сервисы с помощью следующей команды:

– ПБ

```
ansible-playbook -i inventories-auth/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=<перечень сервисов ПБ>  
action=restart" -u <имя пользователя>
```

– ПМ

```
ansible-playbook -i inventories-appstore/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=<перечень сервисов ПМ>  
action=restart" -u <имя пользователя>
```

– ПУ

```
ansible-playbook -i inventories-emm/deploy/hosts.yml play-systemd-  
deploy.yml -vv --extra-vars "apps=<перечень сервисов ПУ> action=restart"  
-u <имя пользователя>
```

– ПУСП

```
ansible-playbook -i inventories-pkgrepo/deploy/hosts.yml play-  
systemd-deploy.yml -vv --extra-vars "apps=<перечень сервисов ПУСП>  
action=restart" -u <имя пользователя>
```

8. ОПИСАНИЕ ПАРАМЕТРОВ КОНФИГУРАЦИОННЫХ ФАЙЛОВ МОДУЛЕЙ ППО

8.1. Описание конфигурационных файлов ПБ

8.1.1. Общий конфигурационный файл ПБ (файл: `/var/ocs/auth/config.yml`)

Файл содержит общие настройки, которые могут использовать любые сервисы.

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле и если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Конфигурационный файл может содержать любые параметры сервисов, которые было решено вынести как единые (по умолчанию) для всех.

Описание параметров общего конфигурационного файла ПБ приведено в таблице (Таблица 26).

Таблица 26

Параметр	Описание	Добавлено	Удалено
<code>config.insecureUri</code>	Флаг использования незащищенного соединения. Этот параметр надо задавать в <code>true</code> если используется незащищенное соединение (<code>http</code> протокол). Он влияет на формирование <code>Cookie</code> заголовков, проверку редиректов.	2.2.0	-
<code>config.insecureRedirectUris</code>	Список <code>url</code> на которые сервер авторизации разрешает делать редирект по протоколу <code>http</code> в процессе аутентификации. Конфиг можно заполнять только при включенной опции <code>config.insecureUri</code>	2.2.0	-
<code>config.publicUri.auth.publicUri</code>	Полный адрес публичного API сервера авторизации	2.2.1	-

Параметр	Описание	Добавлено	Удалено
config.publicUri.auth.publicBasepath	Префикс url публичного API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия.	2.2.1	-
config.publicUri.auth.adminBasepath	Префикс url к API консоли подсистемы безопасности, используемый для внутреннего межподсистемного взаимодействия.	2.2.1	-
config.publicUri.emm.adminUri	Полный адрес API/UI консоли администратора EMM	2.2.1	-
config.session.rememberFor	Время жизни сессии пользователя консоли	2.2.0	-
config.session.renewTimeout	Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а один раз за данный интервал)	2.2.0	-
config.oidcClients.authAdminConsole.scope	Скопы для oidc клиента, который используется для аутентификации в консоли подсистемы безопасности	2.2.0	-
config.oidcClients.authAdminConsole.returnUri	Адрес, на который сервер авторизации сделает редирект после аутентификации в консоли подсистемы безопасности	2.2.0	-
config.database.host	Адрес (хост) базы данных	2.2.0	-
config.database.port	Порт базы данных	2.2.0	-
config.database.user	Имя пользователя базы данных	2.2.0	-
config.database.dbname	Имя базы данных	2.2.0	-
config.database.password	Пароль базы данных	2.2.0	-
config.logger.level	Уровень детализации сообщений логирования. Возможные значения: debug, info, warn, error	2.2.0	-

Параметр	Описание	Добавлено	Удалено
config.logger.caller	Флаг включения в сообщение лога названия функции и номера строки, в которой происходит логирование события	2.2.0	-
config.logger.gateway_gin_log_enabled	Флаг включения логирования входящего запроса на шлюзе (url запроса и http-статус ответа)	2.2.1	-
config.redis.sentinelAddress	Адрес модуля sentinel СУБД Redis	2.2.0	-
config.redis.sentinelPassword	Пароль к модулю sentinel СУБД Redis	2.2.0	-
config.redis.masterName	Идентификатор (имя) БД Redis	2.2.0	-
config.redis.password	Пароль к СУБД Redis	2.2.0	-

8.1.2. Конфигурационный файл сервиса ocs-auth-accounts-devices-api (файл: </var/ocs/auth/ocs-auth-accounts-devices-api/ocs-auth-accounts-devices-api.yml>)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле и если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-auth-accounts-devices-api приведено в таблице (Таблица 27).

Таблица 27

Параметр	Описание	Добавлено	Удалено
config.database.dialect	Тип базы данных для ORM, мы используем "postgres"	2.2.0	-
config.database.args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword"	2.2.0	-

Параметр		Описание	Добавлено	Удалено
		dbname=dbName sslmode=disable timezone=utc"		
config.database	debug	Флаг подключения к базе данных в режиме отладки для вывода запросов в стандартный вывод программы	2.2.0	-
config.	hashWorkers	Количество воркеров, вычисляющих хэши паролей. По умолчанию 16.	2.2.0	-
config.	passwordHistoryDepth	Число последних использованных паролей, которые запрещено использовать пользователями при создании новых паролей. Новый пароль не должен совпадать с паролями из истории в рамках заданного значения.	2.2.0	-
config.validationModel.	login	Регулярное выражение для валидации логина. 1. Формат значения (IMEI или MAC): – regex: "^\\d{15}\$ ^([0-9a-f]{2}:){5}([0-9a-f]{2})\$"	2.2.0	-
config.validationModel.	deviceId	Регулярное выражение для валидации id устройства. 1. Поле обязательно к заполнению: – regex: ^.+ \$"	2.2.0	-
config.	maxAccountInactivityPeriod	Максимальный срок неактивности учетной записи, после которого она должна быть заблокирована Значение:87600h («псевдо-бесконечность»). Учетные записи устройств не должны блокироваться через 45 дней, как	2.2.0	-

Параметр		Описание	Добавлено	Удалено
		это реализуется для учетных записей пользователей		
config.transport.http.tls.	enabled	Флаг включения TLS протокола	2.2.0	-
config.transport.http.tls.	private_key	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу config_folder/app_name/app_name.key	2.2.0	-
config.transport.http.tls.	certificate	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу config_folder/app_name/app_name.crt	2.2.0	-
config.transport.http.tls.	ca_certificate	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0	-

8.1.3. Конфигурационный файл сервиса ocs-auth-accounts-users-api (файл: /var/ocs/auth/ocs-auth-accounts-users-api/ocs-auth-accounts-users-api.yml)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-auth-accounts-users-api приведено в таблице (Таблица 28).

Таблица 28

Параметр		Описание	Добавлено	Удалено
config.logger	level	Уровень детализации сообщений логирования. Возможные значения: debug, info, warn, error	2.2.0	-
config.logger	caller	Флаг включения в сообщение лога названия функции и номера строки, в которой происходит логирование события	2.2.0	-
config.logger	humanReadable	Флаг включения форматирования сообщений лога в обычный текст (не json)	2.2.0	-
config.transport.http	address	Номер порта, на котором запускается приложение (":8080")	2.2.0	-
config.transport.http.tls	enabled	Флаг включения TLS протокола	2.2.0	-
config.transport.http.tls	private_key	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу config_folder/app_name/app_name.key	2.2.0	-
config.transport.http.tls	certificate	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу config_folder/app_name/app_name.crt	2.2.0	-
config.transport.http.tls	ca_certificate	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0	-
config.transport.HTTPDebug	address	Номер порта, по которому запускаются служебные debug-эндпоинты приложения (":8080"). При незаполненном значении совпадает с config.transport.http.address	2.2.0	-
config.transport.HTTPDebug	enabled	[не используется] Флаг включения TLS протокола (для служебных debug-эндпоинтов приложения)	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.transport.HTTPDebug.	private_key	[не используется] Путь к файлу с приватным ключом (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.	certificate	[не используется] Путь к файлу с сертификатом (публичный ключ) (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.	ca_certificate	[не используется] Путь к файлу с доверенным сертификатом (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.	shutdownTime	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.2.0	-
config.transport.nats.	url	Адрес сервера NATS	2.2.0	-
config.transport.nats.	clusterID	Идентификатор кластера NATS (https://docs.nats.io/)	2.2.0	-
config.transport.nats.	clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
config.transport.nats.	durableName	Имя очереди NATS для подписок с сохранением позиции (https://docs.nats.io/)	2.2.0	-
config.jaeger.	address	Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/)	2.2.0	-
config.database.	dialect	Тип базы данных для ORM, мы используем «postgres»	2.2.0	-
config.database.	args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
config.database.	debug	Флаг подключения к базе данных в режиме отладки для вывода запросов в стандартный вывод программы	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.	enableProof	Флаг включения отладочного профилировщика	2.2.0	-
config.	hashWorkers	Количество воркеров, вычисляющих хэши паролей. По умолчанию 16.	2.2.0	-
config.	passwordExpirationTime	Максимальное время действия пароля. Значение: "1440h" # 60 days	2.2.0	-
config.	passwordHistoryDepth	Число последних использованных паролей, которые запрещено использовать пользователями при создании новых паролей. Новый пароль не должен совпадать с паролями из истории в рамках заданного значения.	2.2.0	-
config.passwordSettings.	minLength	Минимальная длина пароля. Значение: 8. Если указать значение меньше, чем 8, то система должна считать, что minPasswordLength = 8.	2.2.0	-
config.passwordSettings.	maxLength	Максимальная длина пароля. Значение: 255. Если указать значение меньше, чем minPasswordLength (минимальная длина пароля), то система должна считать, что maxPasswordLength = minPasswordLength	2.2.0	-
config.passwordSettings.	minDigits	Минимальное число цифр в пароле (3)	2.2.0	-
config.passwordSettings.	minUpperLetters	Минимальное число букв верхнего регистра в пароле (2)	2.2.0	-
config.passwordSettings.	minLowerLetters	Минимальное число букв нижнего регистра в пароле (2)	2.2.0	-
config.passwordSettings.	minSpecialChars	Минимальное число спецсимволов в пароле (2)	2.2.0	-
config.passwordSettings.	upperLetters	Допустимые для пароля символы верхнего регистра ABCDEFGHIJKLMNOPQRSTUVWXYZ	2.2.0	-
config.passwordSettings.	lowerLetters	Допустимые для пароля символы нижнего регистра abcdefghijklmnopqrstuvwxyz	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.passwordSettings.	specialChars	Допустимые для пароля специальные символы !@#\$%^&*()_+	2.2.0	-
config.validationModel.	login	<p>Регулярное выражение для валидации логина:</p> <ol style="list-style-type: none"> Поле обязательно для заполнения: <ul style="list-style-type: none"> – regex: <code>^.+</code> Требования к формату значения: <ul style="list-style-type: none"> – regex: <code>^([\<>()\[\]\.\,;:\s@»]+(\.([\<>()\[\]\.\,;:\s@»]+)*)@((\[[0-9]{1,3}\. [0-9]{1,3}\. [0-9]{1,3}\. [0-9]{1,3}\) ([a-zA-Za-яА-ЯёЁ\ -0-9]+\.)+[a-zA-Za-яА-ЯёЁ]{2,}\.?))\$</code> Требование к длине: <ul style="list-style-type: none"> – regex: <code>^{0,255}</code> 	2.2.0	-
config.validationModel.	firstName	<p>Регулярное выражение для валидации имени пользователя (В сервисе accounts-devices не используется)</p> <ol style="list-style-type: none"> Поле обязательно для заполнения: <ul style="list-style-type: none"> – regex: <code>^.+</code> Требование к длине: <ul style="list-style-type: none"> – regex: <code>^{0,255}</code> 	2.2.0	-
config.validationModel.	lastName	<p>Регулярное выражение для валидации фамилии пользователя (В сервисе accounts-devices не используется)</p> <ol style="list-style-type: none"> Поле обязательно для заполнения: <ul style="list-style-type: none"> – regex: <code>^.+</code> Требование к длине: <ul style="list-style-type: none"> – regex: <code>^{0,255}</code> 	2.2.0	-
config.validationModel.	patronymic	<p>Регулярное выражение для валидации отчества пользователя (В сервисе accounts-devices не используется)</p> <ol style="list-style-type: none"> Требование к длине: <ul style="list-style-type: none"> – regex: <code>^{0,255}</code> 	2.2.0	-
config.	failedLoginTries	<p>Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи</p> <p>Значение: "3"</p>	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.	failedLoginBlockTime	Время блокировки учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации Значение: "15m"	2.2.0	-
config.	maxAccountInactivityPeriod	Максимальный срок неактивности учетной записи, после которого она должна быть заблокирована Значение: 1080h (45 дней)	2.2.0	-

8.1.4. Конфигурационный файл сервиса ocs-auth-adminconsole-ui (файл: </var/ocs/auth/ocs-auth-adminconsole-ui/ocs-auth-adminconsole-ui.yml>)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-auth-adminconsole-ui приведено в таблице (Таблица 29).

Таблица 29

Параметр		Описание	Добавлено	Удалено
publicRuntimeConfig.	contextRoot	Относительный базовый путь для страниц UI. Пример: "/auth/admin"	2.2.0	-
publicRuntimeConfig.	apiContextRoot	Относительный базовый путь для запросов API. Пример: "/auth/admin/api"	2.2.0	-
publicRuntimeConfig.passwordSettings.	minLength	Минимальная длина пароля. Значение: 8. Если указать значение меньше, чем 8, то система должна считать, что minPasswordLength = 8.	2.2.0	-

Параметр	Описание	Добавлено	Удалено
publicRuntimeConfig.passwordSettings.maxLength	Максимальная длина пароля. Значение: 255. Если указать значение меньше, чем minPasswordLength (минимальная длина пароля), то система должна считать, что maxPasswordLength = minPasswordLength	2.2.0	-
publicRuntimeConfig.session.renewTimeout	Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а один раз за данный интервал)	2.2.0	-
publicRuntimeConfig.session.renewUri	URL для продления сессии пользователя консоли	2.2.0	-
publicRuntimeConfig.session.oidcRenewUri	URL для продления OIDC сессии	2.2.0	-
publicRuntimeConfig.logoutUri	URL выхода из системы	2.2.0	-
publicRuntimeConfig.validationModel.login	<p>Регулярные выражения для валидации логина пользователя:</p> <ol style="list-style-type: none"> Поле обязательно для заполнения: <ul style="list-style-type: none"> regex: <code>^.+</code> message: required Требования к формату значения: <ul style="list-style-type: none"> regex: <code>^([^<>() \[\] \. , ; : \s @ »] + (\. [^ <> () \ [\] \ \ . , ; : \ s @ »] +) *) @ ((\ [[0 - 9] { 1 , 3 } \ . [0 - 9] { 1 , 3 } \ . [0 - 9] { 1 , 3 } \ . [0 - 9] { 1 , 3 }) (([a - z A - Z a - я A - Я ё Ë \ - 0 - 9] + \ .) + [a - z A - Z a - я A - Я ё Ë] { 2 , } \ . ?)) \$</code> message: invalidEmail Требование к длине: <ul style="list-style-type: none"> regex: <code>^.{0,255}\$</code> 	2.2.0	-

Параметр	Описание	Добавлено	Удалено
	<ul style="list-style-type: none"> – message: maxLength – messageArgs: <ul style="list-style-type: none"> • maxLength: 255 		
publicRuntimeConfig.validationModel.	<p>firstName</p> <p>Регулярное выражение для валидации имени пользователя</p> <p>1. Поле обязательно для заполнения:</p> <ul style="list-style-type: none"> – regex: ^.+& – message: required <p>2. Требование к длине:</p> <ul style="list-style-type: none"> – regex: ^.{0,255}& – message: maxLength – messageArgs: <ul style="list-style-type: none"> • maxLength: 255 	2.2.0	-
publicRuntimeConfig.validationModel.	<p>lastName</p> <p>Регулярное выражение для валидации фамилии пользователя</p> <p>1. Поле обязательно для заполнения:</p> <ul style="list-style-type: none"> – regex: ^.+& – message: required <p>2. Требование к длине:</p> <ul style="list-style-type: none"> – regex: ^.{0,255}& – message: maxLength – messageArgs: <ul style="list-style-type: none"> • maxLength: 255 	2.2.0	-
publicRuntimeConfig.validationModel.	<p>patronymic</p> <p>Регулярное выражение для валидации отчества пользователя (В сервисе accounts-devices не используется).</p> <p>Требование к длине</p> <p>1. Требование к длине:</p> <ul style="list-style-type: none"> – regex: ^.{0,255}& – message: maxLength – messageArgs: <ul style="list-style-type: none"> • maxLength: 255 	2.2.0	-

Параметр	Описание	Добавлено	Удалено
publicRuntimeConfig.translateCode.audits.action	Настройка локализации параметра «действие» в сообщениях о событиях аудита	2.2.0	-
publicRuntimeConfig.translateCode.audits.objectId	Настройка локализации параметра «объект» в сообщениях о событиях аудита	2.2.0	-
publicRuntimeConfig.translateCode.audits.objectType	Настройка локализации параметра «тип» объектов в сообщениях о событиях аудита	2.2.0	-
publicRuntimeConfig.translateCode.audits.result	Настройка локализации параметра «результат» действий в сообщениях о событиях аудита	2.2.0	-
publicRuntimeConfig.menuItems.monitoring.label	Название пункта меню раздела мониторинга	2.2.0	-
publicRuntimeConfig.menuItems.monitoring.url	Ссылка на раздел мониторинга	2.2.0	-
publicRuntimeConfig.menuItems.monitoring.tabs.indicators.label	Название пункта меню подраздела индикаторы, раздела мониторинга	2.2.0	-
publicRuntimeConfig.menuItems.monitoring.tabs.indicators.url	Ссылка на подраздел индикаторы, раздела мониторинга	2.2.0	-
publicRuntimeConfig.menuItems.monitoring.tabs.audit.label	Название пункта меню подраздела аудит, раздела мониторинга	2.2.0	-
publicRuntimeConfig.menuItems.monitoring.tabs.audit.url	Ссылка на подраздел индикаторы, раздела мониторинга	2.2.0	-
publicRuntimeConfig.menuItems.control.label	Название пункта меню раздела управления	2.2.0	-

Параметр	Описание	Добавлено	Удалено	
publicRuntimeConfig.menuItems.control.	url	Ссылка на раздел управление	2.2.0	-
publicRuntimeConfig.menuItems.administration.	label	Название пункта меню раздела администрирование	2.2.0	-
publicRuntimeConfig.menuItems.administration.	url	Ссылка на раздел администрирование	2.2.0	-
publicRuntimeConfig.menuItems.administration.tabs.accounts.	label	Название пункта меню подраздела Учетные записи, раздела Администрирование	2.2.0	-
publicRuntimeConfig.menuItems.administration.tabs.accounts.	url	Ссылка на подраздел Учетные записи, раздела Администрирование	2.2.0	-
publicRuntimeConfig.menuItems.administration.tabs.settings.	label	Название пункта меню подраздела настройки, раздела администрирование	2.2.0	-
publicRuntimeConfig.menuItems.administration.tabs.settings.	url	Ссылка на подраздел настройки, раздела администрирование	2.2.0	-
publicRuntimeConfig.menuItems.administration.tabs.orgStructure.	label	Название пункта меню подраздела оргструктуры, раздела администрирование	2.2.0	-
publicRuntimeConfig.menuItems.administration.tabs.orgStructure.	url	Ссылка на подраздел оргструктуры, раздела администрирование	2.2.0	-
publicRuntimeConfig.endpoints.getRoles.	path	Относительный путь API запроса списка ролей Пример: "/realms/user/roles"	2.2.0	-

Параметр	Описание	Добавлено	Удалено
publicRuntimeConfig.endpoints.getRoles.	method HTTP-метод API запроса списка ролей Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.getAccountRoles.	path Относительный путь API запроса списка ролей аккаунта Пример: "/realms/user/accounts/{id}/roles"	2.2.0	-
publicRuntimeConfig.endpoints.getAccountRoles.	method HTTP-метод API запроса списка ролей аккаунта Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.addAccountRole.	path Относительный путь API запроса добавления роли аккаунту Пример: "/realms/user/accounts/{id}/roles/{code}"	2.2.0	-
publicRuntimeConfig.endpoints.addAccountRole.	method HTTP-метод API запроса добавления роли аккаунту Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.deleteAccountRole.	path Относительный путь API запроса удаления роли аккаунту Пример: "/realms/user/accounts/{id}/roles/{code}"	2.2.0	-
publicRuntimeConfig.endpoints.deleteAccountRole.	method HTTP-метод API запроса удаления роли аккаунту Пример: GET POST PUT DELETE	2.2.0	-

Параметр	Описание	Добавлено	Удалено
publicRuntimeConfig.endpoints.getAccount.	path Относительный путь API запроса списка аккаунтов Пример: "/realms/user/accounts"	2.2.0	-
publicRuntimeConfig.endpoints.getAccount.	method HTTP-метод API запроса списка аккаунтов Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.createAccount.	path Относительный путь API запроса создания аккаунта Пример: "/realms/user/accounts"	2.2.0	-
publicRuntimeConfig.endpoints.createAccount.	method HTTP-метод API запроса создания аккаунта Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.updateAccount.	path Относительный путь API запроса обновления аккаунта Пример: "/realms/user/accounts/{id}"	2.2.0	-
publicRuntimeConfig.endpoints.updateAccount.	method HTTP-метод API запроса обновления аккаунта Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.getAccount.	path Относительный путь API запроса аккаунта Пример: "/realms/user/accounts/{id}"	2.2.0	-
publicRuntimeConfig.endpoints.getAccount.	method HTTP-метод API запроса аккаунта Пример: GET POST PUT DELETE	2.2.0	-

Параметр	Описание	Добавлено	Удалено
publicRuntimeConfig.endpoints.accountChangePassword.path	Относительный путь API запроса смены пароля аккаунту Пример: "/realms/user/accounts/{id}/changePassword"	2.2.0	-
publicRuntimeConfig.endpoints.accountChangePassword.method	HTTP-метод API запроса смены пароля аккаунту Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.blockAccount.path	Относительный путь API запроса блокировки аккаунта Пример: "/realms/user/accounts/{id}/block"	2.2.0	-
publicRuntimeConfig.endpoints.blockAccount.method	HTTP-метод API запроса блокировки аккаунта Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.unblockAccount.path	Относительный путь API запроса разблокировки аккаунта Пример: "/realms/user/accounts/{id}/unblock"	2.2.0	-
publicRuntimeConfig.endpoints.unblockAccount.method	HTTP-метод API запроса разблокировки аккаунта Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.getAudits.path	Относительный путь API запроса списка событий аудита Пример: "/auditEvents"	2.2.0	-
publicRuntimeConfig.endpoints.getAudits.method	HTTP-метод API запроса списка ролей Пример: GET POST PUT DELETE	2.2.0	-

Параметр	Описание	Добавлено	Удалено
publicRuntimeConfig.endpoints.getSession.path	Относительный путь API запроса списка сессий Пример: <code>"/sessions"</code>	2.2.0	-
publicRuntimeConfig.endpoints.getSession.method	HTTP-метод API запроса списка сессий Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.deleteAccount.path	Относительный путь API запроса удаления учетной записи Пример: <code>"/realms/user/accounts/{id}"</code>	2.2.0	-
publicRuntimeConfig.endpoints.deleteAccount.method	HTTP-метод API запроса удаления учетной записи Пример: GET POST PUT DELETE	2.2.0	-
serverRuntimeConfig.tls.enabled	Флаг включения TLS протокола	2.2.0	-
serverRuntimeConfig.tls.private_key	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу <code>config_folder/app_name/app_name.key</code>	2.2.0	-
serverRuntimeConfig.tls.certificate	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу <code>config_folder/app_name/app_name.crt</code>	2.2.0	-
serverRuntimeConfig.tls.ca_certificate	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу <code>config_folder/ca.crt</code>	2.2.0	-

Параметр		Описание	Добавлено	Удалено
serverRuntimeConfig.pathToEula		Путь к файлу с лицензионным соглашением	2.2.0	-
serverRuntimeConfig.endpoints.getAccountsWithPath	path	URL API запроса списка ролей Пример: "http://ocs-auth-accounts-users-api.local:8019/api/realms/user/accounts"	2.2.0	-
serverRuntimeConfig.endpoints.getAccountsWithMethod	method	HTTP-метод API запроса списка аккаунтов Пример: GET POST PUT DELETE	2.2.0	-
serverRuntimeConfig.endpoints.getAuditEventsWithPath	path	URL API запроса списка событий аудита Пример: "http://ocs-auth-accounts-users-api.local:8019/api/auditEvents"	2.2.0	-
serverRuntimeConfig.endpoints.getAuditEventsWithMethod	method	HTTP-метод API запроса списка событий аудита Пример: GET POST PUT DELETE	2.2.0	-

8.1.5. Конфигурационный файл сервиса ocs-auth-audit-api (файл: </var/ocs/auth/ocs-auth-audit-api/ocs-auth-audit-api.yml>)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-auth-audit-api приведено в таблице (Таблица 30).

Таблица 30

Параметр		Описание	Добавлено	Удалено
config.logger.	level	Уровень детализации сообщений логирования. Возможные значения: debug, info, warn, error	2.2.0	-
config.logger.	caller	Флаг включения в сообщение лога названия функции и номера строки, в которой происходит логирование события	2.2.0	-
config.logger.	humanReadable	Флаг включения форматирования сообщений лога в обычный текст (не json)	2.2.0	-
config.transport.http.	address	Номер порта, на котором запускается приложение (":8080")	2.2.0	-
config.transport.http.tls.	enabled	Флаг включения TLS протокола	2.2.0	-
config.transport.http.tls.	private_key	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу config_folder/app_name/app_name.key	2.2.0	-
config.transport.http.tls.	certificate	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу config_folder/app_name/app_name.crt	2.2.0	-
config.transport.http.tls.	ca_certificate	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0	-
config.transport.HTTPDebug.	address	Номер порта, по которому запускаются служебные debug-эндпоинты приложения (":8080") При незаполненном значении совпадает с config.transport.http.address	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.transport.HTTPDebug.	enabled	[не используется] Флаг включения TLS протокола (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.	private_key	[не используется] Путь к файлу с приватным ключом (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.	certificate	[не используется] Путь к файлу с сертификатом (публичный ключ) (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.	ca_certificate	[не используется] Путь к файлу с доверенным сертификатом (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.	shutdownTime	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.2.0	-
config.transport.nats.	url	Адрес сервера NATS	2.2.0	-
config.transport.nats.	clusterID	Идентификатор кластера NATS (https://docs.nats.io/)	2.2.0	-
config.transport.nats.	clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
config.transport.nats.	durableName	Имя очереди NATS для подписок с сохранением позиции (https://docs.nats.io/)	2.2.0	-
config.jaeger.	address	Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/)	2.2.0	-
config.database.	dialect	Тип базы данных для ORM, мы используем "postgres"	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.datab ase.	args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
config.datab ase.	debug	Флаг подключения к базе данных в режиме отладки для вывода запросов в стандартный вывод программы	2.2.0	-

8.1.6. Конфигурационный файл сервиса ocs-auth-idp-api (файл: </var/ocs/auth/ocs-auth-idp-api/ocs-auth-idp-api.yml>)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-auth-idp-api приведено в таблице (Таблица 31).

Таблица 31

Параметр		Описание	Добавлено	Удалено
config.logger.	level	Уровень детализации сообщений логирования. Возможные значения: debug, info, warn, error	2.2.0	-
config.logger.	caller	Флаг включения в сообщение лога названия функции и номера строки, в которой происходит логирование события	2.2.0	-
config.logger.	humanReadable	Флаг включения форматирования сообщений лога в обычный текст (не json)	2.2.0	-
config.transpo rt.http.tls.	enabled	Флаг включения TLS протокола	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.transport.http.tls.private_key	private_key	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу config_folder/app_name/app_name.key	2.2.0	-
config.transport.http.tls.certificate	certificate	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу config_folder/app_name/app_name.crt	2.2.0	-
config.transport.http.tls.ca_certificate	ca_certificate	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0	-
config.transport.HTTPDebug.address	address	Номер порта, по которому запускаются служебные debug-эндпоинты приложения (":8080") При незаполненном значении совпадает с config.transport.http.address	2.2.0	-
config.transport.HTTPDebug.enabled	enabled	[не используется] Флаг включения TLS протокола (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.private_key	private_key	[не используется] Путь к файлу с приватным ключом (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.certificate	certificate	[не используется] Путь к файлу с сертификатом (публичный ключ) (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.ca_certificate	ca_certificate	[не используется] Путь к файлу с доверенным сертификатом (для служебных debug-эндпоинтов приложения)	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.transpo rt.	shutdownTime	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.2.0	-
config.transpo rt.nats.	url	Адрес сервера NATS	2.2.0	-
config.transpo rt.nats.	clusterID	Идентификатор кластера NATS (https://docs.nats.io/)	2.2.0	-
config.transpo rt.nats.	clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
config.transpo rt.nats.	durableName	Имя очереди NATS для подписок с сохранением позиции (https://docs.nats.io/)	2.2.0	-
config.jaeger.	address	Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/)	2.2.0	-
config.	enableProf	Флаг включения отладочного профилировщика	2.2.0	-
config.idpUi.	loginPageURL	URL на который происходит переадресация браузера клиента для аутентификации.	2.2.0	-
config.idpUi.	errorPageURL	URL на который происходит переадресация браузера клиента при ошибке аутентификации.	2.2.0	-
config.oidcp.	address	URL административного модуля OIDC Provider.	2.2.0	-
config.oidcp.s ession.	remember	Флаг того, что OIDC Provider должен запомнить данного пользователя. Данные авторизации сохраняются в cookies браузера, чтобы не запрашивать авторизацию на каждый запрос.	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.oidcp.session.	rememberFor	Время, на которое нужно запоминать пользователя в секундах. Если передано значение 0, то авторизация запоминается на время жизни сессии браузера с помощью сессионной cookie.	2.2.0	-
config.realms.	name	Имя источника учетных записей.	2.2.0	-
config.realms.	type	Тип источника учетных записей. Возможные значения: accountsService	2.2.0	-
config.realms.	address	URL API источника учетных записей.	2.2.0	-
config.oidcClients.	name	Имя OIDC клиента	2.2.0	-
config.oidcClients.	realm	Имя источника учетных записей. (для связи с realms.name)	2.2.0	-
config.oidcClients.session.	remember	Флаг, определяющий, должна ли запоминаться OIDC сессия при аутентификации.	2.2.0	-
config.	privilegedSessionsLimit	Допустимое количество одновременно запущенных сессий у привилегированной учетной записи	2.2.0	-
config.	unprivilegedSessionsLimit	Допустимое количество одновременно запущенных сессий у непривилегированной учетной записи	2.2.0	-
config.	accountLoginHeaderKey	Имя http-заголовка для передачи логина.	2.2.0	-

8.1.7. Конфигурационный файл сервиса ocs-auth-idp-ui (файл: /var/ocs/auth/ocs-auth-idp-ui/ocs-auth-idp-ui.yml)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-auth-idp-ui приведено в таблице (Таблица 32).

Таблица 32

Параметр		Описание	Добавлено	Удалено
publicRuntimeCon- fig.	contextRoot	Относительный базовый путь для страниц UI. Пример: "/auth/idp"	2.2.0	-
publicRuntimeCon- fig.	apiContextR- oot	Относительный базовый путь для запросов API. Пример: "/auth/idp/api"	2.2.0	-
publicRuntimeCon- fig.endpoints.l ogin.	path	Относительный путь API запроса на аутентификацию Пример: "/login"	2.2.0	-
publicRuntimeCon- fig.endpoints.l ogin.	method	HTTP-метод API запроса добавления роли аккаунту Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeCon- fig.endpoints. changePassword .	path	Относительный путь API запроса на смену пароля Пример: "/changePassword"	2.2.0	-
publicRuntimeCon- fig.endpoints. changePassword .	method	HTTP-метод API запроса добавления роли аккаунту Пример: GET POST PUT DELETE	2.2.0	-

Параметр		Описание	Добавлено	Удалено
publicRuntimeConfig.passwordSettings.	minLength	Минимальная длина пароля. Значение: 8. Если указать значение меньше, чем 8 , то система должна считать, что minLength = 8.	2.2.0	-
publicRuntimeConfig.passwordSettings.	maxLength	Максимальная длина пароля. Значение: 255. Если указать значение меньше, чем minLength (минимальная длина пароля), то система должна считать, что maxLength = minLength	2.2.0	-
publicRuntimeConfig.validationModel.	login	<p>Регулярные выражения для валидации логина пользователя:</p> <ol style="list-style-type: none"> Поле обязательно для заполнения: <ul style="list-style-type: none"> regex: <code>^.+</code> message: required Требования к формату значения: <ul style="list-style-type: none"> regex: <code>^([^<>() \[\] \\. , ; : \s @ »] + (\. [^<>() \[\] \\. , ; : \s @ »] +) *) @ ((\[[[0 - 9] { 1 , 3 } \. [0 - 9] { 1 , 3 } \. [0 - 9] { 1 , 3 } \. [0 - 9] { 1 , 3 }]]) (([a - z A - Z a - я A - Я ё Ё \ - 0 - 9] + \.) + [a - z A - Z a - я A - Я ё Ё] { 2 , } \. ?)) \$</code> message: invalidEmail Требование к длине: <ul style="list-style-type: none"> regex: <code>^{0,255}</code> message: maxLength messageArgs: <ul style="list-style-type: none"> • maxLength: 255 	2.2.0	-
serverRuntimeConfig.tls.	enabled	Флаг включения TLS протокола	2.2.0	-

Параметр		Описание	Добавлено	Удалено
serverRuntimeC onfig.tls.	private_key	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу config_folder/app_name/app_name.key	2.2.0	-
serverRuntimeC onfig.tls.	certificate	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу config_folder/app_name/app_name.crt	2.2.0	-
serverRuntimeC onfig.tls.	ca_certificate	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0	-

8.1.8. Конфигурационный файл сервиса ocs-auth-server-admin (файл: [/var/ocs/auth/ocs-auth-server-admin/ocs-auth-server-admin.yml](#))

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-auth-server-admin приведено в таблице (Таблица 33).

Таблица 33

Параметр		Описание	Добавлено	Удалено
sqa.	opt_out	Флаг отключения передачи телеметрии анонимной статистики hydra Возможные значения: true - отключает телеметрию	2.2.0	-

Параметр		Описание	Добавлено	Удалено
log.	level	Уровень детализации логирования. Возможные значения: "panic", "fatal", "error", "warn", "info", "debug" По умолчанию выбран уровень «info»	2.2.0	-
log.	format	Формат вывода логов. Возможные значения: json	2.2.0	-
serve.	forced_http	Можно ли использовать протокол http. Включается только для разработки. Влияет на параметр установки сессионных кук и на редирект на незащищенные ссылки по протоколу http	2.2.0	-
serve.	insecure_redirects	Список ссылок, на которые можно делать редирект по протоколу http	2.2.0	-
serve.public	port	Номер порта публичного API	2.2.0	-
serve.public.cors.	enabled	Флаг включения механизма CORS для публичного API: https://developer.mozilla.org/ru/docs/Web/HTTP/CORS Возможные значения: false auth_code: 10m, true	2.2.0	-
serve.public.access_log.	disable_for_health	Флаг отключения логов доступа для HEALTH-запросов к публичному API.	2.2.0	-
serve.admin.	port	Номер порта административного API	2.2.0	-
serve.admin.cors.	enabled	Флаг включения механизма CORS для административного API: https://developer.mozilla.org/ru/docs/Web/HTTP/CORS	2.2.0	-
serve.admin.cors.	exposed_headers	не используется так как <code>serve.admin.cors.enabled = false</code>	2.2.0	-
serve.admin.cors.	allow_credentials	не используется так как <code>serve.admin.cors.enabled = false</code>	2.2.0	-
serve.admin.cors.	max_age	не используется так как <code>serve.admin.cors.enabled = false</code>	2.2.0	-

Параметр		Описание	Добавлено	Удалено
serve.admin.cors.	debug	не используется так как <code>serve.admin.cors.enabled = false</code>	2.2.0	-
serve.admin.access_log.	disable_for_health	Флаг отключения логов доступа для HEALTH-запросов к публичному API	2.2.0	-
serve.tls.	allow_termination_from	Список доверенных подсетей (хостов), из которых разрешено принимать терминированный HTTP трафик в формате: <code>x.x.x.x/x</code> . Например, <code>10.189.200.0/24</code> (для подсетей); <code>10.189.200.1/32</code> (для хостов).	2.2.0	-
serve.tls.	mtls-enabled	Флаг включения TLS протокола	2.2.0	-
serve.tls.key	path	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу <code>config_folder/app_name/app_name.key</code>	2.2.0	-
serve.tls.cert	path	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу <code>config_folder/app_name/app_name.crt</code>	2.2.0	-
serve.tls.cert-ca	path	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу <code>config_folder/ca.crt</code>	2.2.0	-
serve.tls	skip_forwarded_protocol_check	Флаг, отменяющий проверку X-Forwarded-Proto заголовка при небезопасном соединении	2.2.1	-
dsn		Имя источника данных, адрес подключения к базе данных. Например: <code>postgres://user:password@host:123/database</code>	2.2.0	-

Параметр		Описание	Добавлено	Удалено
oidc.subject_identifiers.enabled		Алгоритм идентификации субъекта. Hydra поддерживает два алгоритма идентификации субъекта: (http://openid.net/specs/openid-connect-core-1_0.html#SubjectIDTypes) – public: Предоставление одинаковое значение sub (subject) для всех Клиентов (openid). – pairwise: Предоставление отличных значений sub для каждого Клиента, чтобы клиенты не могли соотнести действия конечного пользователя без разрешения.	2.2.0	-
oidc.subject_identifiers.pairwise	salt	Соль для шифрования sub идентификатора. <i><u>Это значение не должно изменяться после установки в производстве. Его изменение приведет к тому, что все клиентские приложения получат новые идентификаторы пользователей от ORY Hydra, что приведет к серьезным осложнениям с аутентификацией на их стороне!</u></i>	2.2.0	-
oidc.dynamic_client_registration	default_scope	Скоуп по умолчанию для динамически зарегистрированных клиентов. Используется только, если при регистрации скоуп не был передан.	2.2.0	-
urls.self	issuer	URL, который будет использован в поле «издатель» в токенах доступа (access token) и идентификации (id token). URL должен использовать HTTPS-протокол, иначе придется использовать флаг --dangerous-force-http при запуске hydra.	2.2.0	-
urls.self	public	URL публичного API сервиса аутентификации. Обычно должен совпадать с URL, переданным в urls.self.issuer.	2.2.0	-

Параметр		Описание	Добавлено	Удалено
urls.	login	URL для пути login, части User Login & Consent flow.	2.2.0	-
urls.	consent	URL для пути consent, части User Login & Consent flow.	2.2.0	-
urls.	logout	URL для пути logout, части User Login & Consent flow.	2.2.0	-
urls.	error	URL для пути error, hydra перенаправляет пользователя на данный URL, в случае ошибки OAuth2	2.2.0	-
urls.	post_logout_redirect	URL на который hydra будет перенаправлять пользователя после того, как пользователь вышел из системы.	2.2.0	-
strategies.	scope	Способ сравнения скоупов. Возможные значения: DEPRECATED_HIERARCHICAL_SCOPE_STRATEGY https://www.ory.sh/docs/oryos.10/oathkeeper/api-access-rules#scope-strategies	2.2.0	-
oauth2.	expose_internal_errors	Установите этот параметр в true, если нужно получить отладочную информацию об ошибке OAuth 2.0 клиентов. Это отладочная информация очень ценна при работе с ошибками, но это так же может вынести наружу ошибку с базы данных.	2.2.0	-
oauth2.has_hers.bcrypt.	cost	Уровень использования CPU для генерации хеш-сумм. Минимальное значение: 4. Значение по умолчанию: 10.	2.2.0	-
secrets.	system	Ключи для шифрования системной информации	2.2.0	-
secrets.	cookie	Ключи для шифрования cookie, передаваемые в браузер	2.2.0	-

8.1.9. Конфигурационный файл сервиса ocs-auth-server-public (файл: /var/ocs/auth/ocs-auth-server-public/ocs-auth-server-public.yml)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-auth-server-public приведено в таблице (Таблица 34).

Таблица 34

Параметр		Описание	Добавлено	Удалено
sqa.	opt_out	Флаг отключения передачи телеметрии анонимной статистики hydra Возможные значения: true - отключает телеметрию	2.2.0	-
log.	level	Уровень детализации логирования. Возможные значения: "panic", "fatal", "error", "warn", "info", "debug" По умолчанию выбран уровень "info"	2.2.0	-
log.	format	Формат вывода логов. Возможные значения: json	2.2.0	-
serve.	forced_http	Можно ли использовать протокол http. Включается только для разработки. Влияет на параметр установки сессионных кук и на редирект на незащищенные ссылки по протоколу http	2.2.0	-
serve.	insecure_redirects	Список ссылок, на которые можно делать редирект по протоколу http	2.2.0	-
serve.public	port	Номер порта публичного API	2.2.0	-

Параметр		Описание	Добавлено	Удалено
serve.public.cors.	enabled	Флаг включения механизма CORS для публичного API: https://developer.mozilla.org/ru/docs/Web/HTTP/CORS Возможные значения: "false", "true", "auth_code: 10m"	2.2.0	-
serve.public.access_log.	disable_for_health	Флаг отключения логов доступа для HEALTH-запросов к публичному API.	2.2.0	-
serve.admin.	port	Номер для порта административного API	2.2.0	-
serve.admin.cors.	enabled	Флаг включения механизма CORS для административного API: https://developer.mozilla.org/ru/docs/Web/HTTP/CORS	2.2.0	-
serve.admin.cors.	exposed_headers	не используется так как <code>serve.admin.cors.enabled = false</code>	2.2.0	-
serve.admin.cors.	allow_credentials	не используется так как <code>serve.admin.cors.enabled = false</code>	2.2.0	-
serve.admin.cors.	max_age	не используется так как <code>serve.admin.cors.enabled = false</code>	2.2.0	-
serve.admin.cors.	debug	не используется так как <code>serve.admin.cors.enabled = false</code>	2.2.0	-
serve.admin.access_log.	disable_for_health	Флаг отключения логов доступа для HEALTH-запросов к публичному API.	2.2.0	-
serve.tls.	allow_termination_from	Список доверенных подсетей (хостов), из которых разрешено принимать терминированный HTTP трафик в формате: x.x.x.x/x. Например, 10.189.200.0/24 (для подсетей); 10.189.200.1/32 (для хостов).	2.2.0	-
serve.tls.	mtls-enabled	Флаг включения TLS протокола	2.2.0	-
serve.tls.key	path	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу <code>config_folder/app_name/app_name.key</code>	2.2.0	-

Параметр		Описание	Добавлено	Удалено
serve.tls.cert	path	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу config_folder/app_name/app_name.crt	2.2.0	-
serve.tls.cert-ca	path	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0	-
serve.tls.skip_forwarded_proto_check	skip_forwarded_proto_check	Флаг, отменяющий проверку X-Forwarded-Proto заголовка при небезопасном соединении	2.2.1	-
dsn		Имя источника данных, адрес подключения к базе данных. Например: postgres://user:password@host:123/database	2.2.0	-
oidc.subject_identifiers.enabled	enabled	Алгоритм идентификации субъекта. Hydra поддерживает два алгоритма идентификации субъекта: (http://openid.net/specs/openid-connect-core-1_0.html#SubjectIDTypes) <ul style="list-style-type: none"> - public: Предоставление одинаковое значение sub (subject) для всех Клиентов (openid). - pairwise: Предоставление отличных значений sub для каждого Клиента, чтобы клиенты не могли соотнести действия конечного пользователя без разрешения 	2.2.0	-

Параметр		Описание	Добавлено	Удалено
oidc.subject_identifiers_pairwise.	salt	Соль для шифрования sub идентификатора. <i>Это значение не должно изменяться после установки в производстве. Его изменение приведет к тому, что все клиентские приложения получат новые идентификаторы пользователей от ORY Hydra, что приведет к серьезным осложнениям с аутентификацией на их стороне!</i>	2.2.0	-
oidc.dynamic_client_registration.	default_scope	Скоуп по умолчанию для динамически зарегистрированных клиентов. Используется только, если при регистрации скоуп не был передан	2.2.0	-
urls.self.	issuer	URL, который будет использован в поле «издатель» в токенах доступа (access token) и идентификации (id token). URL должен использовать HTTPS-протокол, иначе придется использовать флаг --dangerous-force-http при запуске hydra	2.2.0	-
urls.self.	public	URL публичного API сервиса аутентификации. Обычно должен совпадать с URL, переданным в urls.self.issuer	2.2.0	-
urls.	login	URL для пути login, части User Login & Consent flow	2.2.0	-
urls.	consent	URL для пути consent, части User Login & Consent flow	2.2.0	-
urls.	logout	URL для пути logout, части User Login & Consent flow	2.2.0	-
urls.	error	URL для пути error, hydra перенаправляет пользователя на данный URL, в случае ошибки OAuth2	2.2.0	-

Параметр		Описание	Добавлено	Удалено
urls.	post_logout_redirect	URL на который hydra будет перенаправлять пользователя после того, как пользователь вышел из системы	2.2.0	-
strategies.	scope	Способ сравнения скоупов. Возможные значения: DEPRECATED_HIERARCHICAL_SCOPE_STRATEGY https://www.ory.sh/docs/oryos.10/oauth-keeper/api-access-rules#scope-strategies	2.2.0	-
oauth2.	expose_internal_errors	Установите этот параметр в true, если нужно получить отладочную информацию об ошибке OAuth 2.0 клиентов. Это отладочная информация очень ценна при работе с ошибками, но это так же может вынести наружу ошибку с базы данных	2.2.0	-
oauth2.hashers.bcrypt.	cost	Уровень использования CPU для генерации хеш-сумм. Минимальное значение: 4. Значение по умолчанию: 10	2.2.0	-
secrets.	system	Ключи для шифрования системной информации	2.2.0	-
secrets.	cookie	Ключи для шифрования cookie, передаваемые в браузер	2.2.0	-

8.2. Конфигурационные файлы ПМ

8.2.1. Общий конфигурационный файл ПМ (файл: /var/ocs/appstore/config.yml)

Файл содержит общие настройки, которые могут использовать любые сервисы.

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров общего конфигурационного файла ПМ общий приведено в таблице (Таблица 35).

Таблица 35

Параметр	Описание	Добавлено	Удалено
config.insecureUri	Флаг использования незащищенного соединения. Этот параметр надо задавать в true если используется незащищенное соединение (http протокол). Он влияет на формирование Cookie заголовков, проверку редиректов.	2.2.0	-
config.publicUris.auth.publicUri	Полный адрес публичного API сервера авторизации	2.2.1	-
config.publicUris.auth.adminUri	Полный адрес API/UI консоли подсистемы безопасности	2.2.1	-
config.publicUris.aps.devUri	Полный адрес API/UI консоли разработчика	2.2.1	-
config.publicUris.aps.devBasepath	Префикс API/UI консоли разработчика	2.2.1	-
config.publicUris.aps.adminBasepath	Префикс в url для консоли администратора Аврора Маркет	2.2.1	-
config.publicUris.aps.clientUri	Полный адрес клиентского API Аврора Маркет. Это API используется мобильным приложением Аврора Маркет и подсистемой EMM	2.2.1	-
config.publicUris.aps.clientCdnUri	Полный адрес API для получения статических файлов для мобильного клиента Аврора Маркет. Если есть CDN то тут должна быть указана ссылка на CDN, если нет - должна быть указана ссылка на клиентское API Аврора Маркет	2.2.1	-

Параметр	Описание	Добавлено	Удалено
config.publicUri.aps.devCdnUri	Полный адрес API для получения статических файлов для UI консоли разработчика. Если есть CDN то тут должна быть указана ссылка на CDN, если нет - должна быть указана ссылка на API консоли разработчика	2.2.1	-
config.publicUri.aps.adminCdnUri	Полный адрес API для получения статических файлов для UI консоли администратора Аврора Маркет. Если есть CDN, то тут должна быть указана ссылка на CDN, если нет - должна быть указана ссылка на API консоли администратора Аврора Маркет	2.2.1	-
config.publicUri.emm.adminUri	Полный адрес API/UI консоли администратора EMM	2.2.1	-
config.systemUri.auth.publicAddress	Адрес публичного API авторизации - для межсистемного взаимодействия	2.2.1	-
config.systemUri.auth.publicBasepath	Префикс публичного API авторизации - для межсистемного взаимодействия	2.2.1	-
config.systemUri.auth.adminAddress	Адрес административного API авторизации - для межсистемного взаимодействия	2.2.1	-
config.systemUri.auth.adminBasepath	Префикс административного API авторизации - для межсистемного взаимодействия	2.2.1	-
config.session.rememberFor	Время жизни сессии пользователя консоли	2.2.0	-
config.session.renewTimeout	Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а один раз за данный интервал)	2.2.0	-
config.oidcClients.apsAdminConsole.scope	Скопы для oidc клиента, который используется для аутентификации в консоли администратора	2.2.0	-

Параметр	Описание	Добавлено	Удалено
config.oidcClients.apsAdminConsole.returnUri	Адрес, на который сервер авторизации сделает редирект после аутентификации в консоли администратора	2.2.0	-
config.oidcClients.apsDevConsole.scope	Скопы для oidc клиента, который используется для аутентификации в консоли разработчика	2.2.0	-
config.oidcClients.apsDevConsole.returnUri	Адрес, на который сервер авторизации сделает редирект после аутентификации в консоли разработчика	2.2.0	-
config.database.host	Адрес (хост) базы данных	2.2.0	-
config.database.port	Порт базы данных	2.2.0	-
config.database.user	Имя пользователя базы данных	2.2.0	-
config.database.dbname	Имя базы данных	2.2.0	-
config.database.password	Пароль базы данных	2.2.0	-
config.logger.level	Уровень детализации сообщений логирования. Возможные значения: debug, info, warn, error	2.2.0	-
config.logger.caller	Флаг включения в сообщение лога названия функции и номера строки, в которой происходит логирование события	2.2.0	-
config.logger.gateway_gin_log_enabled	Флаг включения логирования входящего запроса на шлюзе (url запроса и http-статус ответа)	2.2.1	-
config.redis.sentinelAddress	Адрес модуля sentinel СУБД Redis	2.2.0	-
config.redis.sentinelPassword	Пароль к модулю sentinel СУБД Redis	2.2.0	-
config.redis.masterName	Идентификатор (имя) БД Redis	2.2.0	-
config.redis.password	Пароль к СУБД Redis	2.2.0	-

Пример конфигурационного файла:

```
config:
  insecureUri: true
  publicUris:
    auth:
      publicUri: "http://feat-2-ocs.ompcloud.ru:8018"
      adminUri: "http://inplapsfeat02.ompcloud:8019"
    aps:
      devUri: "http://inplapsfeat02.ompcloud:8014"
      devBasepath: ""
      adminBasepath: ""
      clientUri: "http://feat-2-ocs.ompcloud.ru:8016"
      clientCdnUri: "http://feat-2-ocs.ompcloud.ru:8016"
      devCdnUri: "http://inplapsfeat02.ompcloud:8014"
      adminCdnUri: "http://inplapsfeat02.ompcloud:8015"
    emm:
      adminUri: "http://inplapsfeat02.ompcloud:8011"
  systemUris:
    # These are system links; they are used to configure
intersubsystem interaction.
    # Only change if it is really necessary.
  auth:
    publicAddress: "http://ocs-auth-public-api-gw.local"
    publicBasepath: ""
    adminAddress: "http://ocs-auth-admin-api-gw.local"
    adminBasepath: ""
  session:
    rememberFor: "5m"
    renewTimeout: "1m"
  oidcClients:
    apsDevConsole:
      scope: "openid offline application:read application:update
application:delete release:read release:update category:read
build:update icon:update icon:read screenshot:update screenshot:delete
screenshot:read"
```

```
    returnUri: "http://inplapsfeat02.ompccloud:8014"
  apsAdminConsole:
    scope: "openid offline application:read release:read
release:update icon:read category:read"
    returnUri: "http://inplapsfeat02.ompccloud:8015"
  database:
    host: "inplapsfeat02.ompccloud"
    port: "5432"
    user: "appstore"
    dbname: "appstore"
    password: "fdasfsaf"
    debug: false
  redis:
    sentinelAddresses: "inplapsfeat02.ompccloud:26379"
    sentinelPassword: "asfasfaf"
    masterName: "redis-ocs"
    password: "asfsafaf"
  transport:
    http:
      address: ":8080"
      tls:
        enabled: false
      shutDownTime: "15s"
    nats:
      url: "nats://FF12fddgdhFLL_feat-
2@inplapsfeat02.ompccloud:4222"
      clusterID: "ocs"
  zipkin:
    address: ""
  logger:
    level: "debug"
    caller: true
    gateway_gin_log_enabled: true

ocs-appstore-applications-api:
```

```
filestorage:
  rootFolderPath: "/ocs/appstore/applications-api"
```

8.2.2. Конфигурационный файл сервиса ocs-appstore-adminconsole-ui (файл: /var/ocs/appstore/ocs-appstore-adminconsole-ui/ocs-appstore-adminconsole-ui.yml)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-appstore-adminconsole-ui приведено в таблице (Таблица 36).

Таблица 36

Параметр		Описание	Добавлено	Удалено
publicRuntimeConfig.	contextRoot	Относительный базовый путь для страниц UI Пример: "/appstore/admin"	2.2.0	-
publicRuntimeConfig.	apiContextRoot	Относительный базовый путь для запросов API Пример: "/appstore/admin/api"	2.2.0	-
publicRuntimeConfig.	apsDevconsoleURL	Ссылка на Консоль разработчика	2.2.0	-
publicRuntimeConfig.session.	renewTimeout	Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а один раз за данный интервал)	2.2.0	-
publicRuntimeConfig.session.	renewUri	URL для продления сессии пользователя консоли	2.2.0	-
publicRuntimeConfig.session.	oidcRenewUri	URL для продления OIDC сессии	2.2.0	-
publicRuntimeConfig.	logoutUri	URL выхода из системы	2.2.0	-

Параметр		Описание	Добавлено	Удалено
defaultDashboard.qrCode.	name	Имя предоставляемой витрины приложений	2.2.0	-
defaultDashboard.qrCode.	url	URL витрины приложений	2.2.0	-
defaultDashboard.qrCode.	apiPrefix	Префикс API для доступа к витрине. Например: "api/v1"	2.2.0	-
defaultDashboard.	link	URL витрины для подключения по ссылке из МУ	2.2.0	-
publicRuntimeConfig.menuItems.monitoring.	label	Название пункта меню раздела мониторинга	2.2.0	-
publicRuntimeConfig.menuItems.monitoring.	url	Ссылка на раздел мониторинга	2.2.0	-
publicRuntimeConfig.menuItems.control.	label	Название пункта меню раздела управления	2.2.0	-
publicRuntimeConfig.menuItems.control.	url	Ссылка на раздел управление	2.2.0	-
publicRuntimeConfig.menuItems.control.tabs.devices.	label	Название пункта меню подраздела устройства, раздела управление	2.2.0	-
publicRuntimeConfig.menuItems.control.tabs.devices.	url	Ссылка на подраздел устройства, раздела управление	2.2.0	-
publicRuntimeConfig.menuItems.control.tabs.users.	label	Название пункта меню подраздела пользователя, раздела управление	2.2.0	-
publicRuntimeConfig.menuItems.control.tabs.users.	url	Ссылка на подраздел пользователя, раздела управление	2.2.0	-
publicRuntimeConfig.menuItems.control.tabs.policies.	label	Название пункта меню подраздела политики, раздела управление	2.2.0	-
publicRuntimeConfig.menuItems.control.tabs.policies.	url	Ссылка на подраздел политики, раздела управление	2.2.0	-

Параметр		Описание	Добавлено	Удалено
publicRuntimeConfig. menuItems.control.tab s.applications.	label	Название пункта меню подраздела приложения, раздела управление	2.2.0	-
publicRuntimeConfig. menuItems.control.tab s.applications.	url	Ссылка на подраздел приложения, раздела управление	2.2.0	-
publicRuntimeConfig. menuItems.control.tab s.dashboards.	label	Название пункта меню подраздела витрины, раздела управление	2.2.0	-
publicRuntimeConfig. menuItems.control.tab s.dashboards.	url	Ссылка на подраздел витрины, раздела управление	2.2.0	-
publicRuntimeConfig. menuItems.administra tion.	label	Название пункта меню раздела администрирование	2.2.0	-
publicRuntimeConfig. menuItems.administra tion.	url	Ссылка на раздел администрирование	2.2.0	-
publicRuntimeConfig.e ndpoints.getApplicatio ns.	path	Относительный путь API запроса списка приложений Пример: "/applications"	2.2.0	-
publicRuntimeConfig.e ndpoints.getApplicatio ns.	method	HTTP-метод API запроса списка приложений Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.e ndpoints.getCategories .	path	Относительный путь API запроса списка категорий Пример: "/categories"	2.2.0	-
publicRuntimeConfig.e ndpoints.getCategories .	method	HTTP-метод API запроса списка категорий Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.e ndpoints.getApplicatio nReleases.	path	Относительный путь API запроса списка релизов приложения Пример: "/applications/{applicationId}/rele ases"	2.2.0	-

Параметр		Описание	Добавлено	Удалено
publicRuntimeConfig.endpoints.getApplicationReleases.	method	HTTP-метод API запроса списка релизов приложения Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.approveRelease.	path	Относительный путь API запроса подтверждения релиза Пример: "/applications/{applicationId}/releases/{releaseId}/approve"	2.2.0	-
publicRuntimeConfig.endpoints.approveRelease.	method	HTTP-метод API запроса подтверждения релиза Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.rejectRelease.	path	Относительный путь API запроса отклонения релиза Пример: "/applications/{applicationId}/releases/{releaseId}/approve"	2.2.0	-
publicRuntimeConfig.endpoints.rejectRelease.	method	HTTP-метод API запроса отклонения релиза Пример: GET POST PUT DELETE	2.2.0	-
publicRuntimeConfig.endpoints.getReleaseArchive.	path	Относительный путь API запроса скачивания архива с информацией о релизе Пример: "/applications/{applicationId}/releases/{releaseId}/archive"	2.2.0	-
publicRuntimeConfig.endpoints.getReleaseArchive.	method	HTTP-метод API запроса скачивания архива с информацией о релизе Пример: GET POST PUT DELETE	2.2.0	-
serverRuntimeConfig.tls.	enabled	Флаг включения TLS протокола	2.2.0	-
serverRuntimeConfig.tls.	private_key	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу config_folder/app_name/app_name.key	2.2.0	-

Параметр		Описание	Добавлено	Удалено
serverRuntimeConfig.tls.	certificate	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу config_folder/app_name/app_name.crt	2.2.0	-
serverRuntimeConfig.tls.	ca_certificate	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0	-
serverRuntimeConfig.	pathToEula	Путь к файлу с лицензионным соглашением	2.2.0	-
serverRuntimeConfig.endpoints.getApplications.	path	URL API запроса списка приложений Пример: "http://ocs-appstore-adminconsole-api-gateway.local/api/applications"	2.2.0	-
serverRuntimeConfig.endpoints.getApplications.	method	HTTP-метод API запроса списка приложений Пример: GET POST PUT DELETE	2.2.0	-
serverRuntimeConfig.endpoints.getCategories.	path	URL API запроса списка категорий Пример: "http://ocs-appstore-adminconsole-api-gateway.local/api/categories"	2.2.0	-
serverRuntimeConfig.endpoints.getCategories.	method	Пример: GET POST PUT DELETE	2.2.0	-

8.2.3. Конфигурационный файл сервиса ocs-appstore-applications-api (файл: [/var/ocs/appstore/ocs-appstore-applications-api/ocs-appstore-applications-api.yml](#))

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-appstore-applications-api приведено в таблице (Таблица 37).

Таблица 37

Параметр		Описание	Добавлено	Удалено
config.logger.	level	Уровень детализации сообщений логирования. Возможные значения: debug, info, warn, error	2.2.0	-
config.logger.	caller	Флаг включения в сообщение лога названия функции и номера строки, в которой происходит логирование события	2.2.0	-
config.logger.	humanReadable	Флаг включения форматирования сообщений лога в обычный текст (не json)	2.2.0	-
config.database.	dialect	Тип базы данных для ORM, мы используем "postgres"	2.2.0	-
config.database.	args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
config.database.	debug	Флаг подключения к базе данных в режиме отладки для вывода запросов в стандартный вывод программы	2.2.0	-
config.filestorage.	rootFolderPath	Путь к директории-хранилищу бинарных данных: иконки, скриншоты, билды	2.2.0	-
config.filestorage.	bufferSize	Размер буфера при отправке бинарных данных клиенту Например: 1024000	2.2.0	-
config.	headerKeyForUserID	Имя HTTP-заголовка, содержащего идентификатор текущего пользователя	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.transport.http.address	address	Номер порта, на котором запускается приложение (":8080")	2.2.0	-
config.transport.http.tls.enabled	enabled	Флаг включения TLS протокола	2.2.0	-
config.transport.http.tls.private_key	private_key	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу config_folder/app_name/app_name.key	2.2.0	-
config.transport.http.tls.certificate	certificate	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу config_folder/app_name/app_name.crt	2.2.0	-
config.transport.http.tls.ca_certificate	ca_certificate	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0	-
config.transport.HTTPDebug.address	address	Номер порта, по которому запускаются служебные debug-эндпоинты приложения (":8080") При незаполненном значении совпадает с config.transport.http.address	2.2.0	-
config.transport.HTTPDebug.enabled	enabled	[не используется] Флаг включения TLS протокола (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.private_key	private_key	[не используется] Путь к файлу с приватным ключом (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.certificate	certificate	[не используется] Путь к файлу с сертификатом (публичный ключ) (для служебных debug-эндпоинтов приложения)	2.2.0	-
config.transport.HTTPDebug.ca_certificate	ca_certificate	[не используется] Путь к файлу с доверенным сертификатом (для служебных debug-эндпоинтов)	2.2.0	-

Параметр		Описание	Добавлено	Удалено
		приложения)		
config.transport.	shutdownTime	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.2.0	-
config.jaeger.	address	Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/)	2.2.0	-
config.	enableProf	Флаг включения отладочного профилировщика	2.2.0	-
config.	CDNURL	Адрес хоста CDN	2.2.0	2.2.1

8.2.4. Конфигурационный файл сервиса ocs-appstore-devconsole-ui (файл: </var/ocs/appstore/ocs-appstore-devconsole-ui/ocs-appstore-devconsole-ui.yml>)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-appstore-devconsole-ui приведено в таблице (Таблица 38).

Таблица 38

Параметр		Описание	Добавлено	Удалено
config.publicRuntimeConfig.	contextRoot	Относительный базовый путь для страниц UI Например: "/appstore/dev"	2.2.0	-
config.publicRuntimeConfig.	apiContextRoot	Относительный базовый путь для запросов API Например: "/appstore/dev/api"	2.2.0	-
config.publicRuntimeConfig.session.	renewTimeout	Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а один раз за данный интервал)	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.publicRuntimeConfig.session.renewUri	renewUri	URL для продления сессии пользователя консоли	2.2.0	-
config.publicRuntimeConfig.session.oidcRenewUri	oidcRenewUri	URL для продления OIDC сессии	2.2.0	-
config.publicRuntimeConfig.logoutUri	logoutUri	URL выхода из системы	2.2.0	-
config.publicRuntimeConfig.endpoints.getApplications.	path	Относительный путь API запроса списка приложений Пример: "/applications"	2.2.0	-
config.publicRuntimeConfig.endpoints.getApplications.	method	HTTP-метод API запроса списка ролей Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpoints.postApplications.	path	Относительный путь API запроса создания приложения Пример: "/applications"	2.2.0	-
config.publicRuntimeConfig.endpoints.postApplications.	method	HTTP-метод API запроса создания приложения Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpoints.putApplication.	path	Относительный путь API запроса обновления приложения Пример: "/applications/{id}"	2.2.0	-
config.publicRuntimeConfig.endpoints.putApplication.	method	HTTP-метод API запроса обновления приложения Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpoints.getApplication.	path	Относительный путь API запроса приложения Пример: "/applications/{id}"	2.2.0	-
config.publicRuntimeConfig.endpoints.getApplication.	method	HTTP-метод API запроса приложения Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpoints.deleteApplication.	path	Относительный путь API запроса приложения Пример: "/applications/{id}"	2.2.1	-
config.publicRuntimeConfig.endpoints.deleteApplication.	method	HTTP-метод API запроса приложения Пример: GET POST PUT DELETE	2.2.1	-

Параметр		Описание	Добавлено	Удалено
config.publicRuntimeConfig.endpoint.s.getReleases.	path	Относительный путь API запроса списка релизов приложений Пример: "/applications/{applicationId}/releases"	2.2.0	-
config.publicRuntimeConfig.endpoint.s.getReleases.	method	HTTP-метод API запроса списка релизов приложений Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpoint.s.getRelease.	path	Относительный путь API запроса релиза приложения Пример: "/applications/{applicationId}/releases/{id}"	2.2.0	-
config.publicRuntimeConfig.endpoint.s.getRelease.	method	HTTP-метод API запроса релиза приложения Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpoint.s.postRelease.	path	Относительный путь API запроса создания приложения Пример: "/applications/{applicationId}/releases"	2.2.0	-
config.publicRuntimeConfig.endpoint.s.postRelease.	method	HTTP-метод API запроса создания приложения Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpoint.s.putRelease.	path	Относительный путь API запроса обновления релиза Пример: "/applications/{applicationId}/releases/{id}"	2.2.0	-
config.publicRuntimeConfig.endpoint.s.putRelease.	method	HTTP-метод API запроса обновления релиза Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpoint.s.getCategories.	path	Относительный путь API запроса списка категорий Пример: "/categories"	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.publicRuntimeConfig.endpointCategories.getCategories.	method	HTTP-метод API запроса списка категорий Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpointBuild.postBuild.	path	Относительный путь API запроса добавления билда Пример: "/applications/{applicationId}/releases/{releaseId}/builds"	2.2.0	-
config.publicRuntimeConfig.endpointBuild.postBuild.	method	HTTP-метод API запроса добавления билда Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpointIcons.postIcon.	path	Относительный путь API запроса добавления иконки Пример: "/applications/{applicationId}/releases/{releaseId}/icons"	2.2.0	-
config.publicRuntimeConfig.endpointIcons.postIcon.	method	HTTP-метод API запроса добавления иконки Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpointScreenshots.postScreenshot.	path	Относительный путь API запроса добавления скриншота Пример: "/applications/{applicationId}/releases/{releaseId}/screenshots"	2.2.0	-
config.publicRuntimeConfig.endpointScreenshots.postScreenshot.	method	HTTP-метод API запроса добавления скриншота Пример: GET POST PUT DELETE	2.2.0	-
config.publicRuntimeConfig.endpointReviews.sendReleaseToReview.	path	Относительный путь API запроса отправки релиза на ревью Пример: "/applications/{applicationId}/releases/{releaseId}/review"	2.2.0	-
config.publicRuntimeConfig.endpointReviews.sendReleaseToReview.	method	HTTP-метод API запроса отправки релиза на ревью Пример: GET POST PUT DELETE	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.publicRuntimeConfig.endpoints.deleteScreenshot.	path	Относительный путь API запроса удаления скриншота Пример: "/applications/{applicationId}/releases/{releaseId}/screenshots/{screenshotId}"	2.2.0	-
config.publicRuntimeConfig.endpoints.deleteScreenshot.	method	HTTP-метод API запроса удаления скриншота Пример: GET POST PUT DELETE	2.2.0	-
config.serverRuntimeConfig.tls.	enabled	Флаг включения TLS протокола	2.2.0	-
config.serverRuntimeConfig.tls.	private_key	Путь к файлу с приватным ключом При незаполненном значении формируется по принципу config_folder/app_name/app_name.key	2.2.0	-
config.serverRuntimeConfig.tls.	certificate	Путь к файлу с сертификатом (публичный ключ) При незаполненном значении формируется по принципу config_folder/app_name/app_name.crt	2.2.0	-
config.serverRuntimeConfig.tls.	ca_certificate	Путь к файлу с доверенным сертификатом При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0	-
config.serverRuntimeConfig.endpoints.getAccount.	path	URL API запроса аккаунта Пример: "http://ocs-appstore-devconsole-api-gateway.local:8014/api/accounts/{id}"	2.2.0	-
config.serverRuntimeConfig.endpoints.getAccount.	method	HTTP-метод API запроса аккаунта Пример: GET POST PUT DELETE	2.2.0	-

Параметр		Описание	Добавлено	Удалено
config.serverRuntimeMeConfig.endpoints.getApplications.	path	URL API запроса списка приложений Пример: "http://ocs-appstore-devconsole-api-gateway.local:8014/api/applications"	2.2.0	-
config.serverRuntimeMeConfig.endpoints.getApplications.	method	HTTP-метод API запроса списка приложений Пример: GET POST PUT DELETE	2.2.0	-
config.serverRuntimeMeConfig.endpoints.getApplication.	path	URL API запроса приложения Пример: "http://ocs-appstore-devconsole-api-gateway.local:8014/api/applications/{id}"	2.2.0	-
config.serverRuntimeMeConfig.endpoints.getApplication.	method	HTTP-метод API запроса приложения Пример: GET POST PUT DELETE	2.2.0	-
config.serverRuntimeMeConfig.endpoints.getReleases.	path	URL API запроса списка релизов Пример: "http://ocs-appstore-devconsole-api-gateway.local:8014/api/applications/{applicationId}/releases"	2.2.0	-
config.serverRuntimeMeConfig.endpoints.getReleases.	method	HTTP-метод API запроса списка релизов Пример: GET POST PUT DELETE	2.2.0	-
config.serverRuntimeMeConfig.endpoints.getRelease.	path	URL API запроса релиза Пример: "http://ocs-appstore-devconsole-api-gateway.local:8014/api/applications/{applicationId}/releases/{id}"	2.2.0	-
config.serverRuntimeMeConfig.endpoints.getRelease.	method	HTTP-метод API запроса релиза Пример: GET POST PUT DELETE	2.2.0	-
config.serverRuntimeMeConfig.endpoints.getCategories.	path	URL API запроса списка категорий	2.2.0	-

Параметр		Описание	Добавлено	Удалено
		Пример: "http://ocs-appstore-adminconsole-api-gateway.local/api/categories"		
config.serverRuntimeConfig.endpoint.s.getCategories.	method	HTTP-метод API запроса списка категорий Пример: GET POST PUT DELETE	2.2.0	-

8.3. Описание конфигурационных файлов ПУ

8.3.1. Общий конфигурационный файл ПУ (файл: /var/ocs/emm/config.yml)

Файл содержит общие настройки, которые могут использовать любые сервисы.

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров общего конфигурационного файла ПУ приведено в таблице (Таблица 39).

Таблица 39

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.insecureUri	Использование незащищенного соединения. Этот параметр надо задавать в true если используется незащищенное соединение (http протокол). Он влияет на формирование Cookie заголовков, проверку редиректов.	true	2.2.0	-
config.publicUri. emm.mobileUri	Полный адрес API для МП «Аврора Центр»	http://example.cloud/emm/mobile	2.2.0	-

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.publicUri. emm.mobileCdnUri	Полный адрес для получения статических файлов через API для МП «Аврора Центр». Если есть CDN то тут должна быть указана ссылка на CDN, если нет - должна быть указана ссылка на API для МП «Аврора Центр»	http://cdn.com/emm/mobile	2.2.1	-
config.publicUri. emm.adminBasepath	Префикс админского API/UI EMM	/emm/admin	2.2.0	-
config.publicUri. emm.adminCdnUri	Полный адрес для получения статических файлов через админское API EMM. Если есть CDN то тут должна быть указана ссылка на CDN, если нет - должна быть указана ссылка на админское API EMM	http://example.cloud/emm/admin	2.2.0	-
config.publicUri. auth.publicUri	Полный адрес публичного API сервера авторизации	http://example.cloud/auth/public	2.2.0	-
config.publicUri. auth.adminUri	Полный адрес админского API/UI сервера авторизации	http://example.cloud/auth/admin	2.2.0	-
config.publicUri. aps.adminUri	Полный адрес админского API/UI подсистемы Aurora market	http://example.cloud/appstore/admin	2.2.0	-
config.systemUri. auth.publicAddress	Хост публичного API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия.	http://ocs-auth-admin-api-gw.local	2.2.0	-
config.systemUri. auth.publicBasepath	Префикс публичного API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия.	""	2.2.0	-

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.systemUris.auth.adminAddress	Хост админского API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия		2.2.1	-
config.systemUris.auth.adminBasepath	Префикс к админскому API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия.	""	2.2.1	-
config.systemUris.aps.marketAddress	Хост API подсистемы Aurora Market, используемый для внутреннего межподсистемного взаимодействия	http://ocs-appstore-client-api-gw.local	2.2.0	-
config.systemUris.aps.marketBasepath	Префикс к API подсистемы Aurora Market, используемый для внутреннего межподсистемного взаимодействия.	""	2.2.0	-
config.systemUris.pkgRepo.adminAddress	Хост админского API подсистемы обновлений, используемый для внутреннего межподсистемного взаимодействия.	http://ocs-pkgrepo-admin-api-gw.local	2.2.1	-
config.systemUris.pkgRepo.adminBasepath	Префикс к админскому API подсистемы обновлений, используемый для внутреннего межподсистемного взаимодействия.	""	2.2.1	-
config.redis.sentinelAddress	Адрес модуля sentinel СУБД Redis		2.2.0	-
config.redis.sentinelPassword	Пароль к модулю sentinel СУБД Redis		2.2.0	-
config.redis.masterName	Идентификатор (имя) БД Redis		2.2.0	-
config.redis.password	Пароль к СУБД Redis		2.2.0	-

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.session.rememberFor	Время жизни сессии	5m	2.2.0	-
config.session.renewTimeout	Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а один раз за данный интервал)		2.2.0	-
config.oidcClients.emmAdminConsole.scope	Скопы для oidc клиента, который используется для аутентификации в консоли администратора ЕММ		2.2.1	-
config.oidcClients.emmAdminConsole.returnUri	Адрес, на который сервер авторизации сделает редирект после аутентификации в консоли администратора emm		2.2.1	-
config.database.host	Адрес (хост) базы данных ПУ		2.2.0	-
config.database.port	Порт базы данных ПУ		2.2.0	-
config.database.user	Имя пользователя базы данных ПУ		2.2.0	-
config.database.dbname	Имя базы данных ПУ		2.2.0	-
config.database.password	Пароль базы данных ПУ		2.2.0	-
config.transport.address	Порт, на котором запускается сервис (модуль) ПУ Пример: ":8080"		2.2.0	-
config.transport.tls.enabled	Доступность TLS протокола		2.2.0	-
config.transport.shutdownDownTime	Время на завершение открытых соединений, перед тем, как сервис завершит работу		2.2.0	-
config.transport.nats.url	Адрес сервера NATS		2.2.0	-

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.transport.nats.clusterID	Идентификатор кластера NATS		2.2.0	-
config.zipkin.address	Адрес подключения к Zipkin		2.1.1	2.2.1
config.tracing.enabled	Доступность трейсера		2.2.1	-
config.tracing.sample_rate	Частота дискретизации трассировки		2.2.1	-
config.tracing.reporting_period	Отчетный период трассировки		2.2.1	-
config.tracing.jaeger_agent_endpoint	Адрес подключения к Jaeger		2.2.1	-
config.logger.level	Уровень детализации сообщений логирования. Возможные значения: <ul style="list-style-type: none"> - debug; - info; - warning; - error 		2.2.0	-
config.logger.caller	Признак включения в лог дополнительных полей (имя файла, название функции) <ul style="list-style-type: none"> - false; - true 	true	2.2.0	-
config.logger.gateway gin_log_enabled	Флаг включения логирования входящего запроса на шлюзе (url запроса и http-статус ответа)		2.2.1	-
qrCodeTtl	Время жизни QR-кода	5m	2.2.0	-
smtp.from	Адрес электронной почты, с которой отправляются письма		2.2.0	-
smtp.address	Адрес сервера эл. почты		2.2.0	-
smtp.from	Адрес электронной почты, с которой отправляются письма		2.2.0	-
smtp.address	Адрес сервера эл. почты		2.2.0	-

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
smtp.authType	Тип авторизации. Может принимать значения CRAM-MD5, PLAIN, либо не заполняться		2.2.1	-
smtp.identity	Идентификатор учетной записи пользователя, обычно совпадает с Username Заполняется, если тип авторизации PLAIN		2.2.1	-
smtp.username	Логин пользователя Заполняется, если тип авторизации PLAIN либо CRAM-MD5		2.2.1	-
smtp.password	Пароль пользователя Заполняется, если тип авторизации PLAIN		2.2.1	-
smtp.host	Адрес (хост) почтового сервера Заполняется, если тип авторизации PLAIN		2.2.1	-
smtp.secret	Ключ, с помощью которого подписываются hmac.md5 данные между сервером и клиентом Заполняется, если тип авторизации CRAM-MD5		2.2.1	-

Пример конфигурационного файла:

```
config:
  insecureUri: true
  publicUris:
    emm:
      mobileUri: "http://example.cloud/emm/mobile"
      adminBasepath: "/emm/admin"
      mobileCdnUri: "http://cdn.cloud/emm/mobile"
      adminCdnUri: "http://example.cloud/emm/admin"
  auth:
```

```
    publicUri: "http://example.cloud/auth/public"
    adminUri: "http://example.cloud/auth/admin"
  aps:
    adminUri: "http://example.cloud/appstore/admin"
  systemUris:
    # These are system links; they are used to configure
intersubsystem interaction.
    # Only change if it is really necessary.
  auth:
    publicAddress: "http://ocs-auth-public-api-gw.local"
    publicBasepath: ""
    adminAddress: "http://ocs-auth-admin-api-gw.local"
    adminBasepath: ""
  aps:
    marketAddress: "http://ocs-appstore-client-api-gw.local"
    marketBasepath: ""
  pkgRepo:
    adminAddress: "http://ocs-pkgrepo-admin-api-gw.local"
    adminBasepath: ""
  redis:
    sentinelAddresses: "localhost:26379"
    sentinelPassword: "some"
    masterName: "redis-ocs"
    password: "some"
  session:
    rememberFor: "5m"
    renewTimeout: "2m"
  oidcClients:
    emmAdminConsole:
      scope: "token:read"
      returnUrl: "http://example.cloud/emm/admin/"
  database:
    host: "localhost"
    port: "5432"
    user: "root"
```

```
    dbname: "ocs"
    password: "ocs"
transport:
  http:
    address: ":8080"
    tls:
      enabled: false
  shutDownTime: "15s"
  nats:
    url: "localhost:4222"
    clusterID: "ocs"
tracing:
  enabled: true
  sample_rate: 100
  reporting_period: 1
  jaeger_agent_endpoint: "localhost:6831"
logger:
  level: "error"
  caller: true
  gateway_gin_log_enabled: "false"
smtp:
  from: "no-reply@inplsfccloud03.ompccloud"
  address: "inplsfccloud03.ompccloud:1025"
  authType: ""
  identity: ""
  username: ""
  password: ""
  host: ""
  secret: ""
qrCodeTtl: "5m"
```

8.3.2. Конфигурационный файл сервиса ocs-emm-adminconsole-ui (файл: [/var/ocs/emm/ocs-emm-adminconsole-ui/ocs-emm-adminconsole-ui.yml](#))

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-emm-adminconsole-ui приведено в таблице (Таблица 40).

Таблица 40

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.publicRuntimeConfig.contextRoot	Относительный базовый путь для страниц пользовательского интерфейса. Например: "/emm/admin"	client: contextRoot: '' apiContextRoot: 'http://ocsdevapp01.ompccloud:8011/api'	2.2.0	-
config.publicRuntimeConfig.apiContextRoot	Относительный базовый путь для запросов API Например: "/emm/admin/api"		2.2.0	-
config.publicRuntimeConfig.session.renewTimeout	Интервал обновлений сессий аутентификации	session: renewTimeout: 1m renewUri: http://ocsdevapp01.ompccloud:8011/api/sessions/renew oidcRenewUri: http://ocsdevapp01.ompccloud:8018/oauth2/sessions/login/renew	2.2.0	-
config.publicRuntimeConfig.session.renewUri	Адрес вызова метода обновления сессии RP		2.2.0	-
config.publicRuntimeConfig.session.oidcRenewUri	Адрес вызова метода обновления сессии OIDC		2.2.0	-
config.publicRuntimeConfig.logoutUri	Uri выхода из системы	logoutUri: "/logout"	2.2.0	-

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.publicRuntimeConfig.menuItems.monitoring.label	Заголовок пункта основного меню «Мониторинг»	label: "Мониторинг"	2.2.0	-
config.publicRuntimeConfig.menuItems.monitoring.url	Адрес страницы для перехода по пункту основного меню «Мониторинг»	url: "/"	2.2.0	-
config.publicRuntimeConfig.menuItems.monitoring.tabs.indicators.label	Заголовок вкладки «Индикаторы» основного меню «Мониторинг»	label: "Индикаторы"	2.2.0	-
config.publicRuntimeConfig.menuItems.monitoring.tabs.indicators.url	Адрес страницы для перехода на вкладку «Индикаторы» основного меню «Мониторинг»	url: "/"	2.2.0	-
config.publicRuntimeConfig.menuItems.monitoring.tabs.audit.label	Заголовок вкладки «Аудит» основного меню «Мониторинг»	label: "Аудит"	2.2.0	-
config.publicRuntimeConfig.menuItems.monitoring.tabs.audit.url	Адрес страницы для перехода на вкладку «Аудит» основного меню «Мониторинг»	url: "http://ocsdevapp01.ompccloud:8019/ui/audit"	2.2.0	-
config.publicRuntimeConfig.menuItems.control.label	Заголовок пункта основного меню «Управление»	label: "Управление"	2.2.0	-
config.publicRuntimeConfig.menuItems.control.url	Адрес страницы для перехода по пункту основного меню «Управление»	url: "/management"	2.2.0	-

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.publicRuntimeConfig.menuItems.controls.devices.label	Заголовок вкладки «Устройства» основного меню «Управление»	label: "Устройства"	2.2.0	-
config.publicRuntimeConfig.menuItems.controls.devices.url	Адрес страницы для перехода на вкладку «Устройства» основного меню «Управление»	url: "/management"	2.2.0	-
config.publicRuntimeConfig.menuItems.controls.users.label	Заголовок вкладки «Пользователи» основного меню «Управление»	label: "Пользователи"	2.2.0	-
config.publicRuntimeConfig.menuItems.controls.users.url	Адрес страницы для перехода на вкладку «Пользователи» основного меню «Управление»	url: "/users"	2.2.0	-
config.publicRuntimeConfig.menuItems.controls.policyServices.label	Заголовок вкладки «Политики» основного меню «Управление»	label: "Политики"	2.2.0	-
config.publicRuntimeConfig.menuItems.controls.policyServices.url	Адрес страницы для перехода на вкладку «Политики» основного меню «Управление»	url: "/policyServices"	2.2.0	-
config.publicRuntimeConfig.menuItems.controls.applications.label	Заголовок вкладки «Приложения» основного меню control	label: "Приложения"	2.2.0	-
config.publicRuntimeConfig.menuItems.controls.applications.url	Адрес страницы для перехода на вкладку «Приложения» основного меню «Управление»	url: "http://ocsdevapp01.ompccloud:8015/ui"	2.2.0	-

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.publicRun timeConfig.men ultems.control.t abs.dashboards. url	Заголовок вкладки «Витрины» основного меню «Управление»	label: "Витрины"	2.2.0	-
config.publicRun timeConfig.men ultems.control.t abs.dashboards. url	Адрес страницы для перехода на вкладку «Витрины» основного меню «Управление»	url: \${aps.adminUri}/ui /dashboards	2.2.0	-
config.publicRun timeConfig.men ultems.administr ation.label	Заголовок пункта основного меню «Администрирование»	label: "Администрирование"	2.2.0	-
config.publicRun timeConfig.men ultems.administr ation.url	Адрес страницы для перехода по пункту основного меню «Администрирование»	url: "http://ocsdevapp0 1.ompccloud:8019/ui "	2.2.0	-
config.publicRun timeConfig.men ultems.administr ation.tabs.opera tors.label	Заголовок вкладки «Операторы» основного меню «Администрирование»	label: "Операторы"	2.2.0	-
config.publicRun timeConfig.men ultems.administr ation.tabs.opera tors.url	Адрес страницы для перехода на вкладку «Операторы» основного меню «Администрирование»	url: "http://ocsdevapp0 1.ompccloud:8019/ui /"	2.2.0	-
config.publicRun timeConfig.men ultems.administr ation.tabs.option s.label	Заголовок вкладки «Настройки» основного меню «Администрирование»	label: "Настройки"	2.2.0	-
config.publicRun timeConfig.men ultems.administr ation.tabs.option s.url	Адрес страницы для перехода на вкладку «Настройки» основного меню «Администрирование»	url: "/options"	2.2.0	-

Параметр	Описание	Пример значения (YAML)	Добавлено	Удалено
config.publicRuntimeConfig.menuItems.administration.tabs.orgStructure.label	Заголовок вкладки «Орг.структура» основного меню «Администрирование»	label: "Орг. структура"	2.2.0	-
config.publicRuntimeConfig.menuItems.administration.tabs.orgStructure.url	Адрес страницы для перехода на вкладку «Орг.структура» основного меню «Администрирование»	url: "/orgStructure"	2.2.0	-
config.serverRuntimeConfig.pathToEula	Путь к файлу с лицензионным соглашением	pathToEula: '/var/ocs/emm/ocs-emm-adminconsole-ui/eula.pdf'	2.2.1	-

8.3.3. Конфигурационный файл сервиса ocs-emm-applications-api (файл: </var/ocs/emm/ocs-emm-applications-api/ocs-emm-applications-api.yml>)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-emm-applications-api приведено в таблице (Таблица 41).

Таблица 41

Параметр	Описание	Добавлено	Удалено
Transport.Address	Адрес сервера и номер порта, на котором запускается приложение ("127.0.0.1:8080")	2.2.0	-
settings.appstore.address	Адрес сервера Аврора Маркет	2.2.0	-
Logger	Логирование. Параметры берутся из п. 8.3.1	2.2.0	-

8.3.4. Конфигурационный файл сервиса ocs-emm-devices-api (файл: /var/ocs/emm/ocs-emm-devices-api/ocs-emm-devices-api.yml)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-emm-devices-api приведено в таблице (Таблица 42).

Таблица 42

Параметр	Описание	Добавлено	Удалено
transport.addresses	Адрес сервера и номер порта, на котором запускается приложение ("127.0.0.1:8080")	2.2.0	-
transport.nats.url	Адрес сервера Nats (см. https://docs.nats.io/)	2.2.0	-
transport.nats.clusterID	Идентификатор кластера Nats	2.2.0	-
transport.nats.clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
transport.nats.DurableName	Имя очереди NATS для подписок с сохранением позиции.	2.2.0	-
transport.nats.MaxInflight	Максимальное кол-во доставляемых клиенту (или подписчику) сообщений без подтверждений	2.2.1	-
database.dialect	Тип базы данных для ORM, мы используем «postgres»	2.2.0	-
database.args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
logger	Логирование. Параметры берутся из п. 8.3.1	2.2.0	-

8.3.5. Конфигурационный файл сервиса ocs-emm-dispatcher-api (файл: /var/ocs/emm/ocs-emm-dispatcher-api/ocs-emm-dispatcher-api.yml)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-emm-dispatcher-api файла приведено в таблице (Таблица 43).

Таблица 43

Параметр	Описание	Добавлено	Удалено
transport.address	Адрес сервера и номер порта, на котором запускается приложение ("127.0.0.1:8080")	2.2.0	-
transport.nats.url	Адрес сервера NATS	2.2.0	-
transport.nats.durableName	Имя очереди NATS для подписок с сохранением позиции.	2.2.0	-
transport.nats.clusterID	Идентификатор кластера NATS	2.2.0	-
transport.nats.clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
natsSubject.deviceConnected	Событие обращения устройства к АММ	2.2.0	-
natsSubject.stateReceived	Событие получения состояния устройства	2.2.0	-
natsSubject.sdjdReceived	Событие получения SDJD событий устройства	2.2.0	-
database.dialect	Тип базы данных для ORM, мы используем «postgres»	2.2.0	-
database.args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword	2.2.0	-

Параметр	Описание	Добавлено	Удалено
	dbname=dbName sslmode=disable timezone=utc"		
deviceInventory.address	Адрес сервиса инвентаризации и управления устройствами (Devices)	2.2.0	-
stateManager.address	Адрес сервиса управления состоянием устройств (State Manager)	2.2.0	-
logger	Логирование. Параметры берутся из п. 8.3.1	2.2.0	-

Для настройки доступа к SMTP-серверу в сценариях получения логов с устройства на электронную почту также в конфигурационный файл необходимо добавить параметры, приведенные в таблице (Таблица 44).

Таблица 44

Параметр	Описание	Добавлено	Удалено
smtp.address	Адрес сервера эл. почты	2.2.1	-
smtp.from	Адрес эл. почты с которой отправляются письма	2.2.1	-
smtp.authType	Тип авторизации. Может принимать значения CRAM-MD5, PLAIN, либо не заполняться	2.2.1	-
smtp.identity	Идентификатор учетной записи пользователя, обычно совпадает с Username Заполняется для типа авторизации PLAIN	2.2.1	-
smtp.username	Логин пользователя Заполняется для типа авторизации PLAIN, CRAM-MD5	2.2.1	-
smtp.password	Пароль пользователя Заполняется для типа авторизации PLAIN	2.2.1	-
smtp.host	Адрес (хост) почтового сервера Заполняется для типа авторизации PLAIN	2.2.1	-
smtp.secret	Ключ, с помощью которого подписываются hmac.md5 данные между сервером и клиентом Заполняется для типа авторизации CRAM-MD5	2.2.1	-

8.3.6. Конфигурационный файл сервиса ocs-emm-enrollments-api (файл: /var/ocs/emm/ocs-emm-enrollments-api/ocs-emm-enrollments-api.yml)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-emm-enrollments-api файла приведено в таблице (Таблица 45).

Таблица 45

Параметр	Описание	Добавлено	Удалено
transport.address	Адрес сервера и номер порта, на котором запускается приложение ("127.0.0.1:8080")	2.2.0	-
transport.nats.url	Адрес сервера Nats	2.2.0	-
transport.nats.clusterID	Идентификатор кластера Nats	2.2.0	-
transport.nats.clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
database.dialect	Тип базы данных для ORM, мы используем «postgres»	2.2.0	-
database.args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
signUp.expire	Время жизни пароля учетной записи устройства (в процессе активации)	2.2.0	-
signUp.gatewayURI	Адрес сервера активации устройства	2.2.0	-
deviceInventory.url	Адрес к сервису управления устройствами	2.2.0	-
accountsClient.url	Адрес к сервису управления аккаунтами	2.2.0	-
logger	Логирование. Параметры берутся из п. 8.3.1	2.2.0	-

Для настройки доступа к SMTP-серверу в сценариях отправки QR-кода на электронную почту также в конфигурационный файл необходимо добавить параметры, приведенные в таблице (Таблица 46).

Таблица 46

Параметр	Описание	Добавлено	Удалено
smtp.Address	Адрес сервера эл. почты	2.2.0	-
smtp.authType	Тип авторизации. Может принимать значения CRAM-MD5, PLAIN, либо не заполняться	2.2.0	-
smtp.from	Адрес электронной почты, с которой отправляются письма	2.2.0	-
smtp.host	Адрес (хост) почтового сервера Заполняется для типа авторизации PLAIN	2.2.0	-
smtp.identity	Идентификатор учетной записи пользователя, обычно совпадает с Username Заполняется для типа авторизации PLAIN	2.2.0	-
smtp.password	Пароль пользователя Заполняется для типа авторизации PLAIN	2.2.0	-
smtp.secret	Ключ, с помощью которого подписываются hmac.md5 данные между сервером и клиентом Заполняется для типа авторизации CRAM-MD5	2.2.0	-
smtp.username	Логин пользователя Заполняется для типа авторизации PLAIN, CRAM-MD5	2.2.0	-

[8.3.7. Конфигурационный файл сервиса ocs-emm-policies-api \(файл: /var/ocs/emm/ocs-emm-policies-api/ocs-emm-policies-api.yml\)](#)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-emm-policies-api приведено в таблице (Таблица 47).

Таблица 47

Параметр	Описание	Добавлено	Удалено
transport.address	Адрес сервера и номер порта, на котором запускается приложение ("127.0.0.1:8080")	2.2.0	-
transport.nats.url	Адрес сервера NATS	2.2.0	-
transport.nats.clusterID	Идентификатор кластера NATS (https://docs.nats.io/)	2.2.0	-
transport.nats.clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
transport.nats.durableName	Имя очереди NATS для подписок с сохранением позиции (https://docs.nats.io/)	2.2.0	-
transport.nats.maxInflight	Максимальное кол-во доставляемых клиенту (или подписчику) сообщений без подтверждений	2.2.1	-
transport.nats.group	Группа подписчиков сообщений Nats	2.2.0	-
transport.nats.policyEventSubject	Событие назначения политики на устройство	2.2.0	-
database.dialect	Тип базы данных для ORM, мы используем «postgres»	2.2.0	-
database.args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
deviceInventoryServiceURL	Адрес сервиса инвентаризации и управления устройствами (Devices)	2.2.0	-
usersServiceURL	Адрес сервиса управления пользователями устройств (Users)	2.2.0	-
logger	Логирование. Параметры берутся из п. 8.3.1	2.2.0	-

8.3.8. Конфигурационный файл сервиса ocs-emm-reports-api (файл: /var/ocs/emm/ocs-emm-reports-api/ocs-emm-reports-api.yml)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-emm-reports-api приведено в таблице (Таблица 48).

Таблица 48

Параметр	Описание	Добавлено	Удалено
transport.address	Адрес сервера и номер порта, на котором запускается приложение ("127.0.0.1:8080")	2.2.0	-
transport.nats.url	Адрес сервера Nats	2.2.0	-
transport.nats.clusterID	Идентификатор кластера Nats (https://docs.nats.io/)	2.2.0	-
transport.nats.clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
transport.nats.MaxInflight	Максимальное кол-во доставляемых клиенту (или подписчику) сообщений без подтверждений	2.2.1	-
database.dialect	Тип базы данных для ORM, мы используем «postgres»	2.2.0	-
database.agrs	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
logger	Логирование. Параметры берутся из п. 8.3.1	2.2.0	-

8.3.9. Конфигурационный файл сервиса ocs-emm-state-manager-api (файл: </var/ocs/emm/ocs-emm-state-manager-api/ocs-emm-state-manager-api.yml>)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла ocs-emm-state-manager-api приведено в таблице (Таблица 49).

Таблица 49

Параметр	Описание	Добавлено	Удалено
transport.debugAddress	Адрес сервера и номер порта, на котором запускается приложение для отладки («127.0.0.1:8080»)	2.2.0	-
transport.shutdownTime	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.2.0	-
transport.address	Адрес сервера и номер порта, на котором запускается приложение («127.0.0.1:8080»)	2.2.0	-
transport.nats.url	Адрес сервера NATS	2.2.0	-
transport.nats.clusterID	Идентификатор кластера NATS (https://docs.nats.io/)	2.2.0	-
transport.nats.clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
transport.nats.maxInflight	Максимальное кол-во доставляемых клиенту (или подписчику) сообщений без подтверждений (минимальное значение 1)	2.2.1	-
transport.nats.durableName	Имя очереди NATS для подписок с сохранением позиции (https://docs.nats.io/)	2.2.0	-
transport.nats.maxRedelivered	Максимальное кол-во повторно доставляемых клиенту (или подписчику) сообщений без подтверждений (минимальное значение 1)	2.2.1	-

Параметр	Описание	Добавлено	Удалено
database.dialect	Тип базы данных для ORM, мы используем «postgres»	2.2.0	-
database.args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
dispatcher.address	Адрес сервиса Диспетчер устройств	2.2.0	-
Jaeger.address	Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/)	2.2.0	-
logger.filter.level	Уровень детализации сообщений логирования. Берется из файла loggerfilterlevel.go. Возможные значения: - debug; - info; - warn; - error	2.2.1 (до 2.2.1 назывался logger.level)	-

8.3.10. Конфигурационный файл сервиса ocs-emm-users-api (файл: [/var/ocs/emm/ocs-emm-users-api/ocs-emm-users-api.yml](#))

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла модуля ocs-emm-users-api приведено в таблице (Таблица 50).

Таблица 50

Параметр	Описание	Добавлено	Удалено
ldapServer.address	Адрес LDAP сервера пример: "ldap://msk1pdc.omp.ru"	2.3.0	-
ldapServer.userName	Логин от технической учетной записи от LDAP сервера	2.3.0	-

Параметр	Описание	Добавлено	Удалено
ldapServer.password	Пароль от технической учетной записи от LDAP сервера	2.3.0	-
ldapServer.parentGroup	Название группы, с которой будет происходить импорт данных орг. структуры из LDAP сервера	2.3.0	-
transport.debugAddress	Адрес сервера и номер порта, на котором запускается приложение для отладки («127.0.0.1:8080»)	2.2.0	-
transport.shutdownTime	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.2.0	-
transport.addresses	Адрес сервера и номер порта, на котором запускается приложение («127.0.0.1:8080»)	2.2.0	-
transport.nats.url	Адрес сервера Nats	2.2.0	-
transport.nats.clusterID	Идентификатор кластера NATS (https://docs.nats.io/)	2.2.0	-
transport.nats.clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
transport.nats.MaxInflight	Максимальное кол-во доставляемых клиенту (или подписчику) сообщений без подтверждений	2.2.1	-
database.dialect	Тип базы данных для ORM, мы используем «postgres»	2.2.0	-
database.agrs	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
deviceInventory.url	Адрес сервиса инвентаризации и управления устройствами (Devices)	2.2.0	-
enablePprof	Флаг включения отладочного профилировщика	2.2.0	-
Jaeger.address	Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/)	2.2.0	-
logger.filterLevel	Уровень детализации сообщений логирования. Берется из файла loggerfilterlevel.go. Возможные значения: - debug;	2.2.1	-

Параметр	Описание	Добавлено	Удалено
	<ul style="list-style-type: none"> - info; - warn; - error 		

8.3.11. Конфигурационный файл сервиса ocs-emm-journal-api (файл: </var/ocs/emm/ocs-emm-journal-api/ocs-emm-journal-api.yml>)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Описание параметров конфигурационного файла модуля ocs-emm-journal-api приведено в таблице (Таблица 51).

Таблица 51

Параметр	Описание	Добавлено	Удалено
transport.address	Адрес сервера и номер порта, на котором запускается приложение ("127.0.0.1:8080")	2.2.0	-
transport.nats.url	Адрес сервера Nats	2.2.0	-
transport.nats.clusterID	Идентификатор кластера Nats (https://docs.nats.io/)	2.2.0	-
transport.nats.clientID	Идентификатор клиента NATS. Если не указан, генерируется как appName + os.Getpid()	2.2.0	-
transport.nats.MaxInflight	Максимальное кол-во доставляемых клиенту (или подписчику) сообщений без подтверждений	2.2.1	-
database.dialect	Тип БД для ORM, используется "postgres"	2.2.0	-
database.agrs	Аргументы подключения к выбранной БД. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.0	-
logger	Логирование. Параметры берутся из п. 8.3.1	2.2.0	-

8.4. Описание конфигурационных файлов ПУСП

8.4.1. Общий конфигурационный файл ПУСП (файл: [/var/ocs/pkgrepo/config.yml](#))

Содержание конфигурационного файла.

```
config:
  publicUri:
    auth:
      publicUri: "http://dev-ocs.ompccloud.ru:8018"
  database:
    host: "ocsdevdb01.ompccloud"
    port: "5432"
    user: "pkgrepo"
    dbname: "pkgrepo"
    password: "fsadfsadf"
  redis:
    sentinelAddresses: "ocsdevapp01.ompccloud:26379"
    sentinelPassword: "fasfasf"
    masterName: "redis-ocs"
    password: "fasfasf"
  transport:
    http:
      address: ":8080"
      tls:
        enabled: false
      shutDownTime: "15s"
    nats:
      url: "nats://FF12fddgdhFLL@ocsdevapp01.ompccloud:4222"
      clusterID: "ocs"
  zipkin:
    address: ""
  logger:
    level: "debug"
    caller: true
```

```
gateway_gin_log_enabled: "true"
```

Описание параметров общего конфигурационного файла ПУСП приведено в таблице (Таблица 52).

Таблица 52

Параметр	Описание	Версия	Удалено
config.publicUri.auth.publicUri	Полный адрес публичного API сервера авторизации	2.2.0	-
config.redis.sentinelAddress	Адрес модуля sentinel СУБД Redis	2.2.0	-
config.redis.sentinelPassword	Пароль к модулю sentinel СУБД Redis	2.2.0	-
config.redis.masterName	Идентификатор (имя) БД Redis	2.2.0	-
config.redis.password	Пароль к СУБД Redis	2.2.0	-
config.database.host	Адрес (хост) базы данных ПУ	2.2.0	-
config.database.port	Порт базы данных ПУ	2.2.0	-
config.database.user	Имя пользователя базы данных ПУ	2.2.0	-
config.database.dbname	Имя базы данных ПУ	2.2.0	-
config.database.password	Пароль базы данных ПУ	2.2.0	-
config.transport.address	Порт, на котором запускается сервис (модуль) ПУ Пример: «:8080»	2.2.0	-
config.transport.tls.enabled	Доступность TLS протокола	2.2.0	-
config.transport.shutdownTime	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.2.0	-
config.transport.nats.url	Адрес сервера NATS	2.2.0	-
config.transport.nats.clusterID	Идентификатор кластера NATS	2.2.0	-
config.logger.level	Уровень детализации сообщений логирования. Возможные значения: - debug; - info; - warning; - error	2.2.0	-

Параметр	Описание	Версия	Удалено
config.logger.caller	Признак включения в лог дополнительных полей (имя файла, название функции) – false; – true	2.2.0	-
config.logger.gateway_gin_log_enabled	Флаг включения логирования входящего запроса на шлюзе (url запроса и http-статус ответа)	2.2.1	-

8.4.2. Конфигурационный файл сервиса pkgrepo (файл: /var/ocs/pkgrepo/ocs-pkgrepo-pkg-repo-api/ocs-pkgrepo-pkg-repo-api.yml)

Сервис сначала проверяет значение нужного параметра в своем собственном конфигурационном файле, и, если параметр отсутствует, то берет значение из общего конфигурационного файла. Если значение найдено в конфигурационном файле сервиса, то общий конфигурационный файл игнорируется.

Содержание конфигурационного файла:

```
config:
# section with common parameters
retrieveReleasesPeriod: 24h
transport:
  address: ":8088"
  debugAddress: ""
  shutDownTime: "15s"
nats:
  url: "nats://localhost:4222"
  clusterID: "test-cluster"
database:
  dialect: "postgres"
  args: "host=localhost port=5432 user=emm dbname=emm
password=ocs sslmode=disable search_path=os_update"
updateServers:
  - address: "https://releases.omprussia.ru"
logger:
  caller: true
```

Описание параметров конфигурационного файла rkgro приведено в таблице (Таблица 53).

Таблица 53

Параметр	Описание	Добавлено	Удалено
retrieveReleasesPeriod	Периодичность запроса новых релизов на OS Repo server Установлено 24 часа	2.2.1	-
transport.debugAddress	Адрес сервера и номер порта, на котором запускается приложение для отладки («127.0.0.1:8080»)	2.2.1	-
transport.address	Адрес сервера и номер порта, на котором запускается приложение («127.0.0.1:8080»)	2.2.1	-
transport.shutdownTime	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.2.1	-
transport.nats.url	Адрес сервера Nats	2.2.1	-
transport.nats.clusterID	Идентификатор кластера Nats	2.2.1	-
database.dialect	Тип базы данных для ORM, мы используем «postgres»	2.2.1	-
database.args	Аргументы подключения к выбранной базе данных. Значения для примера: "host=127.0.0.1 search_path=имя_схемы(account_devices) port=5432 user=dbUserName password=dbPassword dbname=dbName sslmode=disable timezone=utc"	2.2.1	-
updateServers.address	Адреса репозиторий с обновлением ЗМОС	2.2.1	-
logger	Логирование. Параметры берутся из общего конфигурационного файла	2.2.1	-

9. СООБЩЕНИЯ ОБ ОШИБКАХ

В ходе работы с компонентами ПБ пользователям могут выдаваться сообщения об ошибках, приведенные в таблице (Таблица 54).

Таблица 54

№	Текст ошибки в интерфейсе	Действия для устранения ошибки
1.	Данные были сохранены частично	Необходимо повторить позже или обратиться к администратору
2.	Данный пароль был использован ранее. Придумайте новый	Необходимо использовать пароль, который не использовался ранее
3.	Доступ запрещен	Не хватает прав для доступа. Необходимо обратиться к администратору или повторить позже
4.	Не удалось загрузить список ролей	Необходимо повторить позже или обратиться к администратору
5.	Не удалось сохранить данные	Необходимо повторить позже или обратиться к администратору
6.	Неверный логин или пароль	Ошибка аутентификации. Необходимо указать правильное сочетание логина и пароля
7.	Неверный текущий пароль	Необходимо указать корректный текущий пароль
8.	Ошибка. Аккаунт не найден	Попытка удаления аккаунта, которого нет в системе. Необходимо обновить страницу и убедиться, что удаляется корректный аккаунт

№	Текст ошибки в интерфейсе	Действия для устранения ошибки
9.	Превышено количество попыток входа. Повторите попытку позже или обратитесь к администратору	Необходимо повторить позже или обратиться к администратору учетных записей
10.	Такой email уже используется	Необходимо использовать другой email в качестве логина
11.	Учетная запись заблокирована. Обратитесь к администратору	Необходимо обратиться к администратору учетных записей
12.	Что-то пошло не так. Попробуйте позже	Необходимо повторить позже или обратиться к администратору

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 55).

Таблица 55

Термин/ Сокращение	Расшифровка
БД	База данных
Воркер	Потоки, принадлежащие браузеру, которые можно использовать для выполнения JS-кода без блокировки цикла события
ЗМОС	Защищенная мобильная операционная система общего назначения на базе Sailfish Mobile OS RUS, имеющая действительный сертификат соответствия ФСТЭК России, и/или операционная система Аврора, имеющая действительный сертификат соответствия ФСТЭК России
Механизм CORS	Механизм CORS (Cross-origin resource sharing) – технология современных браузеров, которая позволяет предоставить веб-странице доступ к ресурсам другого домена
МП	Мобильное приложение
МУ	Мобильное устройство
ОС	Операционная система
ОТК	Отдел технического контроля
ПБ	Подсистема безопасности
ПМ	Подсистема «Маркет»
ППО	Прикладное программное обеспечение «Аврора Центр»
Предприятие - изготовитель	Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»)
ПУ	Подсистема Платформа управления

Термин/ Сокращение	Расшифровка
ПУСП	Подсистема установки системных пакетов
ПЭВМ	Персональная электронно-вычислительная машина
СЗИ	Средство защиты информации
СЗИ НСД	Средств защиты информации от несанкционированного доступа
СПО	Специальное программное обеспечение
СУБД	Система управления базами данных
Субъекты доступа	<p>Лицо или процесс, действия которого регламентируются правилами разграничения доступа.</p> <p>Субъектами доступа являются пользователи и МП «Аврора Центр» (процесс МП «Аврора Центр») ППО. Субъекту доступа может быть назначена одна или несколько из следующих перечисленных ролей:</p> <ul style="list-style-type: none"> – роль МП «Аврора Центр» - роль назначается учетным записям МП «Аврора Центр» (сервис/процесс без участия пользователей, который управляет МУ); – роль Администратора учетных записей позволяет осуществлять управление учетными записями; – роль Оператора аудита позволяет осуществлять действия по работе с журналом регистрации событий ППО; – роль Администратора Платформы Управления позволяет осуществлять все действия по управлению ПУ через интерфейс ППО; – роль Администратора Аврора Маркет позволяет осуществлять все действия по управлению ПМ через интерфейс системы;

Термин/ Сокращение	Расшифровка
	<ul style="list-style-type: none"> – роль Разработчика позволяет осуществлять добавление новых и обновление ранее загруженных приложений в ПМ, а также получать информацию о приложениях; – роль Пользователя Аврора Маркет позволяет осуществлять загрузку приложений из ПМ, а также получать информацию о приложениях
Токен (маркер)	Токен - аутентификационные данные, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
API	Application Programming Interface – описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой
Cookie	Небольшой фрагмент данных, отправленный веб-сервером и хранимый на ПЭВМ пользователя. Веб-клиент (обычно веб-браузер) всякий раз при попытке открыть страницу соответствующего сайта пересылает этот фрагмент данных веб-серверу в составе HTTP-запроса
CPU	Центральный процессор
CSS3	Cascading Style Sheets 3 – спецификация CSS. Представляет собой формальный язык, реализованный с помощью языка разметки
ECMAScript 5	Встраиваемый расширяемый не имеющий средств ввода-вывода язык программирования, используемый в качестве основы для построения других скриптовых языков

Термин/ Сокращение	Расшифровка
FQDN	Fully Qualified Domain Name — «полностью определённое имя домена», иногда сокращается до «полное имя домена»
HEALTH- запрос	Запрос проверки доступности API
HTML5	HyperText Markup Language, version 5 – язык для структурирования и представления содержимого веб-страницы
HTTP	HyperText Transfer Protocol – протокол прикладного уровня передачи данных. Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом
HTTPS	Hypertext Transfer Protocol Secure - расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов SSL или TLS
IMEI	International Mobile Equipment Identity – уникальный номер мобильного устройства, состоящий из 15 цифр
JSON	JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript
MAC	Media Access Control – уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей
OIDC	OpenID Connect – уровень аутентификации OAuth 2.0, инфраструктуры авторизации. Контролируется OpenID Foundation

Термин/ Сокращение	Расшифровка
ORM	Object-Relational Mapping – технология программирования, которая связывает БД с концепциями объектно-ориентированных языков программирования, создавая «виртуальную объектную базу данных»
QR-код	Quick Response Code – код быстрого реагирования, предоставляющий информацию для быстрого ее распознавания с помощью камеры на мобильном устройстве
SSH	Secure SHell – сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов)
TLS	Transport Layer Security – криптографический протокол, обеспечивающий защищенную передачу данных между узлами в сети Интернет
URL	Uniform Resource Locator – единообразный локатор (определитель местонахождения) ресурса

