

ПРИКЛАДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «АВРОРА ЦЕНТР»

Руководство администратора. Часть 1

Подсистема безопасности

Версия документа 1.0

Листов 170

АННОТАЦИЯ

Настоящий документ является первой частью руководства администратора прикладного программного обеспечения «Аврора Центр» релиз 2.5.0 (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 обновления ОС».

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

СОДЕРЖАНИЕ

1. Общая информация	5
1.1. Назначение и состав ППО	5
1.2. Субъекты доступа и права на доступ к интерфейсам ППО	7
1.3. Назначение и состав ПБ	9
1.4. Описание принципов безопасной работы средства	10
1.5. Условия выполнения	13
2. Подготовка к работе	18
2.1. Начало сеанса работы	18
2.2. Описание интерфейса	21
3. Выполнение программы	27
3.1. Консоль администратора ПБ. Раздел «Администрирование»	27
3.2. Консоль администратора ПБ. Раздел «Мониторинг»	44
4. Описание установки ППО	50
4.1. Общая информация	50
4.2. Порядок действий по приемке ППО	51
4.3. Порядок установки компонентов среды функционирования	52
4.4. Порядок установки ППО	63
4.5. Адреса веб-консолей	66
4.6. Самостоятельная установка и настройка СУБД	67
4.7. Дополнительные настройки ППО и среды функционирования ППО	70
4.8. Проверка корректности установки и функционирования ППО	88
5. Резервное копирование	99
5.1. Резервное копирование после установки (обновления) ППО	99
5.2. Периодическое резервное копирование и резервное копирование перед установкой обновлений	99
6. Описание обновления ППО	102
7. Управление сервисами и настройками сервисов (подсистем) ППО	104
7.1. Управление сервисами ППО	104
7.2. Управление настройками сервисов и подсистем ППО	108

8. Описание удаления ППО	111
9. Конфигурационные файлы сценариев установки среды функционирования	113
9.1. Конфигурационные файлы сценариев установки среды функционирования	113
10. Конфигурационные файлы ППО (сценариев установки ППО)	118
10.1. Конфигурационные файлы ППО (общая информация)	118
10.2. Конфигурационные файлы сценариев установки ППО (общая информация) ...	119
10.3. Описание конфигурационных файлов ППО (сценариев установки ППО)	126
11. Сообщения об ошибках	163
Перечень терминов и сокращений	165

1. ОБЩАЯ ИНФОРМАЦИЯ

1.1. Назначение и состав ППО

ППО предназначено для управления мобильными устройствами (МУ), функционирующими под управлением операционной системы (ОС) Аврора, имеющей действительный сертификат соответствия ФСТЭК России, и управления жизненным циклом МП, 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 (ГИС), 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 обновления ОС (ПООС).

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 Pro¹ или PostgreSQL, в которой хранятся данные ППО, для чего при развертывании создается специальная БД. Для хранения информации о сессиях используется СУБД Redis.

¹ СУБД «Postgres Pro» (сертификат соответствия ФСТЭК России № 3637, действителен до 05 октября 2019 г., техническая поддержка до 05.10.2029 г.).

1.2. Субъекты доступа и права на доступ к интерфейсам ППО

1.2.1. Субъекты доступа (роли) ППО

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:

- МП «Аврора Центр» – роль назначается учетным записям МП «Аврора Центр» (сервис/процесс без участия пользователей, который управляет МУ);
- Администратор учетных записей – роль позволяет осуществлять управление учетными записями;
- Оператор аудита – роль позволяет осуществлять действия по работе с журналом регистрации событий ППО;
- Администратор Платформы Управления – роль позволяет осуществлять все действия по управлению ПУ через интерфейс ППО;
- Администратор Аврора Маркет – роль позволяет осуществлять все действия по управлению ПМ через интерфейс ППО;
- Разработчик – роль позволяет осуществлять добавление новых и обновление ранее загруженных приложений в ПМ, а также получать информацию о приложениях;
- Пользователь Аврора Маркет – роль 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 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
	Сценарии	ПУ	Консоль администратора ПУ Администратор Платформы Управления
	Приложения	ПМ	Консоль администратора ПМ Администратор Аврора Маркет
	Витрины	ПМ	Консоль администратора ПМ Администратор Аврора Маркет
	Связки ключей	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

Раздел	Подраздел	Подсистема	Наименование консоли / Права на доступ у роли
Консоль разработчика ПМ		ПМ	Консоль разработчика ПМ Разработчик
МП «Аврора Маркет»		ПМ	Пользователь Аврора Маркет
МП «Аврора Центр»		ПУ	Сервис/процесс МП «Аврора Центр»

В зависимости от варианта поставки ППО интерфейс верхней панели и состав доступных ролей могут отличаться. Подробное описание вариантов поставки ППО приведено в документе «Формуляр»

1.3. Назначение и состав ПБ

В ПБ реализованы функции безопасности ППО.

ПБ предназначена для:

- идентификации и аутентификацию пользователей и 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 ППО 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 верхнем правом углу каждого из подразделов интерфейса ППО в разделе «О платформе» меню текущего пользователя, нажав на значок  (Рисунок 1).

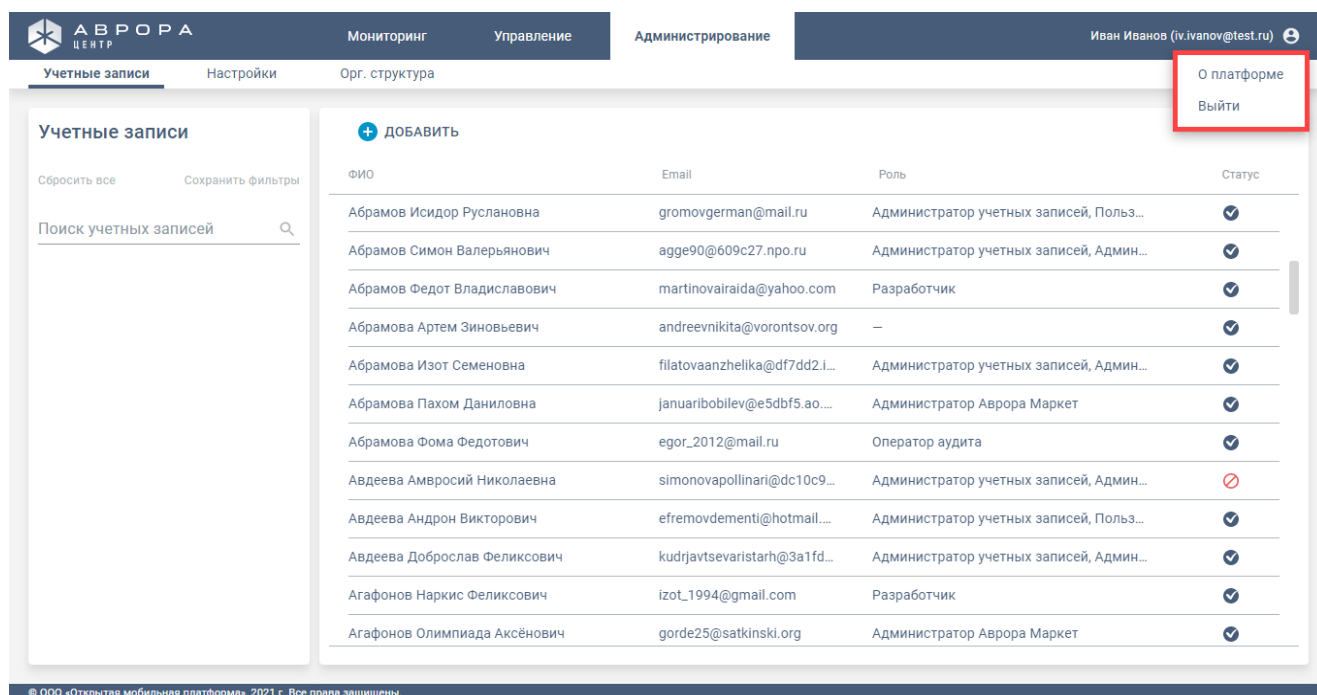


Рисунок 1

При нажатии на активную ссылку «Лицензионное соглашение» (Рисунок 2) отобразится текст «Лицензионного соглашения».

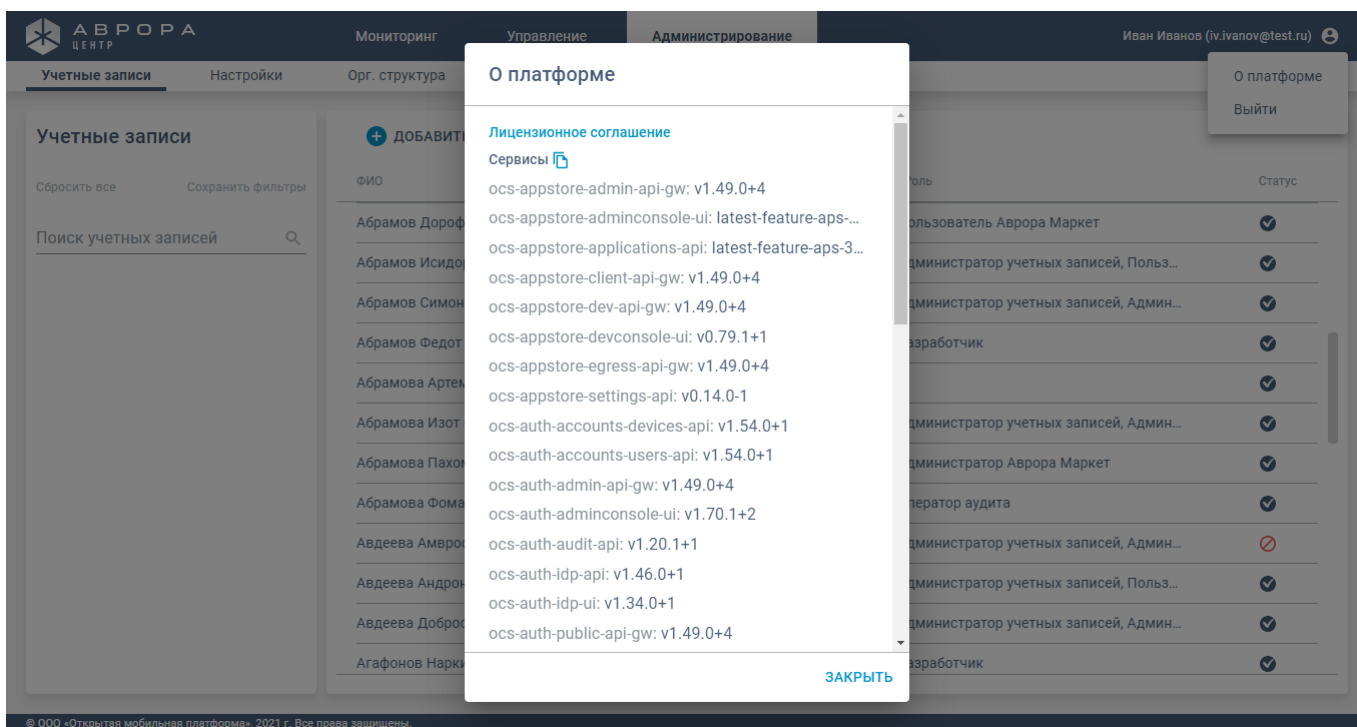


Рисунок 2

Любое использование пользователем ППО означает полное и безоговорочное принятие им 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 характеристики²	
Процессор	2 ядра
Объем оперативной памяти	не менее 4 Гб

² Для пилотных проектов, до 20 МУ.

Параметр	Значение
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; – CentOS версии 8 ³ или выше; – Альт 8 СП ⁴
Балансировщик микросервисов	Nginx Web Server версии 1.18 или выше
Система обнаружения сервисов	Consul версии 1.9 или выше
Средство управления конфигурациями микросервисов	Consul Template версии 0.25 или выше
Сервис гарантированной доставки сообщений	Nats Streaming Server версии 0.20.0 или выше
Прикладное программное обеспечение	ППО «Аврора Центр»

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

³ ППО под управлением ОС CentOS 8 не допускается использовать в информационных системах, обрабатывающих информацию ограниченного доступа, требующую защиты в соответствии с законодательством РФ.

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

Таблица 3

Параметр	Значение
Минимальные аппаратные характеристики⁵	
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; – CentOS версии 8 или выше; – Альт 8 СП
СУБД	Одна из следующих СУБД: – Postgres Pro (сертификат ФСТЭК России № 3637); – Postgres Pro 11; – PostgreSQL 11.11 или выше (для ОС CentOS); – PostgreSQL 12.6 или выше (для ОС CentOS)
СУБД для хранения сессий	Redis 6.0.10 или выше
Расширение СУБД PostgreSQL для партиционирования таблиц БД	pg_partman 4 или выше

⁵ Для пилотных проектов, до 20 МУ.

Параметр	Значение
Расширение СУБД PostgreSQL поддерживающее быстрый поиск схожих строк	pg_trgm

В таблице (Таблица 4) приведены программные характеристики МУ.

Таблица 4

Параметр	Значение
Операционная система	ОС Аврора, имеющая действительный сертификат соответствия ФСТЭК России
Прикладное программное обеспечение	– МП «Аврора Центр»; – МП «Аврора Маркет»

ВНИМАНИЕ! Для работы пользователей с веб-интерфейсом ППО должен использоваться веб-браузер Chrome версии 75 и выше, поддерживающий 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

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

ОС	СУБД	СЗИ НСД
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 11.11	СПО СЗИ НСД «Аккорд-Х К»
CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64	PostgreSQL 11.11	СЗИ НСД «Dallas Lock Linux»
CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64	PostgreSQL 11.11	СЗИ «Secret Net LSP»
Альт 8 СП	Postgres Pro	

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.).

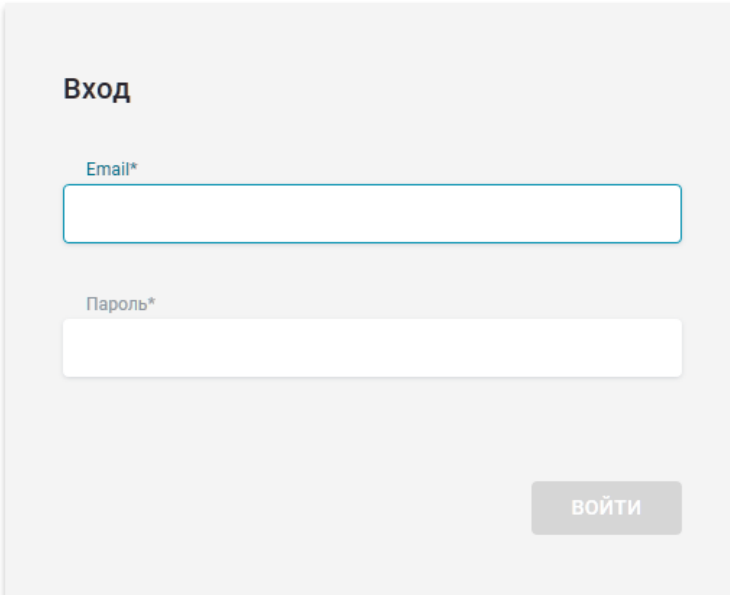
2. ПОДГОТОВКА К РАБОТЕ

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 3).

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**
- Field 1: **Email*** (with an empty text input box)
- Field 2: **Пароль*** (with an empty password input box)
- Button: **ВОЙТИ** (Login)

Рисунок 3

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 4).

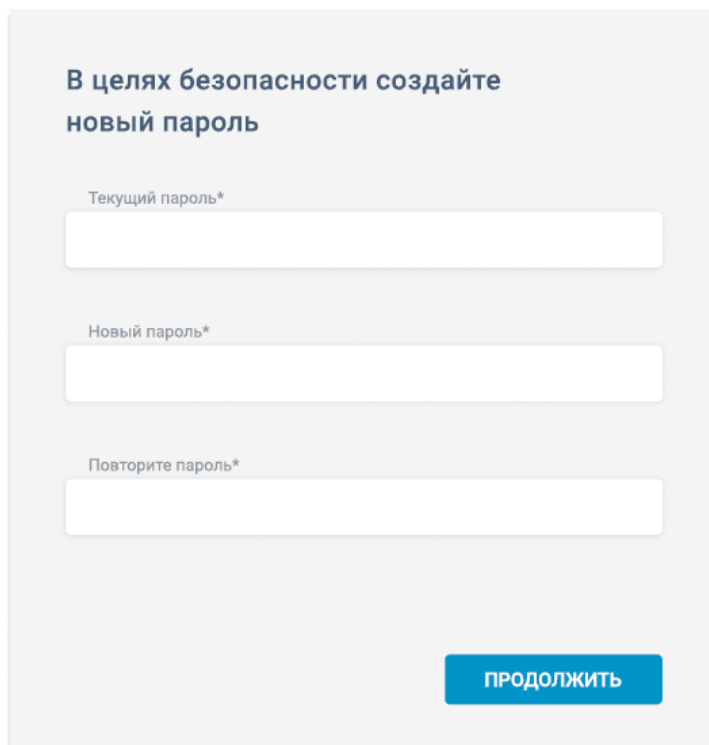


Рисунок 4

Новый пароль должен содержать:

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

Срок действия установленного пароля составляет 60 дней. По истечении срока действия необходимо сменить пароль. Откроется соответствующее окно (см. Рисунок 4). Смена устаревшего пароля выполняется аналогично смене пароля при первом входе.

Новый пароль должен отличаться от трех ранее вводимых паролей

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

При превышении допустимого количества сессий отобразится окно с информационным сообщением (Рисунок 5).

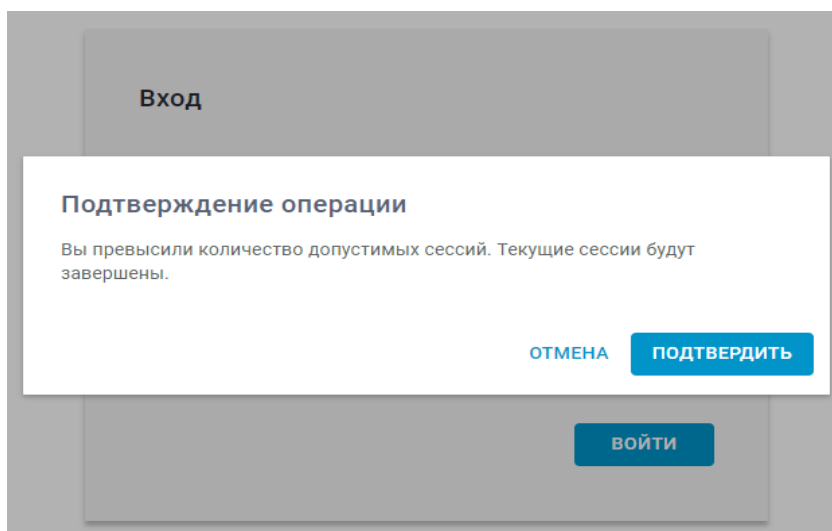


Рисунок 5

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 ПБ 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 3).

Если пользователь ПБ 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

С помощью верхней панели возможно выполнить следующие действия:

- осуществить навигацию между подсистемами ППО (Рисунок 6, Рисунок 7);
- перейти в раздел «О платформе» меню текущего пользователя, нажав на значок  (см. Рисунок 1);
- завершить сеанс работы, нажав на значок  и выбрать пункт «Выйти» (см. Рисунок 1). В результате откроется окно для входа в Консоль администратора ПБ (см. Рисунок 3).

Работа в Консоли администратора ПБ осуществляется в верхней панели в подразделе «Аудит» раздела «Мониторинг» (Рисунок 6), а также в подразделе «Учетные записи» раздела «Администрирование» (Рисунок 7).

В зависимости от варианта поставки ППО интерфейс верхней панели и состав доступных ролей могут отличаться. Подробное описание вариантов поставки ППО приведено в документе «Формуляр»

 АВРОПА
ЦЕНТР
Мониторинг
Управление
Администрирование
Иван Иванов (iv.ivanov@test.ru) 

Индикаторы
Аудит

Аудит



Сбросить все Сохранить фильтры

Поиск в аудите

Время	Субъект (источник)	Действие	Объект	Результат
10:31:20 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение	Информация о подключениях ...	Успех 200
10:31:20 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение	Фоновая задача Список	Успех 200
10:31:20 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение	Отчет о количестве и статусах ...	Успех 200
10:31:20 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение	Отчет об устройствах, соответ...	Успех 200
10:31:20 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение	Отчет об устройствах, соответ...	Успех 200
10:31:20 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение	Модель устройства Список	Успех 200
10:29:12 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение	Роль Список	Успех 200
10:29:11 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение	Учетная запись Список	Успех 200
10:28:56 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение релизов	Приложение 960fff90-112c-4aa2-ac15-d23...	Успех 200
10:28:52 05/03/21	iv.ivanov@test.ru a84d5cd8-3849-4596-8f2a-00...	Получение	Иконка 2641d1a1-5816-4176-ab20-87...	Успех 200

© ООО «Открытая мобильная платформа», 2021 г. Все права защищены.

Рисунок 6

 АВРОПА
ЦЕНТР
Мониторинг
Управление
Администрирование
Иван Иванов (iv.ivanov@test.ru) 

Учетные записи
Настройки
Орг. структура

Учетные записи

Сбросить все Сохранить фильтры


Поиск учетных записей

+ ДОБАВИТЬ

ФИО	Email	Роль	Статус
Абрамов Дороефий Филатович	kallistrat1979@ram...	Пользователь Аврора Маркет	✔
Абрамов Исидор Руслановна	gromovgerman@m...	Администратор учетных записей,...	✔
Абрамов Симон Валерьянович	agge90@609c27.n...	Администратор учетных записей,...	✔
Абрамов Федот Владиславович	martinovairaida@ya...	Разработчик	✔
Абрамова Артем Зиновьевич	andreevnikita@voro...	—	✔
Абрамова Изот Семеновна	filatovaanzhelika@...	Администратор учетных записей,...	✔
Абрамова Пахом Даниловна	januaribobilev@e5d...	Администратор Аврора Маркет	✔
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✔
Авдеева Амвросий Николаевна	simonovapollinari@...	Администратор учетных записей,...	✘
Авдеева Андрон Викторович	efremovdementi@h...	Администратор учетных записей,...	✔
Авдеева Доброслав Феликсович	kudrjvtsevaristarh...	Администратор учетных записей,...	✔

© ООО «Открытая мобильная платформа», 2021 г. Все права защищены.

Рисунок 7

Раздел «О платформе» (см. Рисунок 2) содержит ссылку на «Лицензионное соглашение» и подраздел «Сервисы» с возможностью просмотра версий сервисов ППО и копирования информации о сервисах в буфер обмена при нажатии на значок . Текст «Лицензионного соглашения» отобразится при нажатии на активную ссылку «Лицензионное соглашение».

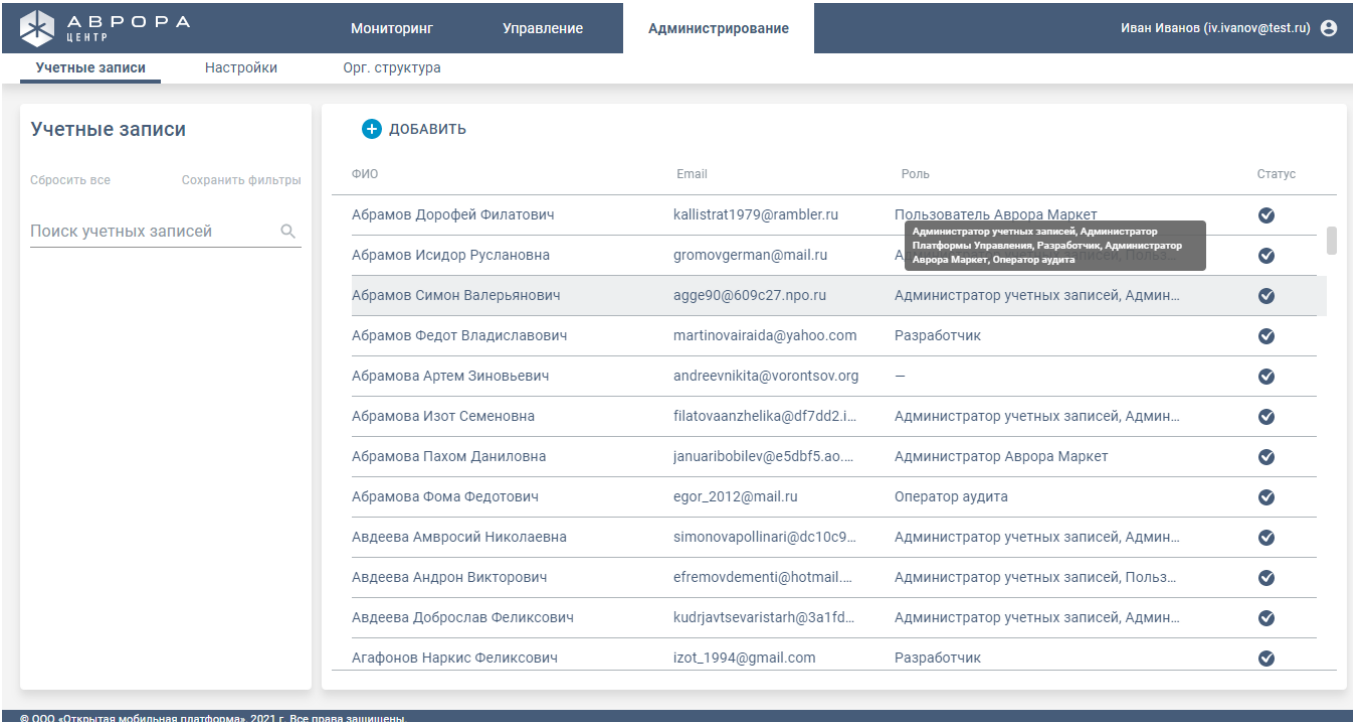
Для выхода из раздела необходимо нажать кнопку «Заккрыть».

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 8).



The screenshot shows the 'Учетные записи' (Accounts) section of the Aurora Center administration interface. The interface includes a top navigation bar with 'Мониторинг', 'Управление', and 'Администрирование' tabs, and a user profile 'Иван Иванов (iv.ivanov@test.ru)'. Below the navigation, there are tabs for 'Учетные записи', 'Настройки', and 'Орг. структура'. The main content area displays a table of user accounts with columns for 'ФИО', 'Email', 'Роль', and 'Статус'. A tooltip is visible over the role of the second user, listing their permissions: 'Администратор учетных записей, Администратор Платформы Управление, Разработчик, Администратор Аврора Маркет, Оператор аудита'.

ФИО	Email	Роль	Статус
Абрамов Дороефй Филатович	kallistrat1979@rambler.ru	Пользователь Аврора Маркет	✓
Абрамов Исидор Руслановна	gromovgerman@mail.ru	Администратор учетных записей, Администратор Платформы Управление, Разработчик, Администратор Аврора Маркет, Оператор аудита	✓
Абрамов Симон Валерьянович	agge90@609c27.npo.ru	Администратор учетных записей, Админ...	✓
Абрамов Федот Владиславович	martinovairaida@yahoo.com	Разработчик	✓
Абрамова Артем Зиновьевич	andreevnikita@vorontsov.org	–	✓
Абрамова Изот Семеновна	filatovaanzhelika@df7dd2.i...	Администратор учетных записей, Админ...	✓
Абрамова Пахом Даниловна	januaribobilev@e5dbf5.ao...	Администратор Аврора Маркет	✓
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✓
Авдеева Амвросий Николаевна	simonovapollinari@dc10c9...	Администратор учетных записей, Админ...	✓
Авдеева Андрон Викторович	efremovdementi@hotmail...	Администратор учетных записей, Польз...	✓
Авдеева Доброслав Феликсович	kudrjavgvaristarh@3a1fd...	Администратор учетных записей, Админ...	✓
Агафонов Наркис Феликсович	izot_1994@gmail.com	Разработчик	✓

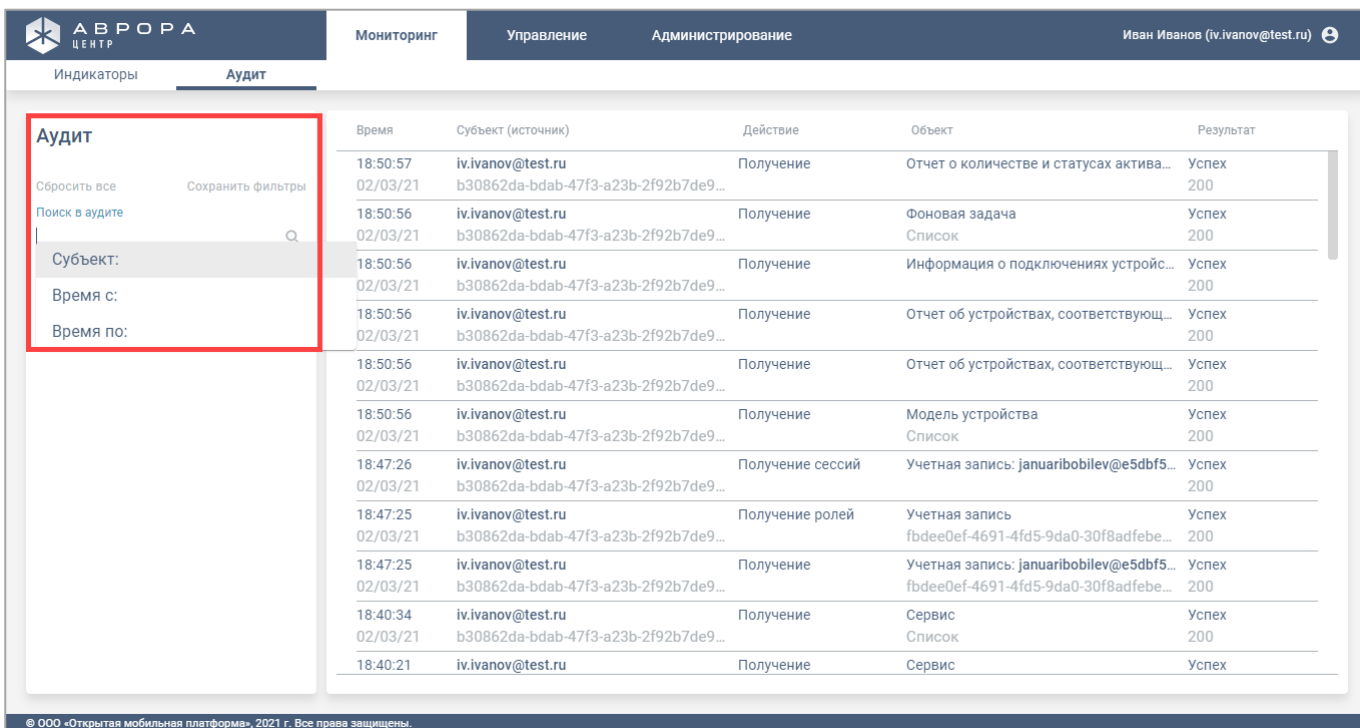
Рисунок 8

2.2.3. Область фильтров

С помощью области фильтров возможно выполнить поиск в следующих разделах:

– «Мониторинг», подраздел «Аудит». Поиск субъектов мониторинга (Рисунок 9);

– «Администрирование», подраздел «Учетные записи». Поиск по учетным записям пользователей (Рисунок 10).



Время	Субъект (источник)	Действие	Объект	Результат
18:50:57 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение	Отчет о количестве и статусах актива...	Успех 200
18:50:56 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение	Фоновая задача Список	Успех 200
18:50:56 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение	Информация о подключениях устройс...	Успех 200
18:50:56 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение	Отчет об устройствах, соответствующ...	Успех 200
18:50:56 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение	Отчет об устройствах, соответствующ...	Успех 200
18:50:56 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение	Модель устройства Список	Успех 200
18:47:26 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение сессий	Учетная запись: januaribobilev@e5dbf5...	Успех 200
18:47:25 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение ролей	Учетная запись fbdee0ef-4691-4fd5-9da0-30f8adfebe...	Успех 200
18:47:25 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение	Учетная запись: januaribobilev@e5dbf5...	Успех 200
18:40:34 02/03/21	iv.ivanov@test.ru b30862da-bdab-47f3-a23b-2f92b7de9...	Получение	Сервис Список	Успех 200
18:40:21	iv.ivanov@test.ru	Получение	Сервис	Успех

Рисунок 9

The screenshot displays the 'Учетные записи' (Accounts) management interface. On the left, a search filter panel is highlighted with a red border, containing the following fields: Имя (Name), Фамилия (Surname), Отчество (Patronymic), Email, Роль (Role), and Статус (Status). The main area shows a table of users with columns for ФИО (Full Name), Email, Роль (Role), and Статус (Status). The table lists 15 users, including 'Абрамов Доротея Филатович' and 'Абрамов Исаидор Руслановна'. A '+ ДОБАВИТЬ' (Add) button is located at the top left of the table area.

Рисунок 10

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

Раздел	Фильтр	Описание
	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»

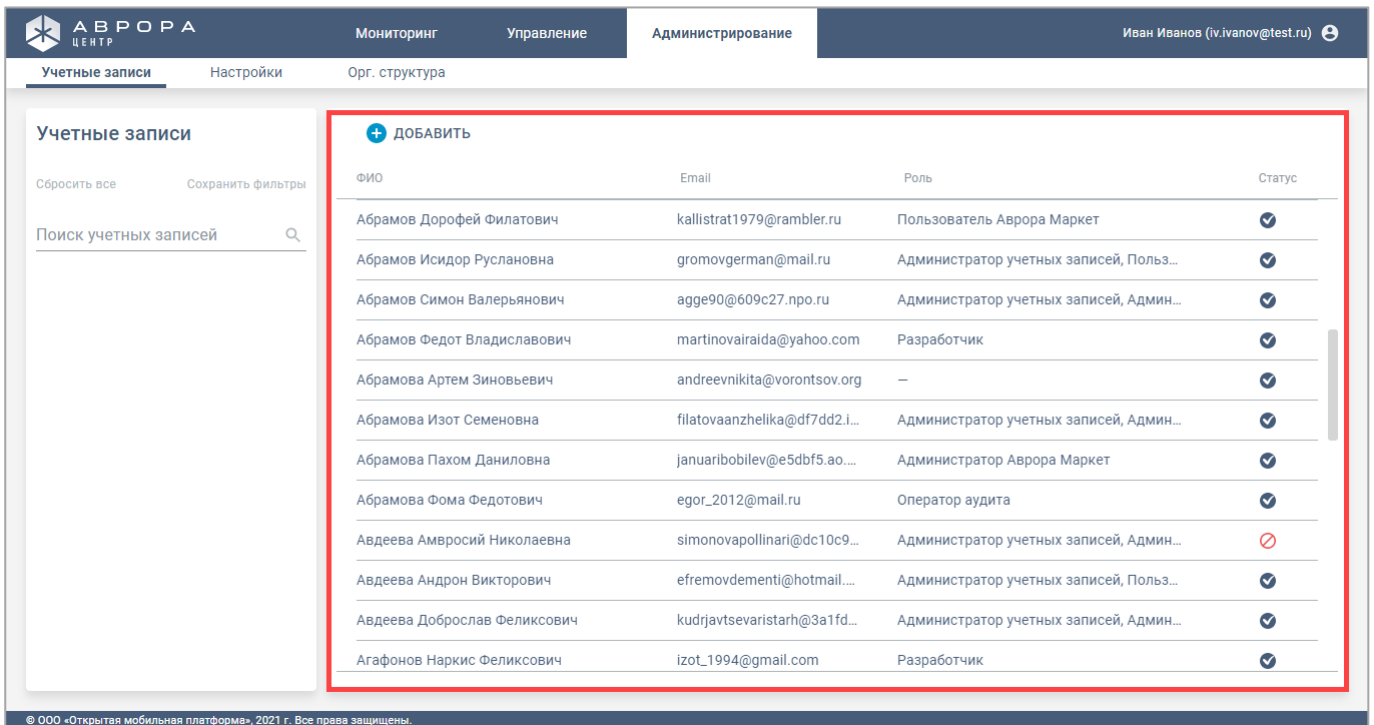
3. ВЫПОЛНЕНИЕ ПРОГРАММЫ

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 11):

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





ФИО	Email	Роль	Статус
Абрамов Дорочей Филатович	kallistrat1979@rambler.ru	Пользователь Аврора Маркет	✓
Абрамов Исидор Руслановна	gromovgerman@mail.ru	Администратор учетных записей, Польз...	✓
Абрамов Симон Валерьянович	agge90@609c27.npo.ru	Администратор учетных записей, Админ...	✓
Абрамов Федот Владиславович	martinovairaida@yahoo.com	Разработчик	✓
Абрамова Артем Зиновьевич	andreevnikita@vorontsov.org	–	✓
Абрамова Изот Семеновна	filatovaanzhelika@df7dd2.i...	Администратор учетных записей, Админ...	✓
Абрамова Пахом Даниловна	januaribobilev@e5dbf5.ao...	Администратор Аврора Маркет	✓
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✓
Авдеева Амвросий Николаевна	simonovapollinari@dc10c9...	Администратор учетных записей, Админ...	✗
Авдеева Андрон Викторович	efremovdementi@hotmail...	Администратор учетных записей, Польз...	✓
Авдеева Доброслав Феликсович	kudrjajtsevaristarh@3a1fd...	Администратор учетных записей, Админ...	✓
Агафонов Наркис Феликсович	izot_1994@gmail.com	Разработчик	✓

Рисунок 11

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;
- Функциональный администратор СУА⁹.

При нажатии на строку учетной записи пользователя ППО откроется карточка, в которой отображается количество активных сессий пользователя и основная информация (Рисунок 12).

⁹ Роль используется в продукте «Сервис уведомлений Аврора», в ППО «Аврора Центр» данная роль не используется.

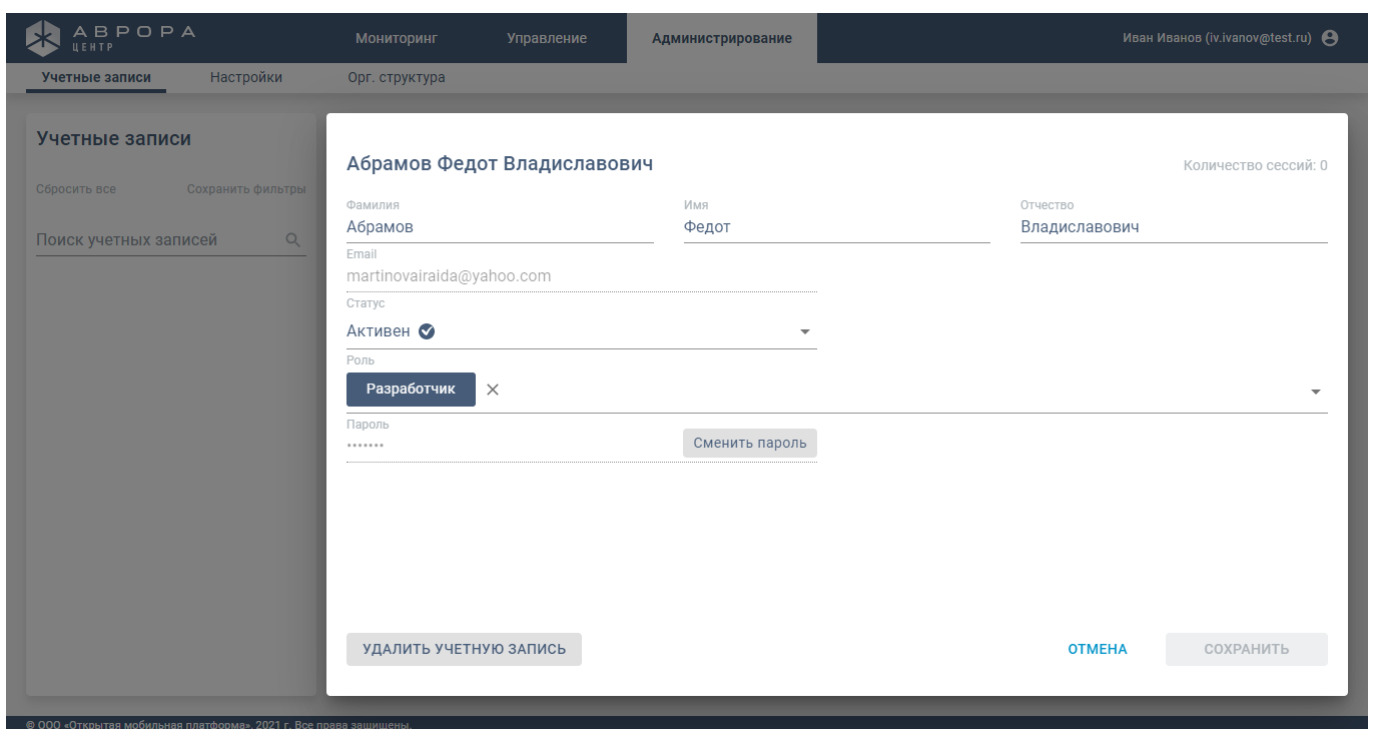


Рисунок 12

С помощью карточки учетной записи можно выполнить следующие действия:

- 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 13).

ФИО	Email	Роль	Статус
Абрамов Дороеф Филатович	kallistrat1979@rambler.ru	Пользователь Аврора Маркет	✓
Абрамов Исидор Руслановна	gromovgerman@mail.ru	Администратор учетных записей, Польз...	✓
Абрамов Симон Валерьянович	agge90@609c27.npo.ru	Администратор учетных записей, Админ...	✓
Абрамов Федот Владиславович	martinovairaida@yahoo.com	Разработчик	✓
Абрамова Артем Зиновьевич	andreevnikita@vorontsov.org	–	✓
Абрамова Изот Семеновна	filatovaanzhelika@df7dd2.i...	Администратор учетных записей, Админ...	✓
Абрамова Пахом Даниловна	januaribobilev@e5dbf5.ao...	Администратор Аврора Маркет	✓
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✓
Авдеева Амвросий Николаевна	simonovapollinari@dc10c9...	Администратор учетных записей, Админ...	✗
Авдеева Андрон Викторович	efremovdementi@hotmail...	Администратор учетных записей, Польз...	✓
Авдеева Доброслав Феликсович	kudrjvtsevaristarh@3a1fd...	Администратор учетных записей, Админ...	✓
Агафонов Наркис Феликсович	izot_1994@gmail.com	Разработчик	✓

Рисунок 13

В открывшейся форме необходимо заполнить следующие поля (Рисунок 14):

- «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

The screenshot shows the 'Новая учетная запись' (New Account) form in the Avrora Center administration interface. The form is titled 'Новая учетная запись' and is located in the 'Учетные записи' (Accounts) section. The form fields are:

- Фамилия (Surname): Empty
- Имя (Name): Empty
- Отчество (Patronymic): Empty
- Email: Empty
- Статус (Status): 'Активен' (Active) with a checkmark icon
- Роль (Role): Empty
- Пароль (Password): Empty
- Повторите пароль (Repeat Password): Empty

At the bottom right of the form, there are two buttons: 'ОТМЕНА' (Cancel) and 'СОЗДАТЬ' (Create).

Рисунок 14

Для создания учетной записи необходимо нажать кнопку «Создать». Для отмены создания учетной записи необходимо нажать кнопку «Отмена» (Рисунок 15).

The screenshot shows the 'Новая учетная запись' (New Account) form in the Avrora Center administration interface, with the following fields filled in:

- Фамилия (Surname): **Абрамов**
- Имя (Name): **Иван**
- Отчество (Patronymic): **Иванович**
- Email: **abramov.i@test.ru**
- Статус (Status): 'Активен' (Active) with a checkmark icon
- Роль (Role): **Пользователь Аврора Маркет** (User Avrora Market) with a close icon (X)
- Пароль (Password): *********
- Повторите пароль (Repeat Password): *********

At the bottom right of the form, there are two buttons: 'ОТМЕНА' (Cancel) and 'СОЗДАТЬ' (Create).

Рисунок 15

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 16).

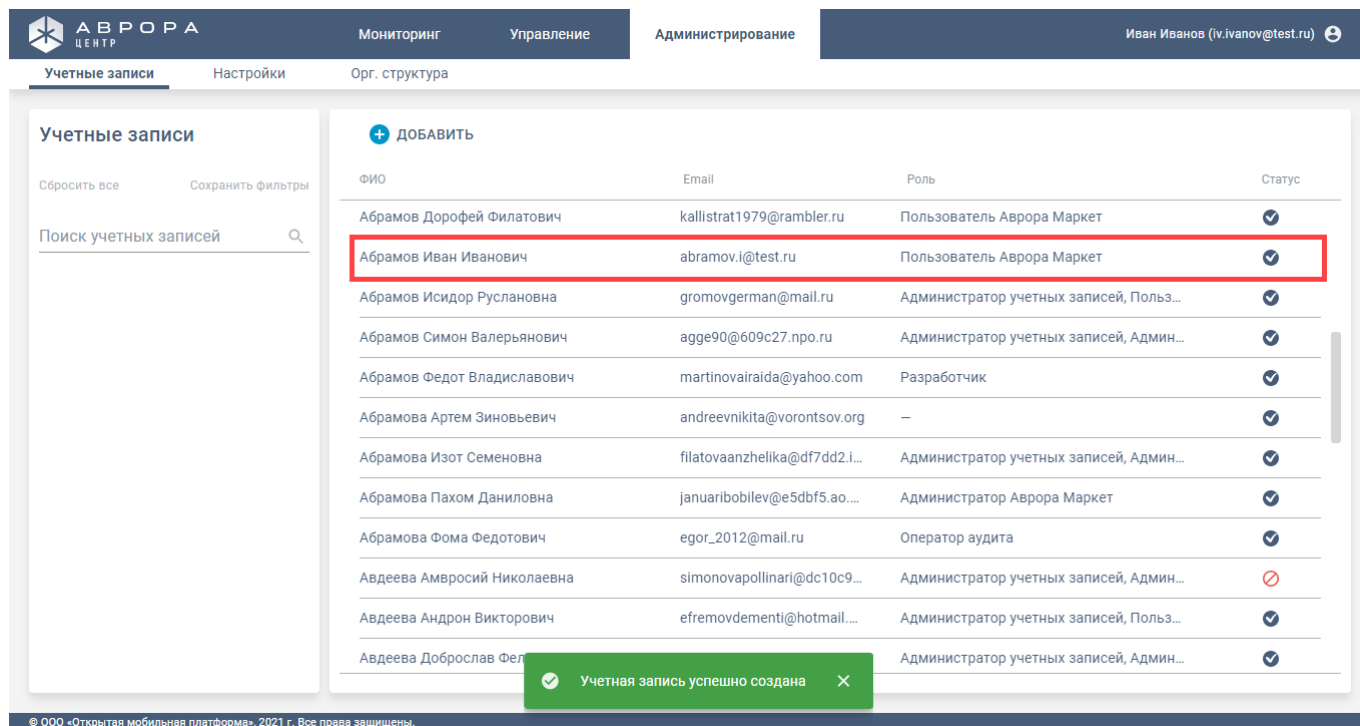


Рисунок 16

3.1.1.2. Редактирование данных учетной записи

Для редактирования данных учетной записи необходимо выполнить следующие действия:

- нажать на строку учетной записи (Рисунок 17);

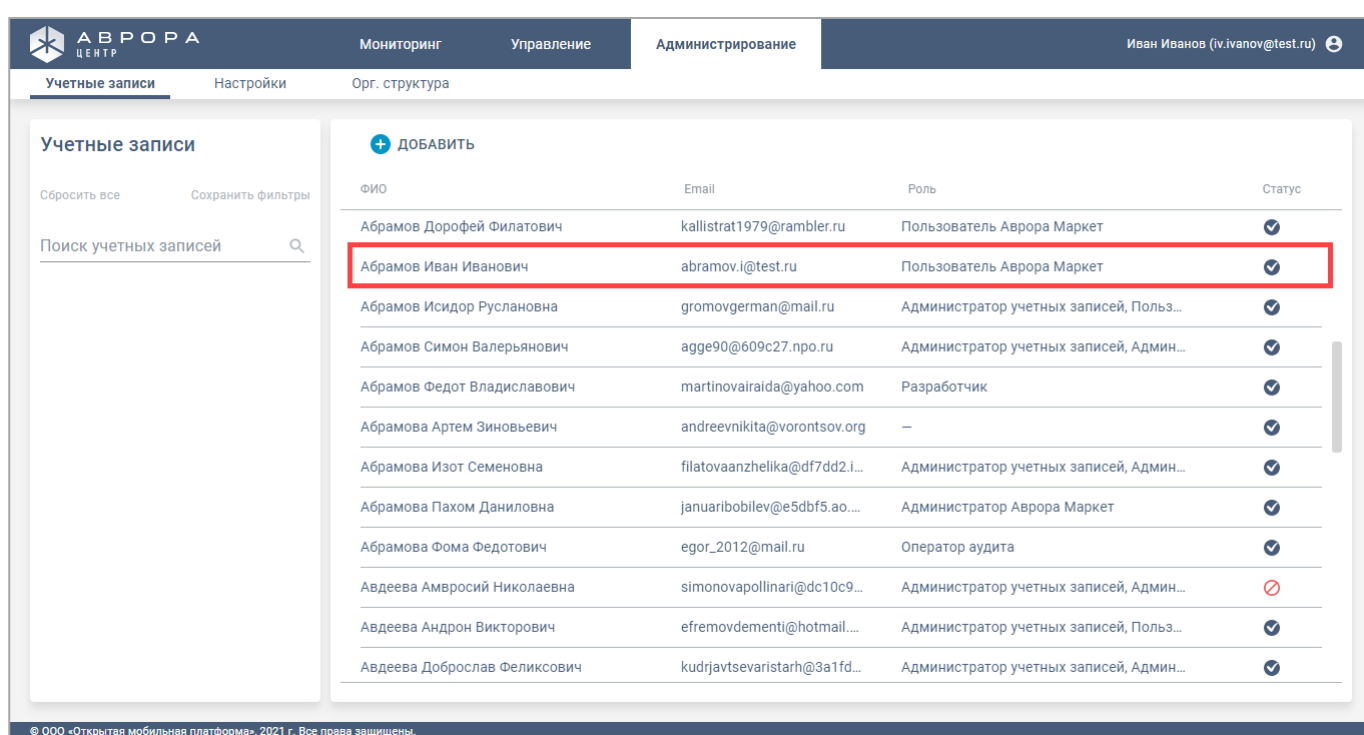


Рисунок 17

- в открывшейся форме внести необходимые изменения;
- нажать кнопку «Сохранить». Для отмены редактирования нажать кнопку «Отмена» (Рисунок 18);

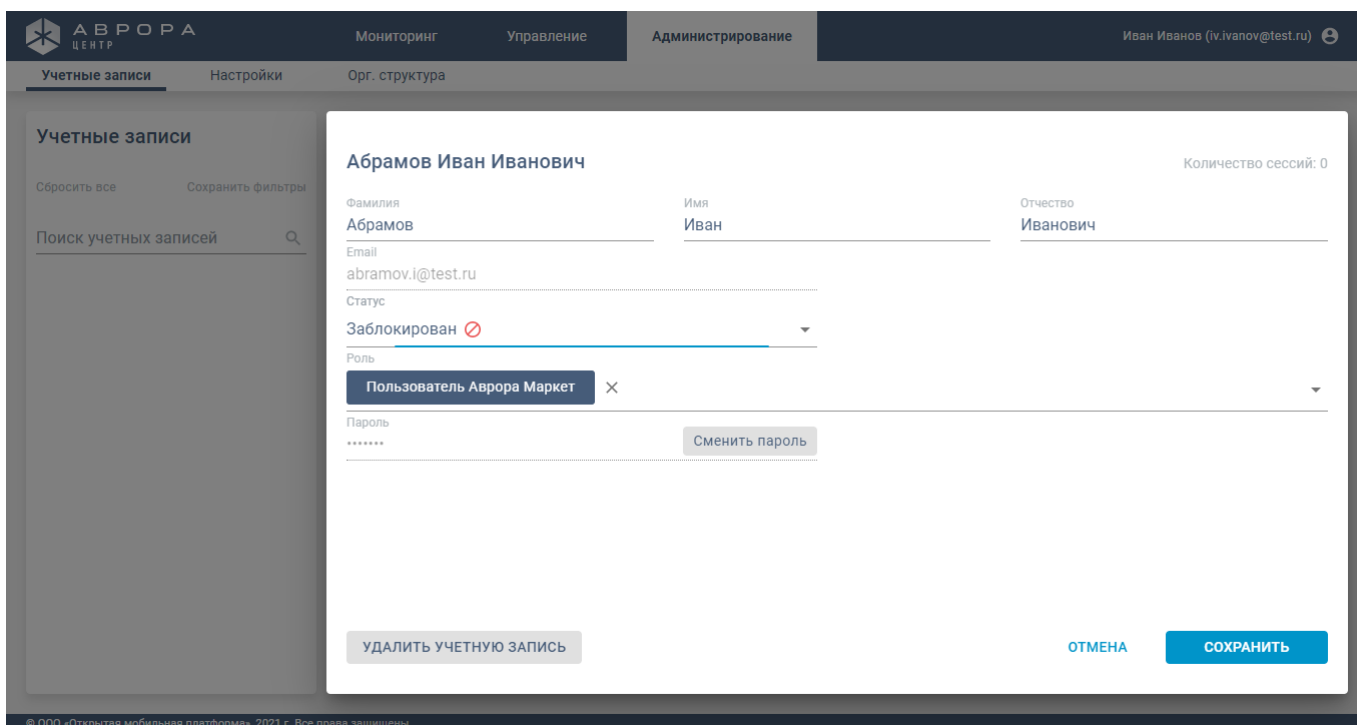


Рисунок 18

Поле «Email» недоступно для изменения

При успешном редактировании данных учетной записи отобразится сообщение «Учетная запись успешно обновлена» (Рисунок 19).

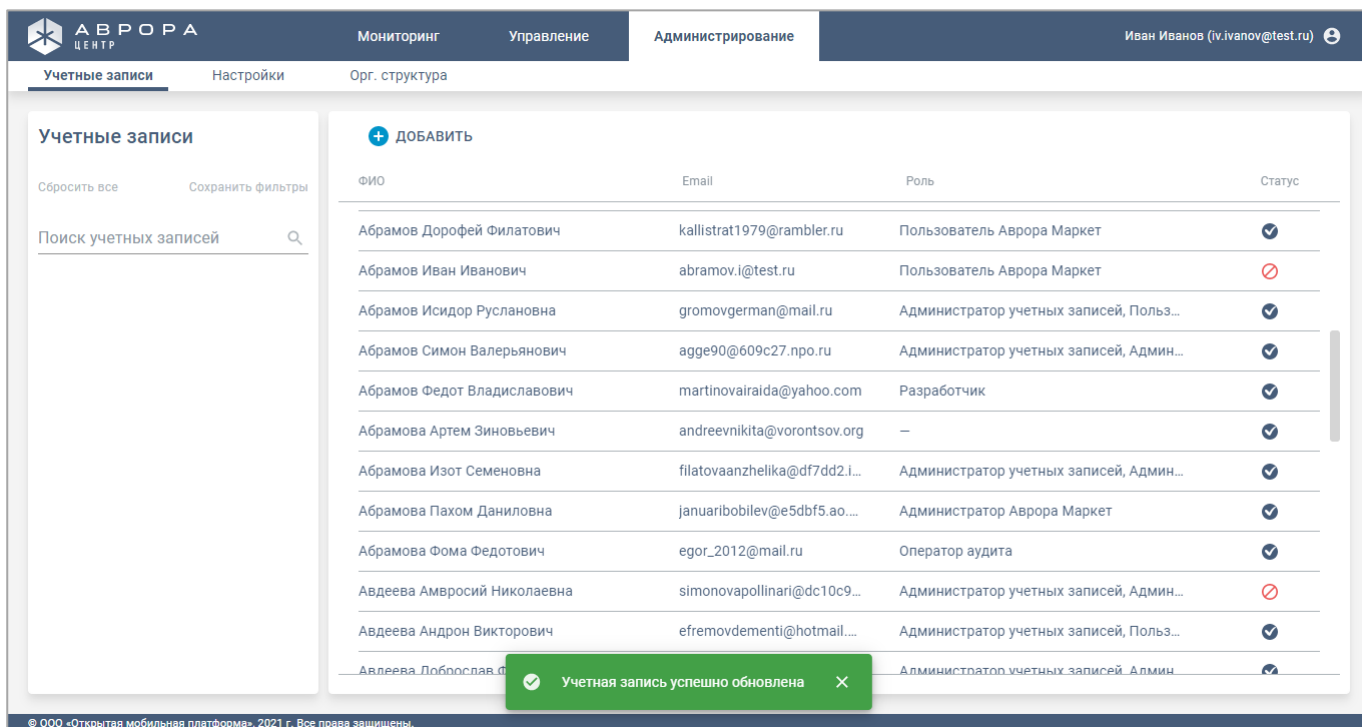




Рисунок 19

3.1.1.3. Работа с фильтрами

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

Фильтры для поиска информации приведены в сводной таблице (см. Таблица 6).

Для поиска по заданным критериям необходимо выполнить следующие действия (Рисунок 20):

- 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

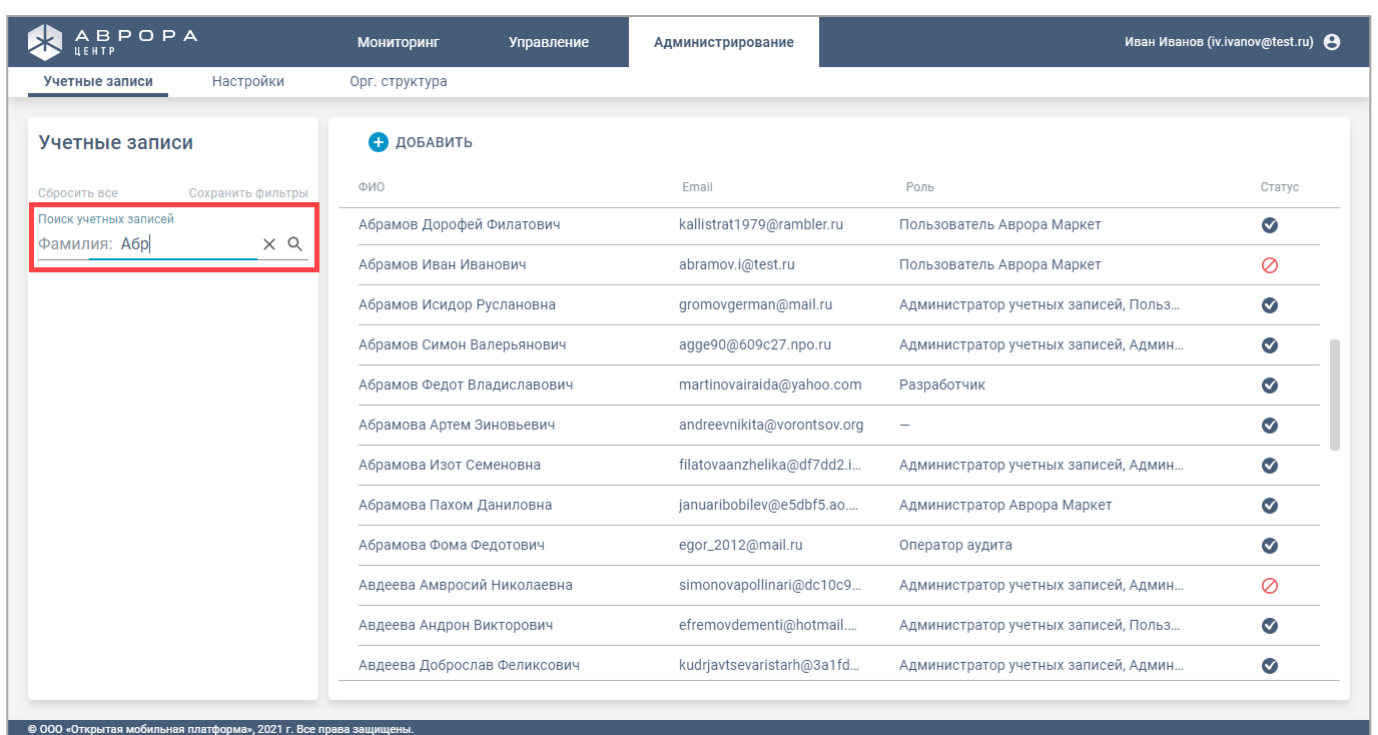


Рисунок 20

В результате выполнится поиск по выбранному фильтру (Рисунок 21).

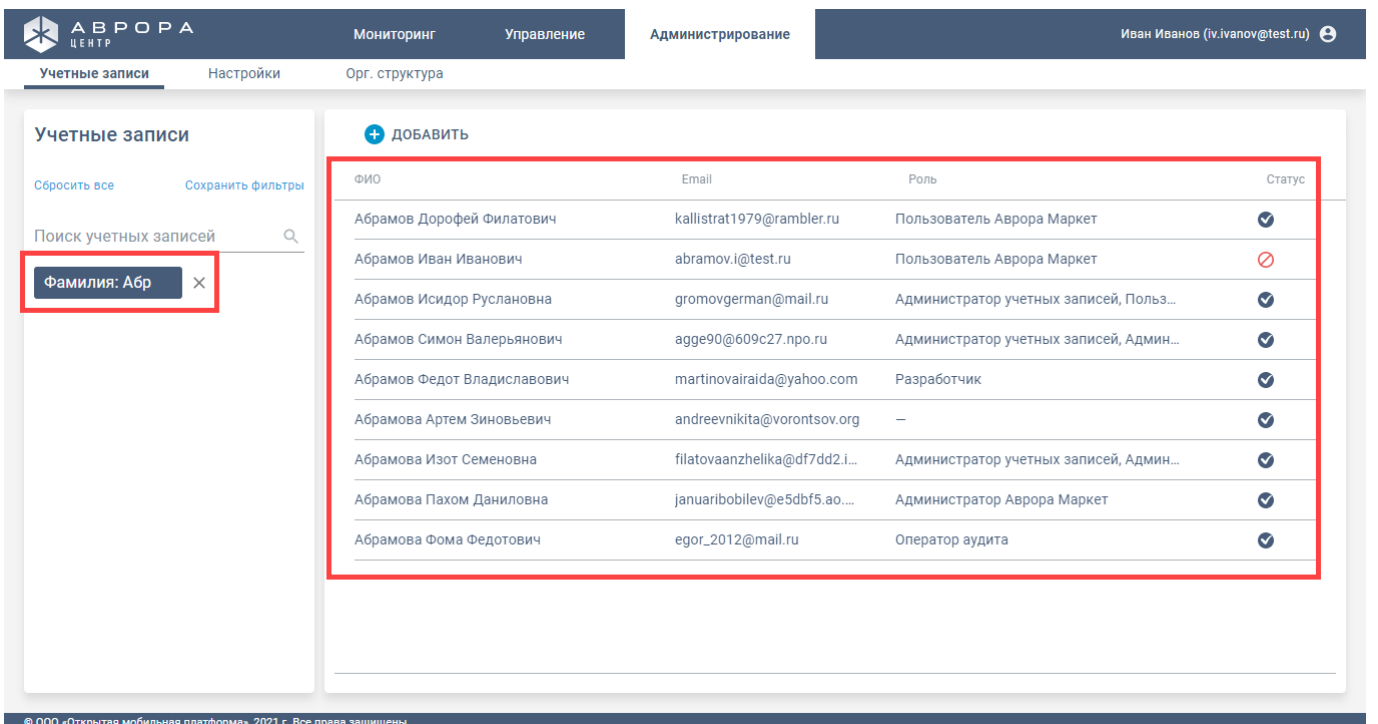
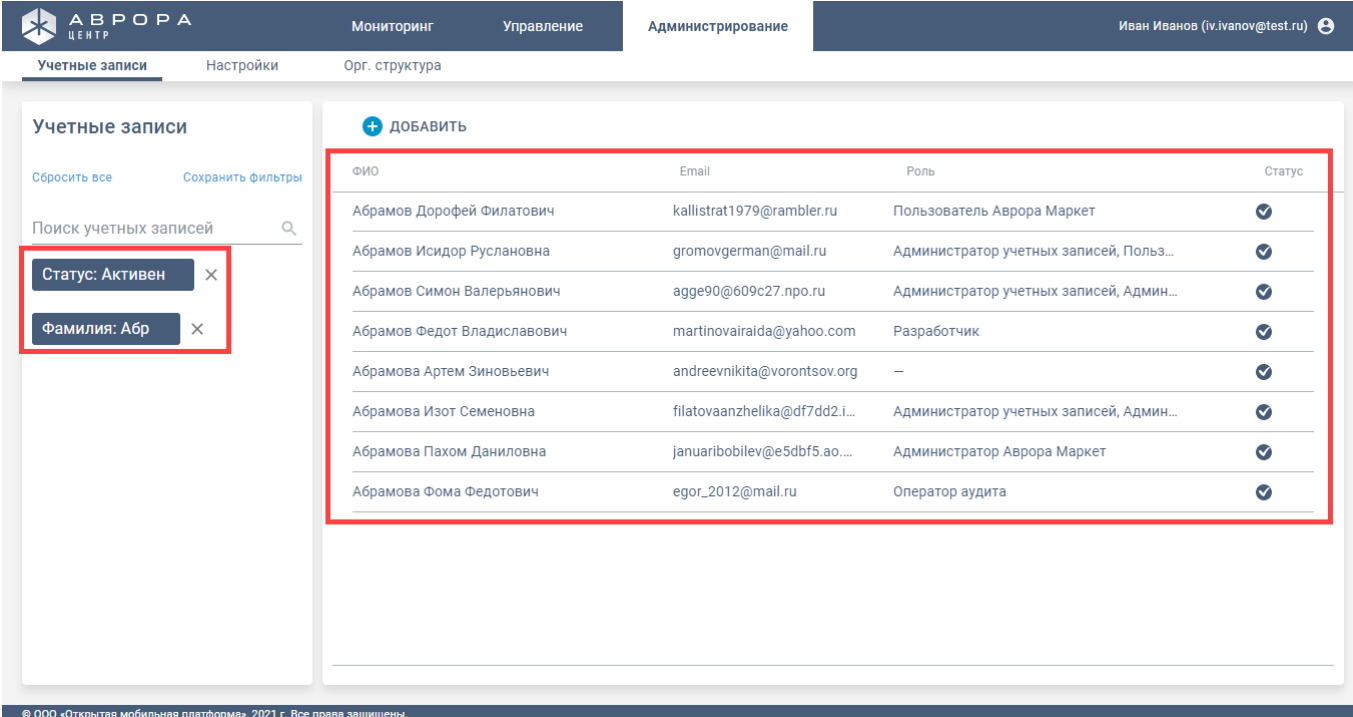


Рисунок 21

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 22).



Учетные записи

Сбросить все Сохранить фильтры

Поиск учетных записей

Статус: Активен ×

Фамилия: Абр ×

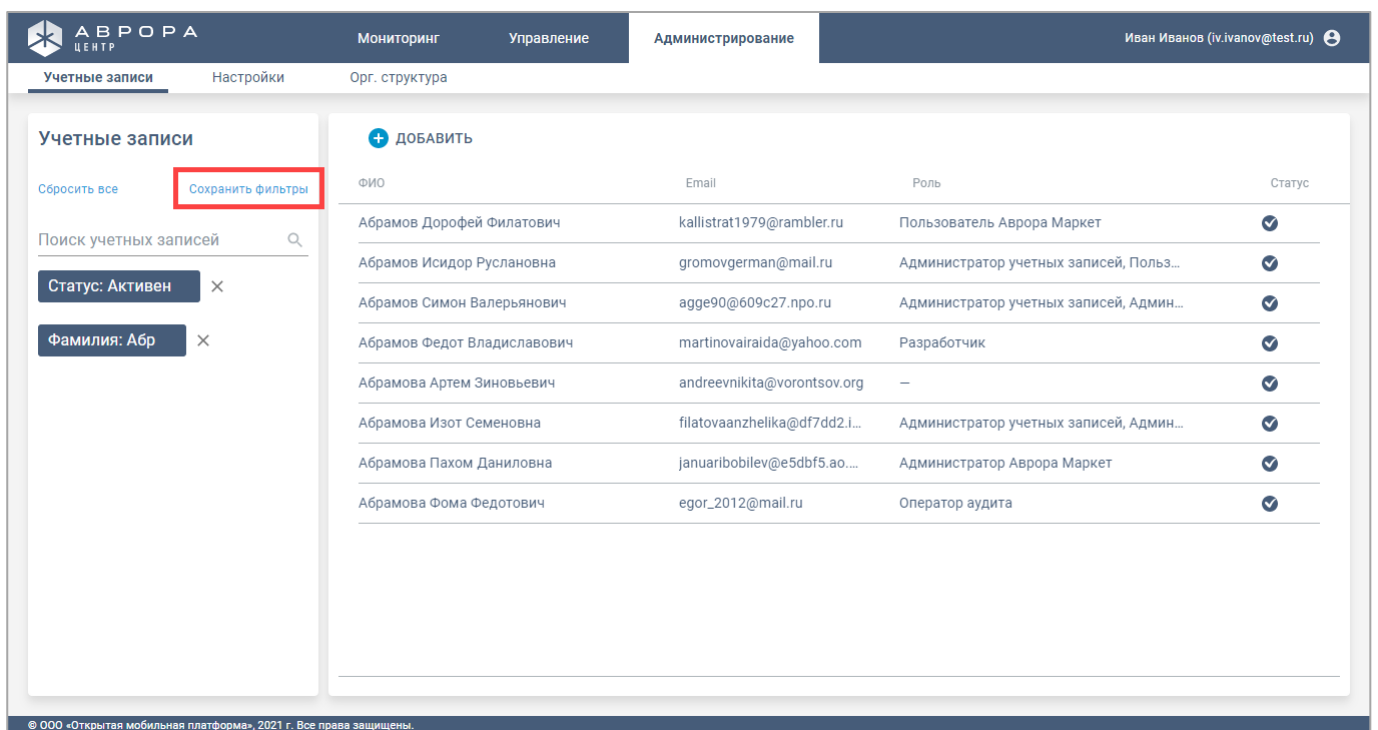
ФИО	Email	Роль	Статус
Абрамов Дорочей Филатович	kallistrat1979@rambler.ru	Пользователь Аврора Маркет	✓
Абрамов Исидор Руслановна	gromovgerman@mail.ru	Администратор учетных записей, Польз...	✓
Абрамов Симон Валерьянович	agge90@609c27.npo.ru	Администратор учетных записей, Админ...	✓
Абрамов Федот Владиславович	martinovairaida@yahoo.com	Разработчик	✓
Абрамова Артем Зиновьевич	andreevnikita@vorontsov.org	—	✓
Абрамова Изот Семеновна	filatovaanzhelika@df7dd2.i...	Администратор учетных записей, Админ...	✓
Абрамова Пахом Даниловна	januaribobilev@e5dbf5.ao....	Администратор Аврора Маркет	✓
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✓

© ООО «Открытая мобильная платформа», 2021 г. Все права защищены.

Рисунок 22

Примененные фильтры можно сохранить в набор, выполнив следующие действия:

- нажать «Сохранить фильтры» (Рисунок 23);



Учетные записи

Сбросить все **Сохранить фильтры**

Поиск учетных записей

Статус: Активен ×

Фамилия: Абр ×

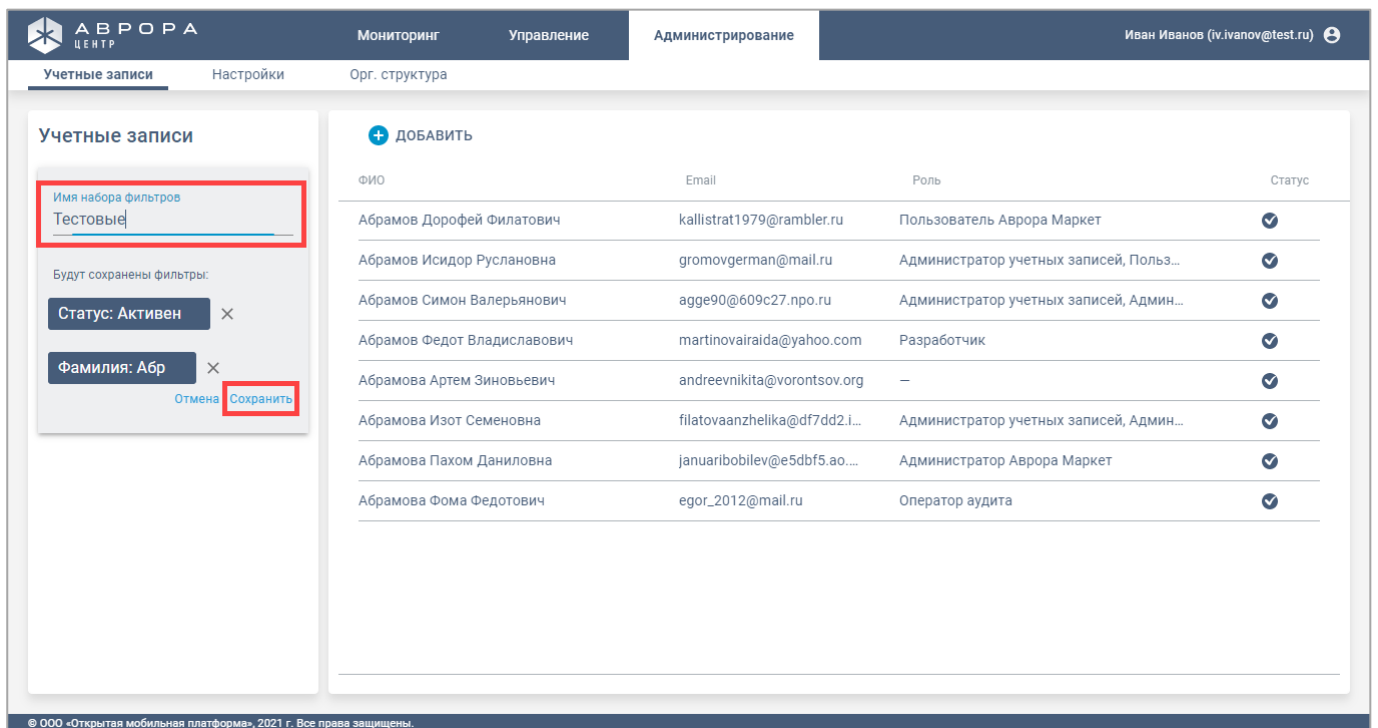
+ ДОБАВИТЬ

ФИО	Email	Роль	Статус
Абрамов Дорочей Филатович	kallistrat1979@rambler.ru	Пользователь Аврора Маркет	✓
Абрамов Исидор Руслановна	gromovgerman@mail.ru	Администратор учетных записей, Польз...	✓
Абрамов Симон Валерьянович	agge90@609c27.npo.ru	Администратор учетных записей, Админ...	✓
Абрамов Федот Владиславович	martinovairaida@yahoo.com	Разработчик	✓
Абрамова Артем Зиновьевич	andreevnikita@vorontsov.org	—	✓
Абрамова Изот Семеновна	filatovaanzhelika@df7dd2.i...	Администратор учетных записей, Админ...	✓
Абрамова Пахом Даниловна	januaribobilev@e5dbf5.ao...	Администратор Аврора Маркет	✓
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✓

© ООО «Открытая мобильная платформа», 2021 г. Все права защищены.

Рисунок 23

- ввести имя набора фильтров;
- нажать «Сохранить» (Рисунок 24).



Учетные записи

Имя набора фильтров
Тестовые

Будут сохранены фильтры:

Статус: Активен ×

Фамилия: Абр ×



Отмена **Сохранить**

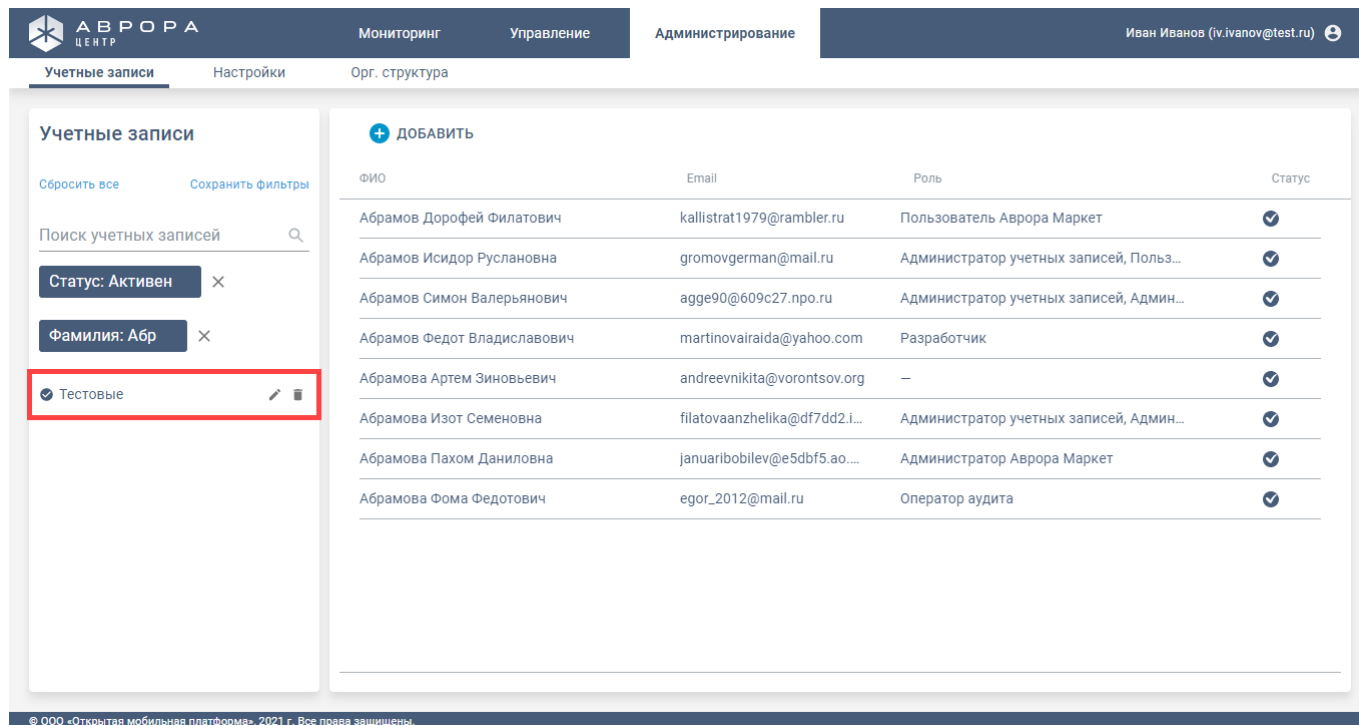
+ ДОБАВИТЬ

ФИО	Email	Роль	Статус
Абрамов Дорочей Филатович	kallistrat1979@rambler.ru	Пользователь Аврора Маркет	✓
Абрамов Исидор Руслановна	gromovgerman@mail.ru	Администратор учетных записей, Польз...	✓
Абрамов Симон Валерьянович	agge90@609c27.npo.ru	Администратор учетных записей, Админ...	✓
Абрамов Федот Владиславович	martinovairaida@yahoo.com	Разработчик	✓
Абрамова Артем Зиновьевич	andreevnikita@vorontsov.org	—	✓
Абрамова Изот Семеновна	filatovaanzhelika@df7dd2.i...	Администратор учетных записей, Админ...	✓
Абрамова Пахом Даниловна	januaribobilev@e5dbf5.ao...	Администратор Аврора Маркет	✓
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✓

© ООО «Открытая мобильная платформа», 2021 г. Все права защищены.

Рисунок 24

В результате выбранная комбинация фильтров сохранится в набор. При необходимости набор можно редактировать, нажав на значок , или удалить, нажав на значок  (Рисунок 25).





Учетные записи

Сбросить все Сохранить фильтры

Поиск учетных записей

Статус: Активен ×

Фамилия: Абр ×

Тестовые  

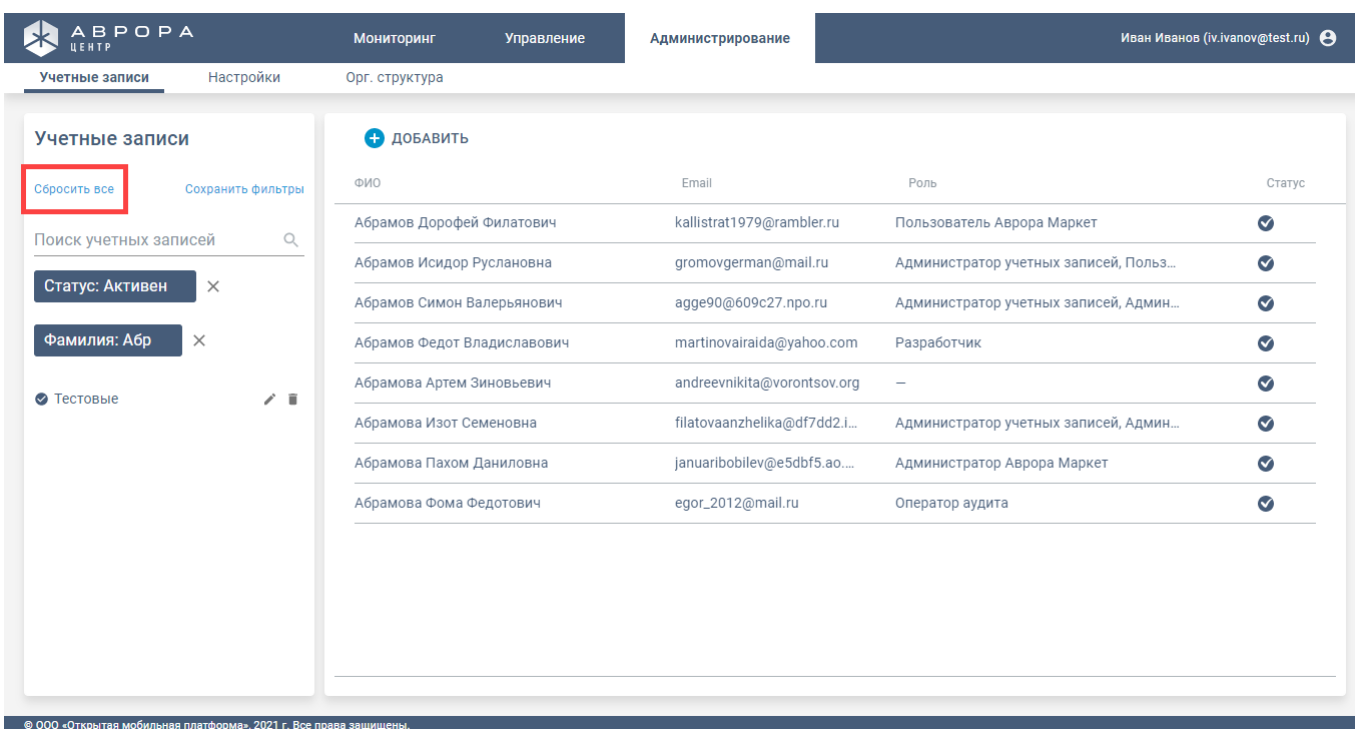
ФИО	Email	Роль	Статус
Абрамов Дорюфей Филатович	kallistrat1979@rambler.ru	Пользователь Аврора Маркет	✓
Абрамов Исидор Руслановна	gromovgerman@mail.ru	Администратор учетных записей, Польз...	✓
Абрамов Симон Валерьянович	agge90@609c27.npo.ru	Администратор учетных записей, Админ...	✓
Абрамов Федот Владиславович	martinovairaida@yahoo.com	Разработчик	✓
Абрамова Артем Зиновьевич	andreevnikita@vorontsov.org	—	✓
Абрамова Изот Семеновна	filatovaanzhelika@df7dd2.i...	Администратор учетных записей, Админ...	✓
Абрамова Пахом Даниловна	januaribobilev@e5dbf5.ao...	Администратор Аврора Маркет	✓
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✓

© ООО «Открытая мобильная платформа», 2021 г. Все права защищены.

Рисунок 25

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

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



Учетные записи

Сбросить все Сохранить фильтры

Поиск учетных записей

Статус: Активен

Фамилия: Абр

Тестовые

+ ДОБАВИТЬ

ФИО	Email	Роль	Статус
Абрамов Дорофей Филатович	kallistrat1979@rambler.ru	Пользователь Аврора Маркет	✓
Абрамов Исидор Руслановна	gromovgerman@mail.ru	Администратор учетных записей, Польз...	✓
Абрамов Симон Валерьянович	agge90@609c27.npo.ru	Администратор учетных записей, Админ...	✓
Абрамов Федот Владиславович	martinovairaida@yahoo.com	Разработчик	✓
Абрамова Артем Зиновьевич	andreevnikita@vorontsov.org	–	✓
Абрамова Изот Семеновна	filatovaanzhelika@df7dd2.i...	Администратор учетных записей, Админ...	✓
Абрамова Пахом Даниловна	januaribobilev@e5dbf5.ao...	Администратор Аврора Маркет	✓
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✓

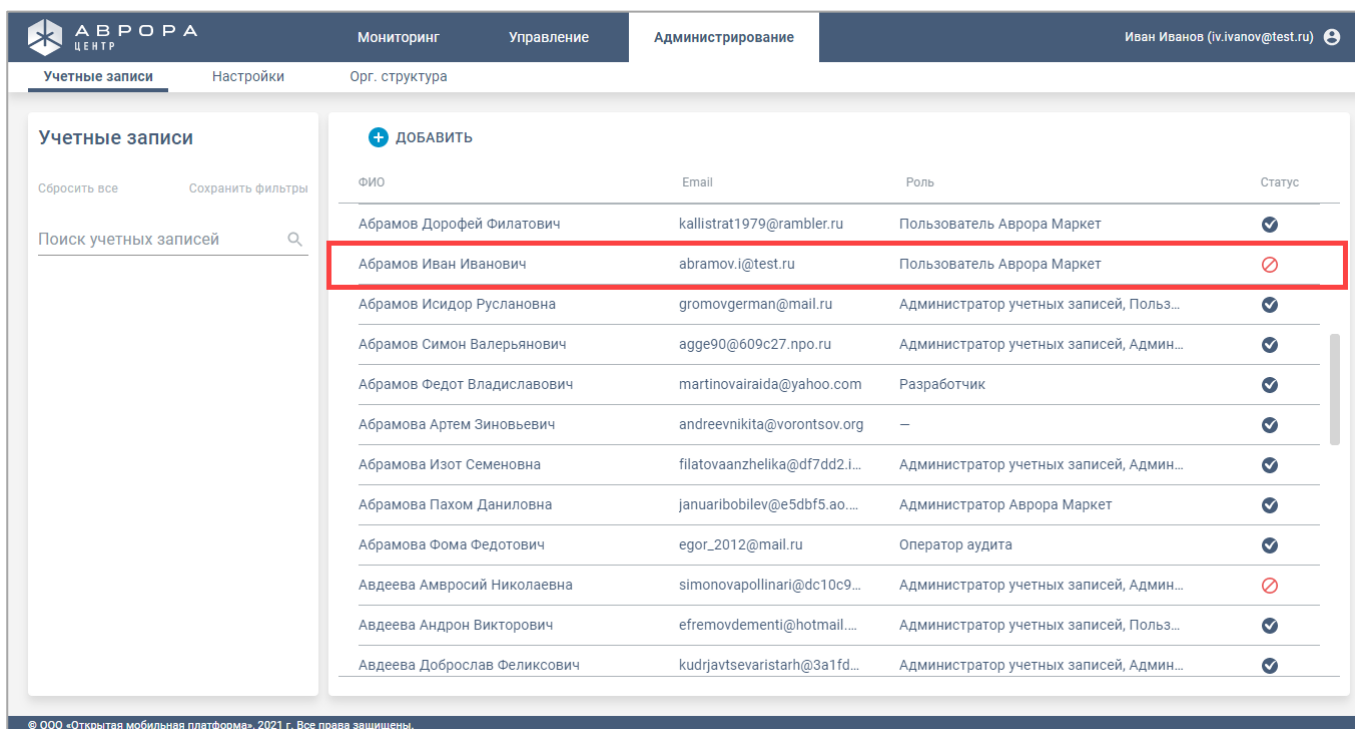
© ООО «Открытая мобильная платформа», 2021 г. Все права защищены.

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);



Учетные записи

Сбросить все Сохранить фильтры

Поиск учетных записей

+ ДОБАВИТЬ

ФИО	Email	Роль	Статус
Абрамов Дорофей Филатович	kallistrat1979@rambler.ru	Пользователь Аврора Маркет	✓
Абрамов Иван Иванович	abramov.i@test.ru	Пользователь Аврора Маркет	✗
Абрамов Исидор Руслановна	gromovgerman@mail.ru	Администратор учетных записей, Польз...	✓
Абрамов Симон Валерьянович	agge90@609c27.npo.ru	Администратор учетных записей, Админ...	✓
Абрамов Федот Владиславович	martinovairaida@yahoo.com	Разработчик	✓
Абрамова Артем Зиновьевич	andreevnikita@vorontsov.org	–	✓
Абрамова Изот Семеновна	filatovaanzhelika@df7dd2.i...	Администратор учетных записей, Админ...	✓
Абрамова Пахом Даниловна	januaribobilev@e5dbf5.ao...	Администратор Аврора Маркет	✓
Абрамова Фома Федотович	egor_2012@mail.ru	Оператор аудита	✓
Авдеева Амвросий Николаевна	simonovapollinari@dc10c9...	Администратор учетных записей, Админ...	✗
Авдеева Андрон Викторович	efremovdementi@hotmail...	Администратор учетных записей, Польз...	✓
Авдеева Доброслав Феликсович	kudrjavitsevaristarh@3a1fd...	Администратор учетных записей, Админ...	✓

© ООО «Открытая мобильная платформа», 2021 г. Все права защищены.

Рисунок 27

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

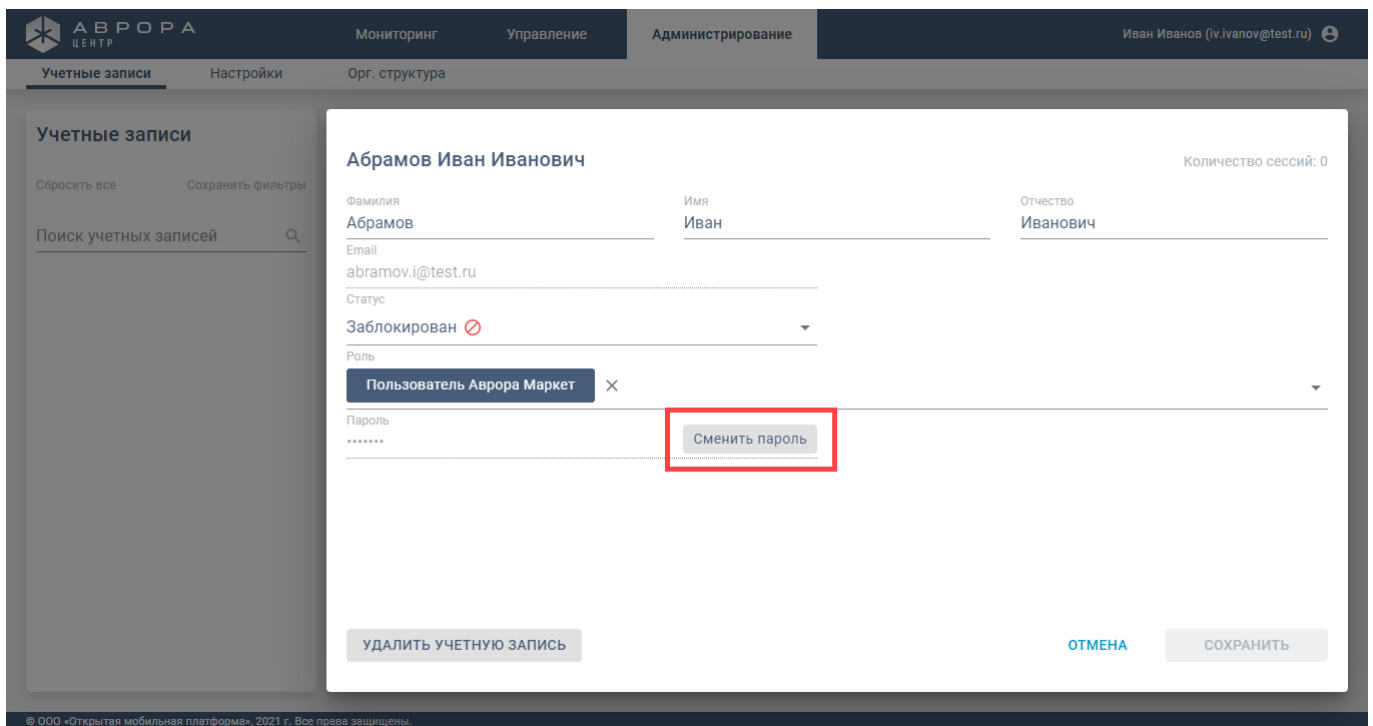


Рисунок 28

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

– далее нажать кнопку «Сохранить». Для отмены смены пароля нажать кнопку «Отмена».

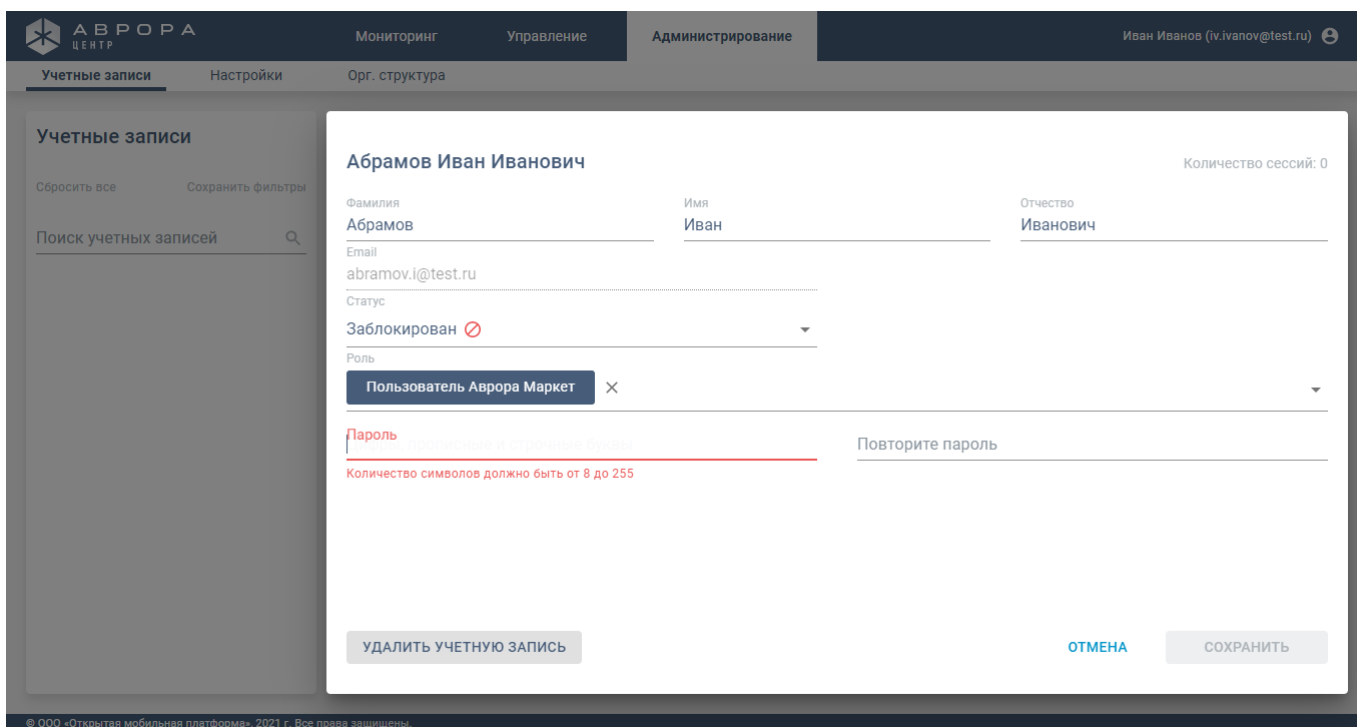


Рисунок 29

При успешном изменении пароля учетной записи отобразится сообщение «Учетная запись успешно обновлена» (Рисунок 30).

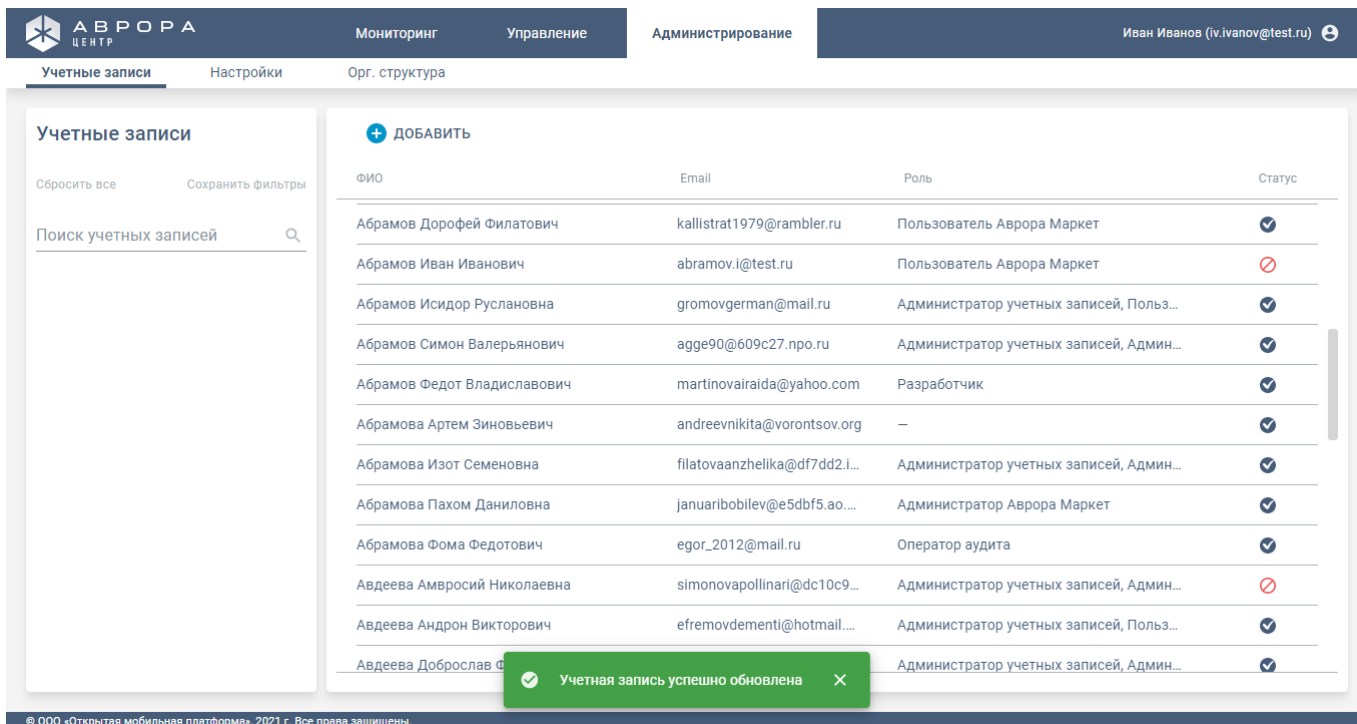


Рисунок 30

3.1.1.5. Удаление учетной записи

Для удаления данных учетной записи необходимо выполнить следующие действия:

- нажать на строку учетной записи (см. Рисунок 27);
- в открывшейся форме нажать кнопку «Удалить учетную запись»

(Рисунок 31);

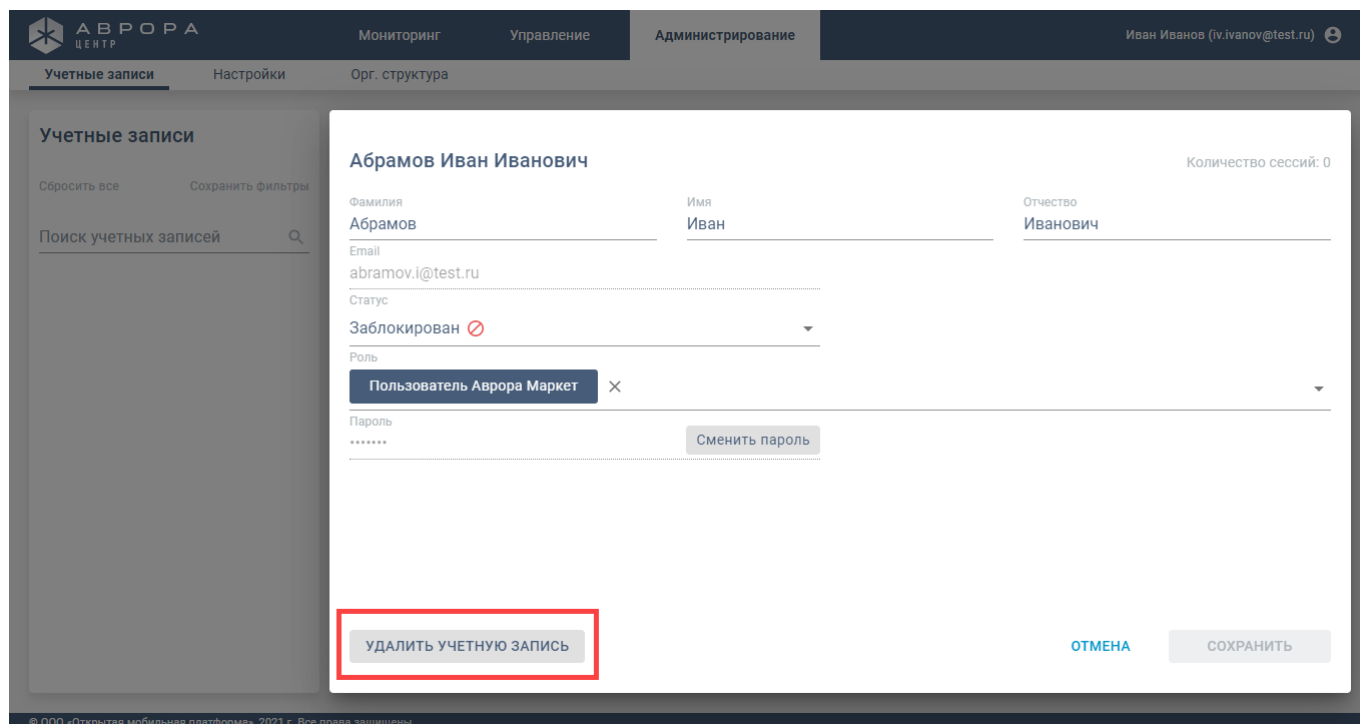


Рисунок 31

– в открывшемся окне нажать кнопку «Подтвердить» (Рисунок 32). Для отмены удаления нажать кнопку «Отмена»;

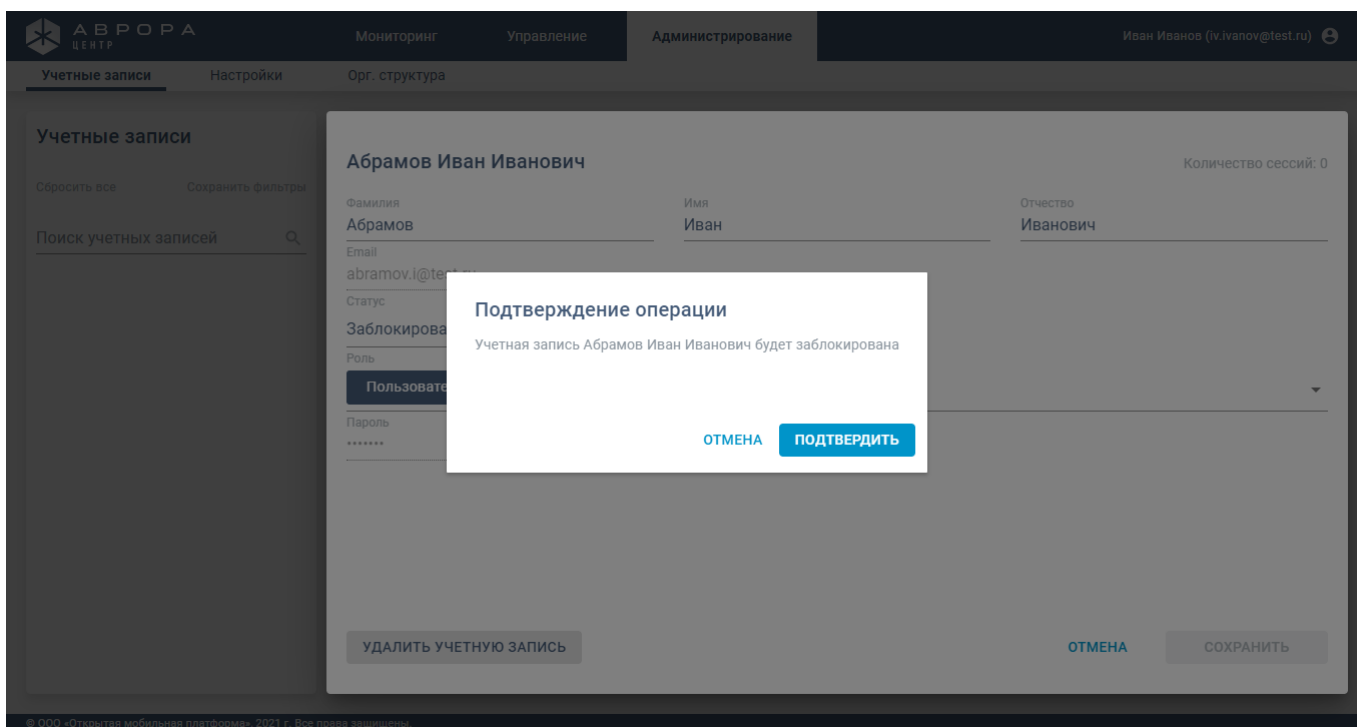


Рисунок 32

– в результате отобразится сообщение «Учетная запись успешно удалена» (Рисунок 33).

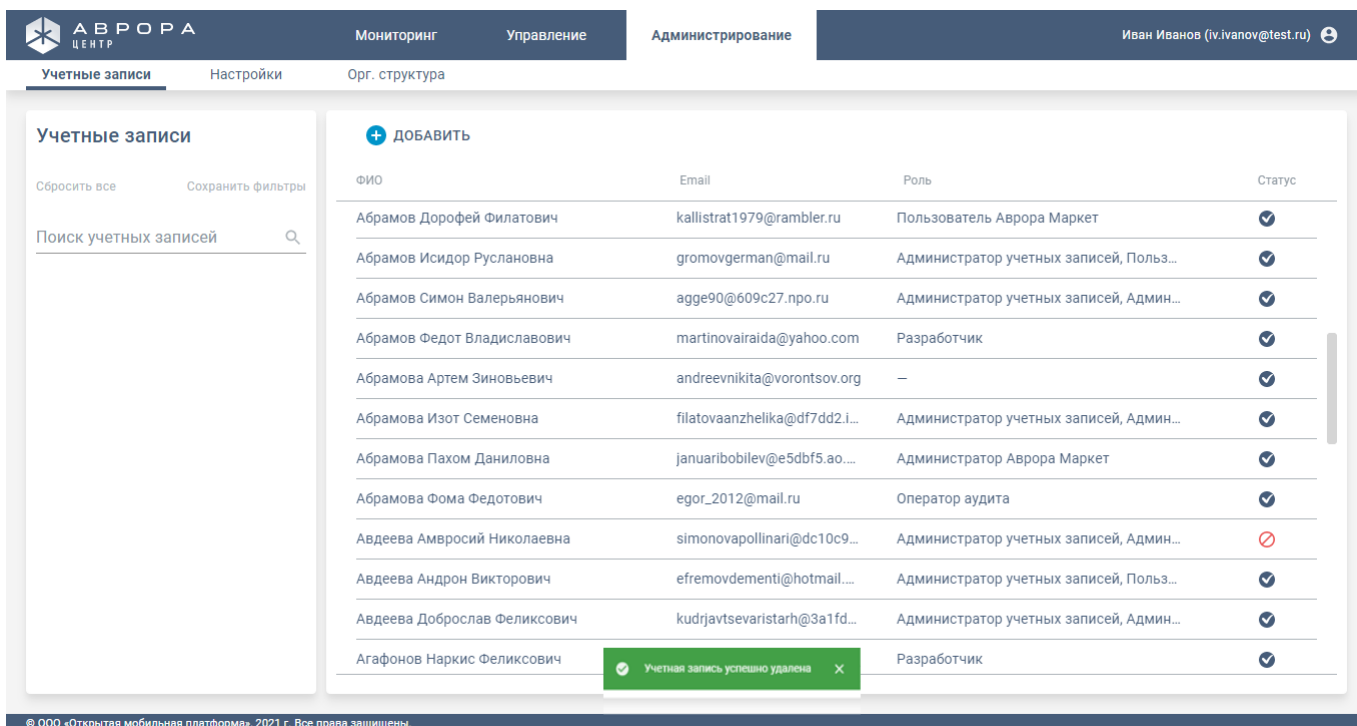


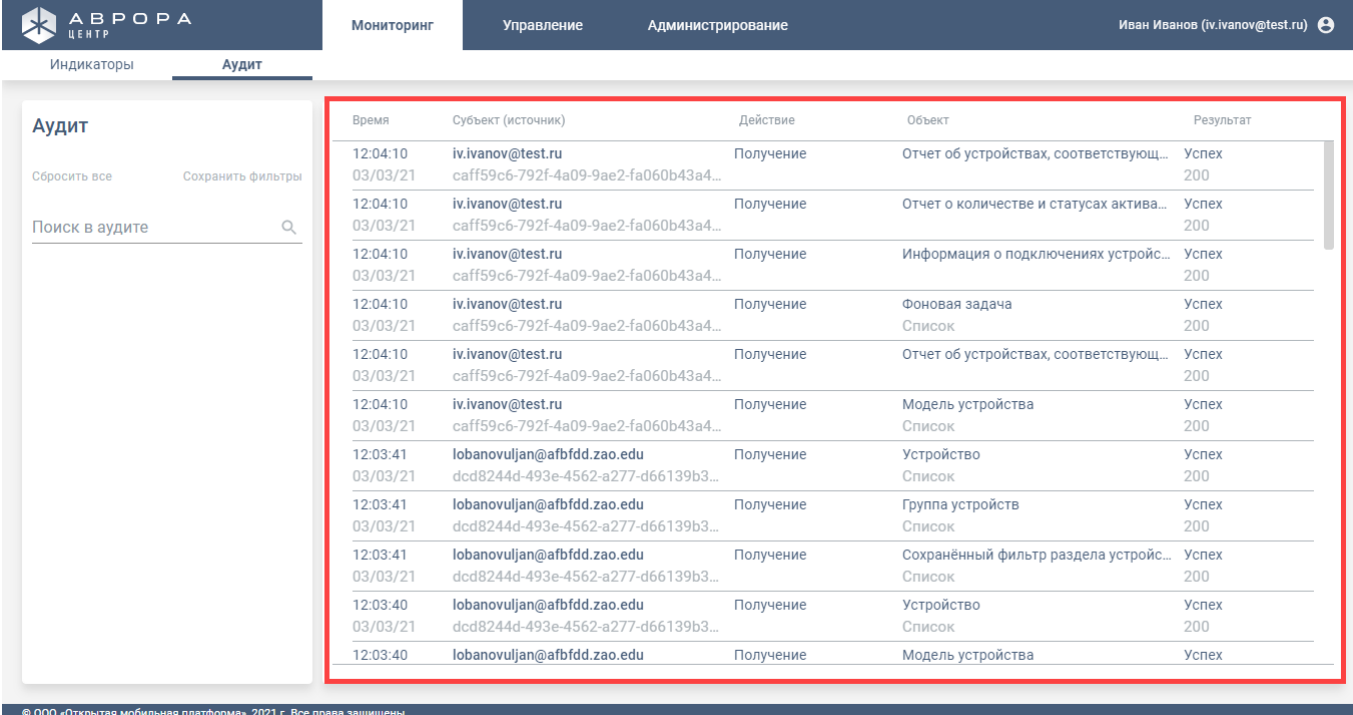
Рисунок 33

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 34).



Время	Субъект (источник)	Действие	Объект	Результат
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Отчет об устройствах, соответствующ...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Отчет о количестве и статусах актива...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Информация о подключениях устройс...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Фоновая задача Список	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Отчет об устройствах, соответствующ...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Модель устройства Список	Успех 200
12:03:41 03/03/21	lobanovuljan@afbddd.zao.edu dcd8244d-493e-4562-a277-d66139b3...	Получение	Устройство Список	Успех 200
12:03:41 03/03/21	lobanovuljan@afbddd.zao.edu dcd8244d-493e-4562-a277-d66139b3...	Получение	Группа устройств Список	Успех 200
12:03:41 03/03/21	lobanovuljan@afbddd.zao.edu dcd8244d-493e-4562-a277-d66139b3...	Получение	Сохранённый фильтр раздела устройс...	Успех 200
12:03:40 03/03/21	lobanovuljan@afbddd.zao.edu dcd8244d-493e-4562-a277-d66139b3...	Получение	Устройство Список	Успех 200
12:03:40 03/03/21	lobanovuljan@afbddd.zao.edu dcd8244d-493e-4562-a277-d66139b3...	Получение	Модель устройства	Успех

Рисунок 34

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

Таблица 8

Элемент	Описание	Возможные значения
Время	Время и дата наступления события	– дата в формате DD/ММ/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"> – «Вход в систему»; – «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 или формат вывода информации на экране – «Список» 	<ul style="list-style-type: none"> – «Отчет об устройствах, соответствующих политике»; – «Информация о подключениях устройств»; – «Сохранённый фильтр раздела устройства»; – «Модель устройства»; – «Фоновая задача»; – «Отчет о количестве и статусах активации устройств»; – «Категория»; – «Приложение»; – «Релиз»; – «Иконка»; – «Билд»; – «Скриншот»; – «Учетная запись»;

Элемент	Описание	Возможные значения
		<ul style="list-style-type: none"> – «Роль»; – «Событие аудита»; – «Параметры доступа к серверу Аврора Маркет»; – «Связь»; – «Группа устройств»; – «Устройство»; – и т.д.
Результат	Ответ ППО и код состояния HTTP	<ul style="list-style-type: none"> – Создано; – Обновлено; – Ошибка 401 (403, 404 и т.д.); – Успех 200 (201 и т.д.)

3.2.1.2. Работа с фильтрами

В области фильтров предусмотрена возможность поиска по заданным критериям (см. Таблица 6, см. Рисунок 9).

Для поиска необходимо выполнить следующие действия (см. Рисунок 9):

- 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 35).

Время	Субъект (источник)	Действие	Объект	Результат
12:04:12 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Событие аудита Список	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Отчет об устройствах, соответствующ...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Отчет о количестве и статусах актива...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Информация о подключенных устройс...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Фоновая задача Список	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Отчет об устройствах, соответствующ...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Модель устройства Список	Успех 200
12:02:57 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Роль Список	Успех 200
12:02:48 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Учетная запись Список	Успех 200
11:56:04 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Учетная запись Список	Успех 200
11:55:56	iv.ivanov@test.ru	Получение	Учетная запись	Успех

Рисунок 35

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 36);

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

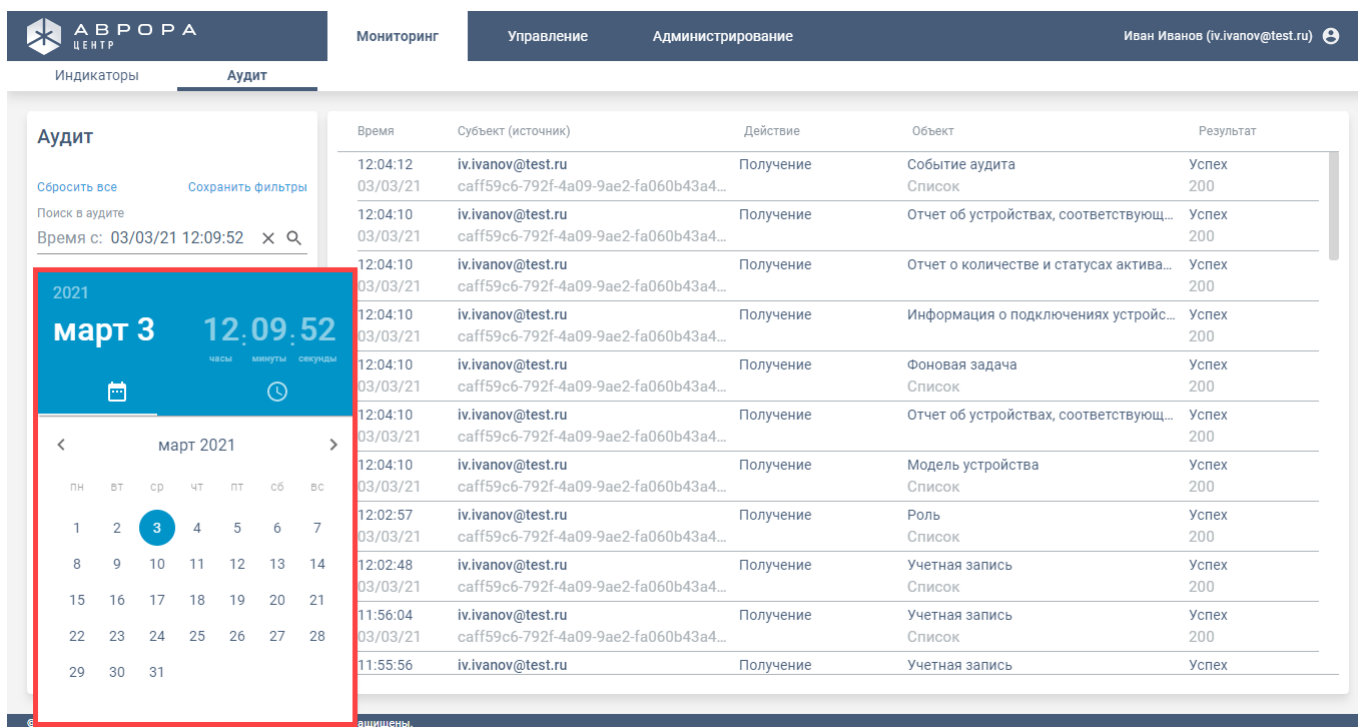



Рисунок 36

— далее после выбора даты события необходимо выбрать время события, коснувшись значка . В результате отобразится циферблат, где необходимо выбрать время события (Рисунок 37);

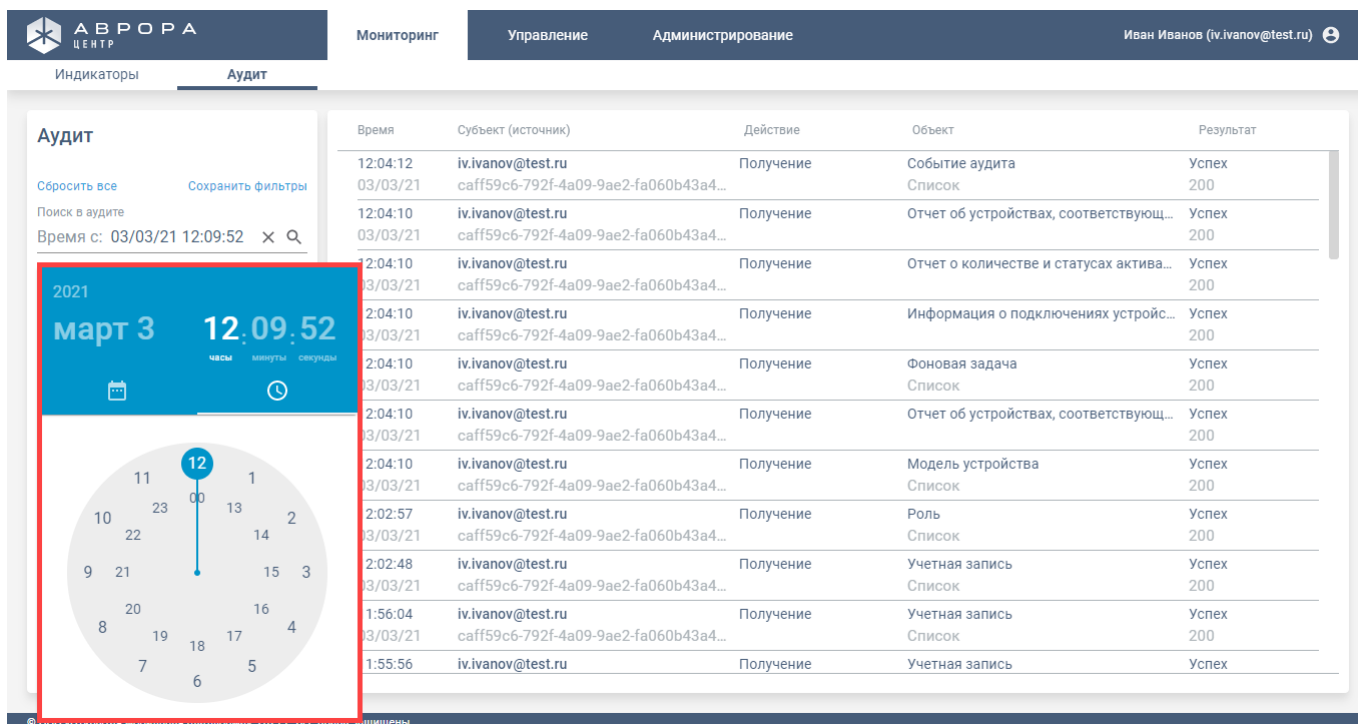


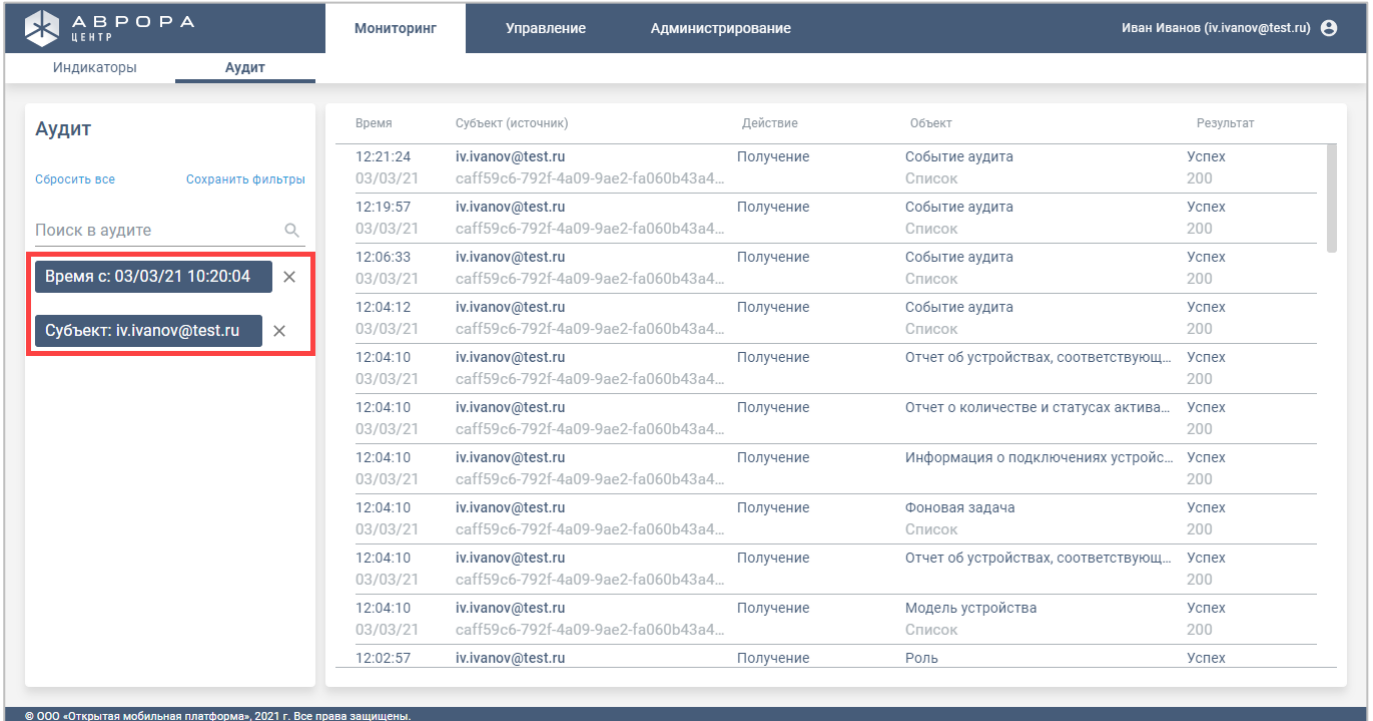


Рисунок 37

- нажать на значок , для очистки поля нажать на значок ;
- в рабочей области отобразится перечень, сформированный с применением выбранных фильтров (Рисунок 38).



The screenshot shows the 'Аудит' (Audit) section of the AVROPA CENTR interface. The left sidebar contains a search bar and two active filters: 'Время с: 03/03/21 10:20:04' and 'Субъект: iv.ivanov@test.ru'. The main area displays a table of audit events.

Время	Субъект (источник)	Действие	Объект	Результат
12:21:24 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Событие аудита Список	Успех 200
12:19:57 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Событие аудита Список	Успех 200
12:06:33 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Событие аудита Список	Успех 200
12:04:12 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Событие аудита Список	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Отчет об устройствах, соответствующ...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Отчет о количестве и статусах актива...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Информация о подключении устройс...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Фоновая задача Список	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Отчет об устройствах, соответствующ...	Успех 200
12:04:10 03/03/21	iv.ivanov@test.ru caff59c6-792f-4a09-9ae2-fa060b43a4...	Получение	Модель устройства Список	Успех 200
12:02:57	iv.ivanov@test.ru	Получение	Роль	Успех

Рисунок 38

Для формирования более детальной выборки необходимо добавить несколько фильтров

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 39).

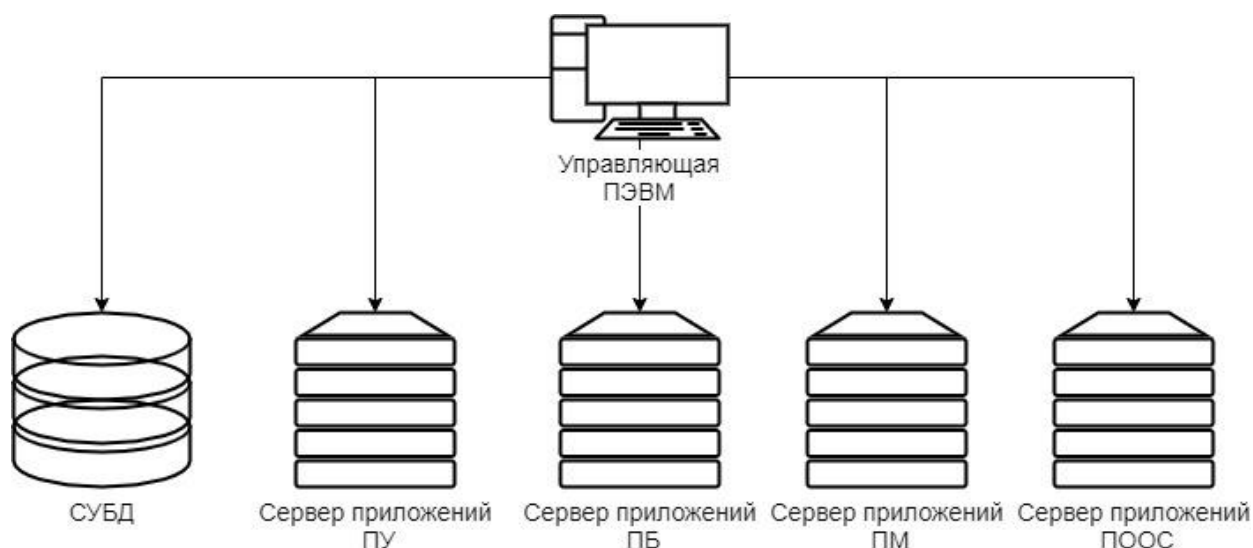


Рисунок 39

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 4.7.7.3 настоящего документа;

2) Конфигурационные файлы модулей ППО:

- ПБ;
- ПМ;
- ПУ;
- ПООС.

Описание параметров конфигурационных файлов модулей ППО приведено в разделе 9 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 ППО рассчитаны с использованием программы «Программа фиксации и контроля целостности информации «ФИКС-Unix 1.0» (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 680, действителен до 26 февраля 2021 г., окончание срока технической поддержки 26 февраля 2026 г.) либо с использованием программы «Программа фиксации и контроля исходного состояния программного комплекса «ФИКС» версия 2.0.2 по алгоритму Уровень-3 (разработчик ЗАО «ЦБИ-сервис», сертификат соответствия ФСТЭК России № 1548, действителен до 15 января 2020 г., окончание срока технической поддержки 15 января 2025 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 7/8 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 7/8 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 7/8

```
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.

```
"ip-адрес" "имя_хоста.имя_домена"
```

Например (в файле `/etc/hosts`):

```
192.168.0.108 ocs-app.local
```

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. Задать текущие дату и время с помощью команды:

```
date -s 'YYYY-MM-DD HH:MI:SS'
```

Например:

```
date -s '2021-03-31 12:34:56'
```

4.3.1.10. 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 7/8 (управляющая ПЭВМ):

```
sudo yum -y install epel-release  
sudo yum -y install jq  
sudo yum -y install python2-pip  
sudo python -m pip install --upgrade "pip < 21.0"  
sudo python -m pip install wheel  
sudo python -m pip install ansible==2.9.18  
sudo yum -y install sed  
sudo yum -y install coreutils
```

– ОС Альт 8 СП (управляющая ПЭВМ):

```
sudo apt-get install python-module-pip
sudo python -m pip install --upgrade "pip<21.0"
sudo python -m pip install ansible==2.9.18
sudo python -m pip install psycopg2
sudo apt-get -y install jq
sudo apt-get -y install coreutils
```

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

4.3.2.3. Скопировать каталог /server, находящийся на DVD с Изделием, на управляющую ПЭВМ.

4.3.2.4. Перейти в каталог /server с помощью команды:

```
cd <путь к каталогу server>
```

4.3.2.5. Назначить пользователю право на исполнение файла installer_<вариант поставки¹⁰>.sh с помощью команды:

¹⁰ Варианты поставки ППО описаны в п. 5.1.1 документа «Формуляр». Файл installer_ac.sh соответствует варианту поставки №1, файл installer_am.sh - варианту №2, файл installer_mm.sh - варианту №3.


```
chmod +x installer-<вариант поставки>.sh
```

Например:

```
chmod +x installer-ac.sh
```

4.3.2.6. Запустить installer-<вариант поставки>.sh с помощью команды:

```
./installer-<вариант поставки>.sh
```

Например:

```
./installer-ac.sh
```

4.3.2.7. Ознакомиться с «Лицензионным соглашением» и принять его

Для того чтобы принять «Лицензионное соглашение» (Рисунок 37), необходимо после вопроса «Вы принимаете условия лицензии (y/n)?» ввести «у».

В результате в каталоге с файлом installer_<вариант поставки>.sh будет создан каталог install-<версия ППО>. Например, /install-release-v2.5.0.

```
[omr@ocs-app ~]$ ./installer_ac.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»), 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» (ППО «Аврора Центр»), состоящее из следующих подсистем: прикладного программного обеспечения «Аврора Центр: Платформа управления» (ППО «Аврора Центр: Платформа управления»), прикладного программного обеспечения «Аврора Центр: Маркет» (ППО «Аврора Центр: Маркет») и Сервиса уведомлений Аврора, подробное описание функциональных возможностей которого содержится в Документации. Данное Лицензионное соглашение применяется как к ППО «Аврора Центр», включающему в себя все перечисленные выше подсистемы, так и к каждой подсистеме в отдельности вне зависимости от комплектности.

«Документация» – относящиеся к ПО сопроводительные материалы, в том числе Руководство по установке и настройке, Руководство Пользователя, Руководство Администратора, которые принадлежат Правообладателю.

«Устройство» – это аппаратная система (физическая или виртуальная) со встроенным запоминающим устройством, на которых может быть запущено ПО.

«Права на интеллектуальную собственность» – все права на интеллектуальную и промышленную собственность, включая права на изобретения, открытия и патенты на изобретения, включая заявки на выдачу патентов и ранее выданные патенты, повторные заявки или заявки в продолжение и частичные продолжения; авторские права; образцы и промышленные образцы; товарные знаки, знаки обслуживания, оформление товара и права на аналогичные объекты; секреты производства (ноу-хау), коммерческую тайну и конфиденциальную информацию; права на топологии интегральных микросхем и права на фотошаблоны; и другие исключительные права.

«Лицензионное соглашение» – предоставляемое Вам Правообладателем ограниченное право на использование функциональности ПО на условиях простой (неисключительной) лицензии в соответствии с условиями настоящего Лицензионного соглашения.

«Конечный пользователь» – любое юридическое лицо (организация), которое приобрело ПО для собственного использования и не для продажи.

«Пользователь» – физическое лицо, непосредственно осуществляющее эксплуатацию ПО в целях и порядке, определяемом Конечным пользователем.

Настоящее Лицензионное соглашение является юридическим соглашением между Вами (далее по тексту – Конечный пользователь) и Правообладателем.

Рисунок 40

4.3.3. Порядок установки и настройки компонентов среды функционирования

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

4.3.3.1. Перейти в каталог со сценариями установки с помощью команды:

```
cd install-<версия ППО>/install-<вариант поставки>
```

Например:

```
cd install-release-v2.5.0/install-ac/
```

Дальнейшие действия по установке и настройке компонентов среды функционирования ППО, а также ППО, необходимо выполнять из данного каталога

4.3.3.2. 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:
    ocs:
      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 п. 9.1.1 настоящего документа.

4.3.3.3. В конфигурационном файле `config/vars/_vars.yml` необходимо задать, либо поменять предустановленные значения следующих параметров:

- параметры подключения подсистем ППО к БД

```
postgresql:
  dbname: example_db_name      # database name
  port: 5432                   # port
  user: example_user          # user
  password: ocs                # password
```

– пароль суперпользователя СУБД PostgreSQL, который был задан при установке СУБД:

```
postgres_password: "postgres"
```

– токен доступа к сервису гарантированной доставки сообщений Nats

Streaming Server:

```
nats: auth_token: "FF12fddgdhFLL"
```

– пароль доступа к СУБД Redis в параметре `redis_password`:

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

– токен доступа к системе обнаружения сервисов Consul:

```
consul_acl_master_token: "ae9f5abb-6b8f-9252-59c5-53bcb651f182"
```

Описание параметров конфигурационного файла `config/vars/_vars.yml` приведено в п. 9.1.2 настоящего документа.

4.3.3.4. Настроить параметры взаимодействия клиентов СУБД (при необходимости)

По умолчанию сценарии установки автоматически задают параметры взаимодействия клиентов (например, серверов приложений ППО) СУБД.

Дополнительную настройку взаимодействия клиентов СУБД необходимо осуществлять в соответствии с п. 4.7.2.

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

```
set -o pipefail
```

4.3.3.6. Установить на сервера приложений и сервера БД необходимые пакеты с помощью команд:

– сервера приложений:

```
ansible-playbook -i inventories/hosts.yml play-managed-node-  
prerequisites.yml -vv -u <ИМЯ ПОЛЬЗОВАТЕЛЯ> --extra-vars "node_type=app"  
--limit app
```

– сервера БД:

```
ansible-playbook -i inventories/hosts.yml play-managed-node-  
prerequisites.yml -vv -u <ИМЯ ПОЛЬЗОВАТЕЛЯ> --extra-vars "node_type=db"  
--limit postgresql
```

Например:

– сервера приложений:

```
ansible-playbook -i inventories/hosts.yml play-managed-node-
prerequisites.yml -vv -u omp --extra-vars "node_type=app" --limit app
```

– сервера БД:

```
ansible-playbook -i inventories/hosts.yml play-managed-node-
prerequisites.yml -vv -u omp --extra-vars "node_type=db" --limit
postgresql
```

Порядок действий для самостоятельной установки пакетов приведен в п. 4.7.8.

4.3.3.7. Установить компоненты среды функционирования ППО с помощью команды:

```
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh --database
<версия СУБД PostgreSQL> --extra-vars "force_upgrade=true"
```

Например:

```
ANSIBLE_USER="omp" ./deploy-infra.sh --database "11" --extra-vars
"force_upgrade=true"
```

Описание параметров команды приведено в таблице (Таблица 9).

Таблица 9

Параметр	Описание	Допустимые значения
--database	Версия СУБД PostgreSQL	«11» - при использовании СУБД PostgreSQL 11 «12» - при использовании СУБД PostgreSQL 12 При отсутствии параметра будет установлена СУБД PostgreSQL 11

Параметр	Описание	Допустимые значения
<имя пользователя>	В параметре указывается имя привилегированного sudo-пользователя, под которым настроен SSH-доступ к серверам приложений и БД. 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	
--skip-database	При наличии данного параметра СУБД не устанавливается	

При использовании СУБД Postgres Pro, либо если установку СУБД PostgreSQL 11/12 необходимо выполнить самостоятельно (без использования сценариев установки компонентов среды функционирования ППО), то команда установки компонентов среды функционирования имеет следующий вид:

```
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh --skip-database
```

Описание установки и настройки СУБД Postgres Pro, а также требования к самостоятельной установке СУБД приведены подразделе 4.6.

4.4. Порядок установки ППО

Для установки ППО необходимо выполнить следующие действия:

4.4.1. Обеспечение синхронизации времени между нодами кластера

При эксплуатации ППО в кластерной конфигурации, необходимо обеспечить синхронизацию времени между нодами кластера (например, с помощью утилиты `crony`).

Для проверки синхронизации времени необходимо запустить `bash`-скрипт, предварительно задав адреса хостов в переменной `HOSTS`:

```
#!/bin/bash
HOSTS="
example-db01.ompcloud
example-db02.ompcloud
example-inplint01.ompcloud
example-inplint02.ompcloud
example-inplint03.ompcloud
"
# Prepare ssh sessions to increase speed time checking.
for i in $HOSTS
do
    ssh $i "echo $i session created" > /dev/null
done
for i in $HOSTS
do
    ssh $i "echo $i `date`" &
done
sleep 10
```

4.4.2. Выполнение настройки ППО (подсистем ППО)

ВНИМАНИЕ! Перед выполнением настроек необходимо ознакомиться с информацией, приведенной в п. 10.2.7.

ПБ необходимо устанавливать всегда. Установка остальных подсистем ППО (ПМ, ПУ и ПООС) является опциональной, либо зависит от варианта поставки ППО

Для настройки ППО необходимо выполнить следующие действия:

4.4.2.1. Перейти в созданный каталог (каталог: /install-<версия ППО>/install-<вариант поставки>/) и отредактировать конфигурационный файл config/vars/_vars.yml

В данном конфигурационном файле необходимо задать, либо поменять предустановленные значения:

– доменное имя для межсервисного взаимодействия в рамках одной ноды (узла сервера) должно иметь значение local (domain: local);

– внешние (публичные) адреса ППО:

```
aps_admin_address: "http://ocs-app.local:8009"
aps_client_address: "http://ocs-app.local:8009"
aps_dev_address: "http://ocs-app.local:8009"
aps_market_address: "http://ocs-app.local:8009"
auth_admin_address: "http://ocs-app.local:8009"
auth_public_address: "http://ocs-app.local:8009"
emm_admin_address: "http://ocs-app.local:8009"
emm_mobile_address: "http://ocs-app.local:8009"
pkgrepo_admin_address: "http://ocs-app.local:8009"
pkgrepo_mobile_address: "http://ocs-app.local:8009"
push_admin_address: "http://ocs-app.local:8009"
push_public_address: "http://ocs-app.local:8009"
```

– уровень детализации сообщений логирования (рекомендуется задать "info" при тестовой эксплуатации и "warning" при промышленной эксплуатации):

```
logger_level: "info"
```

Описание config/vars/_vars.yml параметров конфигурационного файла приведено в п. 10.3.2, 10.3.3, 10.3.4, 10.3.5.

4.4.2.2. Задать секретные ключи клиентов (сервисов) в конфигурационных файлах подсистем ППО (файлы: config/subsystems/<название подсистемы>/vars/_vars.yml)

Секретные ключи клиентов (сервисов) задаются в параметре *_client_secret, например:

```
auth_admin_console_client_secret:  
"7dd7c204aa4f6192e70fadc5642d3755" # Secret for OIDC client auth-admin-  
console
```

Описание параметров конфигурационных файлов config/subsystems/<название подсистемы>/vars/_vars.yml приведено в п. 10.3.2, 10.3.3, 10.3.4, 10.3.5.

4.4.2.3. В секциях system и cookie конфигурационного файла config/subsystems/auth/config/services/config.yml.j2 задать пароли, используемые для защиты критичной информации (например, cookie сессии).

Для этого необходимо удалить приведенные примеры и задать новые значения паролей, например:

```
system:  
  - kdj%93cxk+  
cookie:  
  - 9v_wer8*&r
```

Важно! При обновлении ППО нельзя удалять старые пароли. Новые пароли должны быть добавлены в начало списка.

Описание параметров конфигурационного файла config/subsystems/auth/config/services/config.yml.j2 приведено в п. 10.3.2.

4.4.2.4. Выполнить другие дополнительные настройки ППО и настройки подсистем ППО (при необходимости)

Важно! Перед установкой ППО выполнить дополнительные настройки ППО и настройки подсистем ППО (при необходимости).

Перечень и описание дополнительных настроек ППО приведен в подразделе 4.7.

Перечень и описание настроек ПМ приведен в документе «Руководство администратора. Часть 2. Подсистема «Маркет».

Перечень и описание настроек ПУ приведен в документе «Руководство администратора. Часть 3. Подсистема Платформа управления».

4.4.3. Установка ППО

Для установки ППО необходимо выполнить команду:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --database <СУБД>
```

Описание параметров запуска скрипта `deploy-ac.sh` и их возможные значения приведены в пункте 7.1.

Например:

```
ANSIBLE_USER=omp ./deploy-ac.sh --database 11
```

Для установки подсистем по отдельности необходимо в параметре `--subsystems` задать имя подсистемы, например:

– ПБ:

```
ANSIBLE_USER=omp ./deploy-ac.sh --subsystems auth --database 11
```

– ПМ:

```
ANSIBLE_USER=omp ./deploy-ac.sh --subsystems appstore --database 11
```

– ПУ:

```
ANSIBLE_USER=omp ./deploy-ac.sh --subsystems emm --database 11
```

– ПООС:

```
ANSIBLE_USER=omp ./deploy-ac.sh --subsystems pkgrepo --database 11
```

4.4.4. Проверка корректности установки и функционирования ППО

Проверка осуществляется в соответствии с подразделом 4.8.

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 10) приведены адреса веб-консолей.

Таблица 10

Веб-консоль	URL-адрес веб-консоли
При разделении трафика по портам	
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
При разделении трафика по basepath (url-адресам)	
Консоль администратора ПБ	http://<сервер приложения>:8009/auth/admin/
Консоль администратора ПМ	http://<сервер приложения>:8009/appstore/admin/
Консоль разработчика ПМ	http://<сервер приложения>:8009/appstore/dev/
Консоль администратора ПУ	http://<сервер приложения>:8009/emm/admin/

4.6. Самостоятельная установка и настройка СУБД

4.6.1. Порядок установки и настройки СУБД Postgres Pro

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

4.6.1.1. 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
```

4.6.1.2. Установить и инициализировать СУБД Postgres Pro

При инициализации СУБД должны быть установлены следующие значения параметров:

```
LC_COLLATE 'en_US.UTF-8'
LC_CTYPE 'en_US.UTF-8'
ENCODING UTF8
```

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
```

4.6.1.3. 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.

4.6.1.4. Установить расширение pg_partman с помощью команды:

- ОС CentOS версии 7

```
sudo rpm -ivh pg_partman11pro-v4.3.0-1.el7.x86_64.rpm
```

– ОС Альт 8 СП

```
sudo rpm -ivh pg_partman11pro-4.3.0-1.alt.x86_64.rpm
```

Указанные rpm-пакеты находятся на DVD с загрузочными модулями ППО в каталоге `/server/install-infra.tar.gz/install-infra/binary/postgresql/pg_partman/`.

4.6.1.5. Перезапустить сервис СУБД Postgres Pro с помощью команды:

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

4.6.2. Порядок установки и настройки СУБД PostgreSQL 11/12

4.6.2.1. Установить на сервера БД, работающие под управлением ОС CentOS 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 CentOS версии 8 (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
sudo yum -y install python38
sudo yum -y install python38-pip
ln -s /usr/libexec/platform-python /usr/bin/python
```

4.6.2.2. Выполнить установку и настройку СУБД PostgreSQL 11/12 в соответствии с документацией на СУБД.

При инициализации СУБД должны быть установлены следующие значения параметров:

```
LC_COLLATE 'en_US.UTF-8'  
LC_CTYPE 'en_US.UTF-8'  
ENCODING UTF8
```

4.6.2.3. Установить расширение pg_partman с помощью команды:

– ОС CentOS версии 7 и СУБД PostgreSQL 11

```
sudo rpm -ivh pg_partman11-4.2.0-1.rhel7.x86_64.rpm
```

– ОС CentOS версии 8 и СУБД PostgreSQL 11

```
sudo rpm -ivh pg_partman11-4.4.0-1.rhel8.x86_64.rpm
```

– ОС Альт 8 СП и СУБД PostgreSQL 11

```
sudo rpm -ivh pg_partman11-4.1.0-1-alt.x86_64.rpm
```

– ОС CentOS версии 7 и СУБД PostgreSQL 12

```
sudo rpm -ivh pg_partman12-4.4.1-1.rhel7.x86_64.rpm
```

– ОС CentOS версии 8 и СУБД PostgreSQL 12

```
sudo rpm -ivh pg_partman12-4.4.0-1.rhel8.x86_64.rpm
```

Указанные rpm-пакеты находятся на DVD с загрузочными модулями ППО в каталоге /server/install-infra.tar.gz/install-infra/binary/postgresql/pg_partman/.

4.6.2.4. Перезапустить сервис СУБД 12 в соответствии с документацией на СУБД.

4.7. Дополнительные настройки ППО и среды функционирования ППО

4.7.1. Настройка взаимодействия сервера приложений ПУ с SMTP-сервером

Для настройки взаимодействия ППО с SMTP-сервером необходимо в секции SMTP конфигурационного файла ПУ (файл: config/subsystems/emm/config/services/config.yml.j2) задать требуемые значения:

– адрес эл. почты, с которого отправляются письма (параметр: from);

- адрес сервера эл. почты (параметр: address);
- тип аутентификации (параметр: authType);
- параметры для заданного типа аутентификации (username, password и др.).

Значения параметров from и username должны быть идентичны, иначе почтовый сервер будет отклонять сообщения

Подробное описание параметров конфигурационного файла /var/ocs/emm/config.yml приведено в п. 10.3.4

В ПУ поддерживаются следующие типы аутентификации SMTP:

- PLAIN

```
smtp:
  from: "no-reply@inplscloud03.omplcloud"
  address: "inplscloud03.omplcloud:1025"
  tls: true
  authType: "PLAIN"
  host: "inplscloud03.omplcloud"
  username: "no-reply@inplscloud03.omplcloud"
  password: "test_password"
  identity: "no-reply@inplscloud03.omplcloud"
```

- CRAM-MD5

```
smtp:
  from: "no-reply@inplscloud03.omplcloud"
  address: "inplscloud03.omplcloud:1025"
  tls: true
  authType: "CRAM-MD5"
  username: "no-reply@inplscloud03.omplcloud"
  secret: "test_secret"
```

- LOGIN

```
smtp:
  from: "no-reply@inplscloud03.omplcloud"
  address: "inplscloud03.omplcloud:1025"
  tls: true
  authType: "LOGIN"
```

```
username: "no-reply@inp1sfcloud03.ompccloud"  
password: "password"
```

4.7.2. Настройка взаимодействия клиентов СУБД

Настройки взаимодействия клиентов с СУБД задаются в секции `pg_hba_settings` конфигурационного файла `config/vars/_vars_infra.yml`.

В данной секции содержатся следующие параметры:

- `type` - тип подключения к СУБД;
- `name` - имена пользователей СУБД, правила доступа для которых определяет данная запись;
- `database` - имена баз данных, доступ к которым описывает данная запись;
- `address` - IP-адрес подключения или IP-адрес подсети
- `method` - метод аутентификации.

Описание секций конфигурационного файла приведено в п. 9.1.3.

4.7.3. Настройка разделения трафика

ППО позволяет разделять входящий трафик (`url`-запросы) следующими способами:

- по портам - в данном случае каждая Консоль администратора/разработчика (либо API для взаимодействия с МП) привязана к определенному порту;
- по `basepath` (`url`-адресам) - в данном случае каждая Консоль администратора/разработчика (либо API для взаимодействия с МП) привязана к определенному `url`-адресу;
- по доменам (субдоменам) – в данном случае каждая Консоль администратора/разработчика и API для взаимодействия с МП (либо группа консолей и API) привязана к определенному домену. Рекомендуется публичные консоли и API привязывать к домену, который имеет доступ из сети Интернет, а внутренние консоли (Консоли администраторов) привязывать к домену, не имеющему доступ из сети Интернет.

При установке ППО «по умолчанию» разделение трафика осуществляется по basepath (url-адресам)

Для того чтобы выполнить настройку разделения трафика, необходимо в конфигурационном файле `config/vars/_vars.yml` задать значения параметров в соответствии с таблицей (Таблица 11).

Приведенные в таблице значения basepath (не пустые значения basepath) и номера портов носят рекомендательный характер и могут быть изменены. При разделении трафика по портам, значения basepath в конфигурационном файле должны быть пустыми

Таблица 11

Сервис (модуль)	Адрес: порт	Basepath
При разделении трафика по портам		
Auth public API gateway (интерфейс ППО для идентификации и аутентификации пользователей)	auth_public_address: "http://<сервер приложения>:8018"	auth_public_basepath: ""
Auth admin API gateway (Консоль администратора ПБ)	auth_admin_address: "http://<сервер приложения>:8019"	auth_admin_basepath: ""
AMM device API gateway (API для взаимодействия с МП «Аврора Центр»)	emm_mobile_address: "http://<сервер приложения>:8012"	emm_mobile_basepath: ""
AMM admin API gateway (Консоль администратора ПУ)	emm_admin_address: "http://<сервер приложения>:8011"	emm_admin_basepath: ""
Aurora market admin API gateway (Консоль администратора ПМ)	aps_admin_address: "http://<сервер приложения>:8015"	aps_admin_basepath: ""
Aurora market development API gateway (Консоль разработчика ПМ)	aps_dev_address: "http://<сервер приложения>:8014"	aps_dev_basepath: ""
Aurora market client API gateway (API для взаимодействия с МП «Аврора Маркет»)	aps_client_address: "http://<сервер приложения>:8016" aps_market_address: "http://<сервер приложения>:8016"	aps_client_basepath: "" aps_market_basepath: ""

Сервис (модуль)	Адрес: порт	Basepath
Package repository admin API gateway (API для взаимодействия с ПООС только для взаимодействия ПУ с ПООС)	pkgrepo_admin_address: "http://<сервер приложения>:8022"	pkgrepo_admin_basepath: ""
Файловый сервер ПООС	pkgrepo_mobile_address: "http://<сервер приложения>:8030"	pkgrepo_mobile_basepath: ""
При разделении трафика по basepath (url-адресам)		
Auth public API gateway (интерфейс ППО для идентификации и аутентификации пользователей)	auth_public_address: "http://<сервер приложения>:8009"	auth_public_basepath: "/auth/public"
Auth admin API gateway (Консоль администратора ПБ)	auth_admin_address: "http://<сервер приложения>:8009"	auth_admin_basepath: "/auth/admin"
AMM device API gateway (API для взаимодействия с МП «Аврора Центр»)	emm_mobile_address: "http://<сервер приложения>:8009"	emm_mobile_basepath: "/emm/mobile"
AMM admin API gateway (Консоль администратора ПУ)	emm_admin_address: "http://<сервер приложения>:8009"	emm_admin_basepath: "/emm/admin"
Aurora market admin API gateway (Консоль администратора ПМ)	aps_admin_address: "http://<сервер приложения>:8009"	aps_admin_basepath: "/appstore/admin"
Aurora market development API gateway (Консоль разработчика ПМ)	aps_dev_address: "http://<сервер приложения>:8009"	aps_dev_basepath: "/appstore/dev"
Aurora market client API gateway (API для взаимодействия с МП «Аврора Маркет»)	aps_client_address: "http://<сервер приложения>:8009" aps_market_address: "http://<сервер приложения>:8009"	aps_client_basepath: "/appstore/mobile" aps_market_basepath: "/appstore/mobile"
Package repository admin API gateway (API для взаимодействия с ПООС, только для взаимодействия ПУ с ПООС)	pkgrepo_admin_address: "http://<сервер приложения>:8009"	pkgrepo_admin_basepath: "/pkgrepo/admin"

Сервис (модуль)	Адрес: порт	Basepath
Файловый сервер ПООС	pkgrepo_mobile_address: "http://<сервер приложения>:8009"	pkgrepo_mobile_basepath: "/pkgrepo/mobile"
При разделении трафика по доменам		
Auth public API gateway (интерфейс ППО для идентификации и аутентификации пользователей)	auth_public_address: "http://<субдомен.домен>"	auth_public_basepath: ""
Auth admin API gateway (Консоль администратора ПБ)	auth_admin_address: "http://<субдомен.домен>"	auth_admin_basepath: ""
AMM device API gateway (API для взаимодействия с МП «Аврора Центр»)	emm_mobile_address: "http://<субдомен.домен>"	emm_mobile_basepath: ""
AMM admin API gateway (Консоль администратора ПУ)	emm_admin_address: "http://<субдомен.домен>"	emm_admin_basepath: ""
Aurora market admin API gateway (Консоль администратора ПМ)	aps_admin_address: "http://<субдомен.домен>"	aps_admin_basepath: ""
Aurora market development API gateway (Консоль разработчика ПМ)	aps_dev_address: "http://<субдомен.домен>"	aps_dev_basepath: ""
Aurora market client API gateway (API для взаимодействия с МП «Аврора Маркет»)	aps_client_address: "http://<субдомен.домен>" aps_market_address: "http://<субдомен.домен>"	aps_client_basepath: "" aps_market_basepath: ""
Package repository admin API gateway (API для взаимодействия с ПООС только для взаимодействия ПУ с ПООС)	pkgrepo_admin_address: "http://<субдомен.домен>"	pkgrepo_admin_basepath: ""
Файловый сервер ПООС	pkgrepo_mobile_address: "http://<субдомен.домен>"	pkgrepo_mobile_basepath: ""

Ниже приведен пример разделение трафика на два домена (внутренний – не доступный из сети Интернет, и внешний – доступный из сети Интернет):

```
aps_admin_address: "https://int-ocs.ompcloud"  
aps_dev_address: "https://int-ocs.ompcloud"  
aps_market_address: "https://int-ocs.ompcloud.ru"  
auth_admin_address: "https://int-ocs.ompcloud"  
auth_public_address: "https://int-ocs.ompcloud.ru"  
emm_admin_address: "https://int-ocs.ompcloud"  
emm_mobile_address: "https://int-ocs.ompcloud.ru"  
pkgrepo_admin_address: "https://int-ocs.ompcloud.ru"
```

Описание параметров конфигурационного файла `config/vars/_vars.yml` приведено в п. 10.3.2, 10.3.3, 10.3.4, 10.3.5.

4.7.4. Пример настройки единого файлового хранилища

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

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`.

В файловом хранилище создать каталог, в котором будут храниться файлы МП (иконки, скриншоты, rpm-пакеты), загружаемые разработчиками. Для этого нужно создать каталог в соответствии с параметром `filestorage_path` конфигурационного файла `config/subsystems/appstore/vars/_vars.yml` и в созданном каталоге создать каталог `applications-api`:

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

Параметр `filestorage_path` конфигурационного файла `config/subsystems/appstore/vars/_vars.yml` может иметь следующий вид:

```
filestorage_path: "/ocs/appstore"
```

Описание параметров конфигурационного файла `config/subsystems/appstore/vars/_vars.yml` приведено в п. 10.3.3.

В файловом хранилище создать каталог, в котором будут храниться пакеты ОС ПООС:

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

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

4.7.5. Настройка кэширования ответов сервисов

Для увеличения производительности ППО применяется кэширование ответов сервисов с помощью Nginx. При этом доступ к закэшированным данным осуществляется через шлюзы доступа ППО.

Настройки кэширования задаются в следующих конфигурационных файлах сценариев установки среды функционирования ППО:

1) в конфигурационном файле `shared_roles/nginx/defaults/main.yml` задаются:

- `cache_enabled` - включение/выключение кэширования;
- `cache_path` - каталог хранения кэша;
- `keys_zone` - имя зоны в разделяемой памяти, где будет храниться кэш;
- `keys_zone_size` - размер зоны в разделяемой памяти;
- `cache_max_size` - максимальный размер выделяемой под кэш памяти (когда место заканчивается, `nginx` сам удаляет устаревшие данные);
- `cache_inactive` - время, после которого кэш будет автоматически очищаться.

Например:

```
cache_enabled: true
cache_path: "/var/cache/nginx"
keys_zone: "proxy_cache"
keys_zone_size: "50m"
cache_max_size: "10G"
cache_inactive: "30m"
```

Максимальный размер выделяемой под кэш памяти должен быть не менее 10 Гб

2) в конфигурационных файлах `config/subsystems/<название подсистемы>/vars/services.yml` задаются API функции (endpoint-ы) ППО для которых необходимо выполнять кэширование, а также параметры кэширования для каждой API функции:

- `proxy_cache` - включение кэширования для API функции;
- `proxy_cache_valid` - время кэширования ответа (возможно задать время кэширования для определенных статусов ответа);
- `proxy_cache_lock` - параметр определяет возможность прохождения нескольких запросов на бэкенд (к сервисам ППО). При значении «on» запрещается прохождение нескольких запросов к сервису ППО, все повторные запросы будут ожидать появления ответа в кэше, либо таймаут блокировки запроса к странице.
- `proxy_cache_use_stale` - параметр определяет, в каких случаях можно использовать устаревший закэшированный ответ;

– `add_header: "X-Cache-Status $upstream_cache_status"` - директива добавляет HTTP-заголовок, содержащий статус кэширования.

Например:

```
nginx_location_dashboard:
    path: "~ /v1/dashboards/[^/]+$"
    proxy_cache: "proxy_cache"
    proxy_cache_valid: "200 {{ cache_interval_dynamic }}"
    proxy_cache_lock: "on"
    proxy_cache_use_stale: "updating"
    add_header: "X-Cache-Status $upstream_cache_status"
```

4.7.6. 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 ГИС, 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 12).

Таблица 12

Параметр	Значение (для ГИС 1-го класса)
Конфигурационный файл ПБ: <code>/var/ocs/auth/config.yml</code>	
Период времени неиспользования идентификатора (учетной записи) пользователя, через которое происходит его блокирование: <code>config.maxAccountInactivityPeriod</code>	не более 45 дней <code>maxAccountInactivityPeriod: 1080h</code>
Минимальная длина пароля: <code>config.passwordSettings.minLength</code>	не менее 8 символов <code>config.passwordSettings.minLength: 8</code>

Параметр	Значение (для ГИС 1-го класса)
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: config.passwordHistoryDepth	passwordHistoryDepth: 3
Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки: config.failedLoginTries	не более 3 failedLoginTries: 3
Время блокировки учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации: config.failedLoginBlockTime	не менее 15 минут failedLoginBlockTime: "15m"
Количество одновременных сессий для привилегированных учетных записей: config.privilegedSessionsLimit	не более 2-х privilegedSessionsLimit: 2
Время бездействия (неактивности) пользователя, через которое осуществляется завершение сеанса пользователя: config.session.rememberFor	не более 5 минут rememberFor: 5m
Конфигурационные файлы ПМ и ПУ: /var/ocs/appstore/config.yml /var/ocs/emm/config.yml	

Параметр	Значение (для ГИС 1-го класса)
Время бездействия (неактивности) пользователя, через которое осуществляется завершение сеанса пользователя: config.session.rememberFor	не более 5 минут rememberFor: 5m

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.

4.7.7. Действия по реализации функций безопасности среды функционирования ППО

4.7.7.1. 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).

4.7.7.2. 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, остальной трафик должен быть запрещен. Перечень внешних портов ППО в зависимости от варианта настройки приведен в таблице (Таблица 13).

Таблица 13

Номер порта (протокол)	Описание	Конфигурационный файл, в котором задается порт	Тип порта ¹¹
Сервисы ППО «Аврора Центр»			
10000 - 10500 (tcp)	Порты сервисов ППО	shared_roles/systemd-deploy/templates/systemd-supPLICANT.sh.j2 /usr/bin/systemd-supPLICANT.sh	внутренний
Nginx			
80 (tcp)	Служит для взаимодействия сервисов ППО друг с другом и используется в том случае, когда осуществляется разделение трафика по basepath (url-адресам)	shared_roles/consul-template/defaults/main.yml	внутренний
8009 (tcp)	Балансировщик микросервисов (Nginx Web Server). Используется в том случае, когда осуществляется разделение трафика по basepath (url-адресам)	shared_roles/consul-template/templates/ocs.conf.ctmpl.j2 /etc/consul-template/templates/ocs.conf.ctmpl	внешний

¹¹ Типы портов:

1. Внешние - доступ к данному типу портов осуществляется из-за пределов контролируемой зоны. Например, запросы от пользователей с ролью Пользователь Аврора Маркет. Доступ к данным портам имеет нарушитель;
2. Внутренние - доступ к данному типу портов может осуществляться только из контролируемой зоны. Данные порты используются для взаимодействия: между сервисами ППО, сервисов ППО с компонентами среды функционирования ППО, компонентами среды функционирования ППО, привилегированных пользователей с ППО.

Номер порта (протокол)	Описание	Конфигурационный файл, в котором задается порт	Тип порта ¹¹
8011 (tcp)	АММ admin API gateway (Консоль администратора ПУ)	config/subsystems/emm/vars/services.yml	внешний или внутренний
8012 (tcp)	АММ device API gateway (API для взаимодействия с МП «Аврора Центр»)	config/subsystems/emm/vars/services.yml	внешний
8014 (tcp)	Aurora market development API gateway (Консоль разработчика ПМ)	config/subsystems/appstore/vars/services.yml	внешний
8015 (tcp)	Aurora market admin API gateway (Консоль администратора ПМ)	config/subsystems/appstore/vars/services.yml	внешний или внутренний
8016 (tcp)	Aurora market client API gateway (API для взаимодействия с МП «Аврора Маркет»)	config/subsystems/appstore/vars/services.yml	внешний
8018 (tcp)	Auth public API gateway (интерфейс ППО для идентификации и аутентификации пользователей)	config/subsystems/auth/vars/services.yml	внешний
8019 (tcp)	Auth admin API gateway (Консоль администратора ПБ)	config/subsystems/auth/vars/services.yml	внутренний
8022 (tcp)	Package repository admin API gateway (API для взаимодействия с ПУСП, только для взаимодействия ПУ с ПУСП)	config/subsystems/pkgrepo/vars/services.yml	внутренний

Номер порта (протокол)	Описание	Конфигурационный файл, в котором задается порт	Тип порта ¹¹
8023 (tcp)	Package repository device API (API для взаимодействия МП «Аврора Центр» с ПУСП)	config/subsystems/pkgrepo/vars/services.yml	внутренний
8030 (tcp)	Файловый сервер ПУСП	config/subsystems/pkgrepo/vars/ocs-pkgrepo-nginx-static.yml	внешний
СУБД PostgreSQL			
5432 (tcp)	СУБД PostgreSQL	shared_roles/postgresql/defaults/main.yml	внутренний
СУБД Redis			
6379 (tcp)	redis-server	shared_roles/redis/defaults/main.yml	внутренний
26379 (tcp)	redis-sentinel	shared_roles/redis/defaults/main.yml	внутренний
Consul			
8300 (tcp)	https://www.consul.io/docs/install/ports		внутреннее
8301 (tcp/udp)	https://www.consul.io/docs/install/ports		внутренний
8302 (tcp/udp)	https://www.consul.io/docs/install/ports		внутренний
8600 (tcp/udp)	https://www.consul.io/docs/install/ports	shared_roles/consul/defaults/main.yml	внутренний
8500 (tcp)	https://www.consul.io/docs/install/ports	shared_roles/consul/defaults/main.yml	внутренний
Nats Streaming Server			
4222 (tcp)	nats_port	shared_roles/nats-streaming-server/defaults/main.yml	внутренний
6222 (tcp)	nats_cluster_port	shared_roles/nats-streaming-server/defaults/main.yml	внутренний

Номер порта (протокол)	Описание	Конфигурационный файл, в котором задается порт	Тип порта ¹¹
8222 (tcp)	nats_monitoring_port	shared_roles/nats-streaming-server/defaults/main.yml	внутренний
Dnsmasq			
53	dnsmasq		внутренний
Операционная система			
22	Порт SSH. Используется для развертывания и администрирования ППО. Внимание: возможность использования данного порта определяется документацией СЗИ от НСД.		внутренний

Рекомендуется запретить доступ к ППО привилегированных пользователей из-за пределов контролируемой зоны, запретив доступ к Консоли администратора ПБ. Также при необходимости можно запретить доступ к остальным веб-консолям. Для этого, в зависимости от варианта настройки ППО, разрешить трафик только на требуемых портах, либо только по требуемым url-адресам в соответствии с таблицей (Таблица 11)

4.7.7.3. Настройка ОС

В целях затруднения возможностей сбора информации о системе, необходимо исключить метки времени из заголовков TCP пакетов. Для этого необходимо выполнить следующие действия:

4.7.7.4. В конфигурационный файл `/etc/sysctl.conf` добавить строку:

```
net.ipv4.tcp_timestamps = 0
```

4.7.7.5. Применить конфигурацию, выполнив команду:

```
sysctl -p /etc/sysctl.conf
```

4.7.7.6. Проверить корректность конфигурации, выполнив команду:

```
sysctl -a | grep net.ipv4.tcp_timestamps
```

Если настройки сделаны правильно, то должно быть выведено значение:

```
net.ipv4.tcp_timestamps = 0
```

4.7.8. Самостоятельная установка необходимых пакетов на сервера приложений и сервера БД

Для установки необходимых пакетов на сервера приложений и сервера БД необходимо выполнить следующие действия:

4.7.8.1. Получить список необходимых пакетов

Перечень необходимых пакетов, которые должны быть установлены на сервера приложений и сервера БД задан в файле `play-managed-node-prerequisites.yml`, находящемся в каталоге со сценариями установки ППО. Данный файл имеет следующую структуру:

```
- name: install requirements to <операционная система>
  - name: install os packages on db node
    loop:
      <перечень пакетов сервера БД>
  - name: install os packages on app node
    loop:
      <перечень пакетов сервера приложений>
```

В секции `name: install requirements to <операционная система>` задается перечень пакетов для указанной ОС. Данная секция содержит две подсекции, в которых задается перечень пакетов для сервера приложений и сервера БД.

В подсекции `name: install os packages on db node` задается перечень пакетов для сервера БД.

В подсекции `name: install os packages on app node` задается перечень пакетов для сервера приложений.

Пример перечня пакетов, для сервера приложений и сервера БД, функционирующих под управлением ОС CentOS 7:

```
tasks:
  - name: install requirements to CentOS7
    block:
      - debug:
          msg: install requirements to CentOS7

      - name: install os packages on db node
        package:
          name: "{{ item }}"
          state: present
        loop:
          - epel-release
          - jq
          - unzip
          - perl-libs
          - libxslt
          - postgresql-libs
          - libicu
          - python-psycopg2
        when: node_type == "db" or node_type == "all"

      - name: install os packages on app node
        package:
          name: "{{ item }}"
          state: present
        loop:
          - net-tools
          - epel-release
          - jq
          - unzip
          - perl-libs
          - libxslt
          - postgresql-libs
          - libicu
          - dnsmasq
```

```
        - bind-utils
        when: node_type == "app" or node_type == "all"
        when: ansible_distribution == "CentOS" and
ansible_distribution_major_version == "7"
```

4.7.8.2. Установить пакеты

Установка пакетов осуществляется в соответствии с документацией на ОС.

4.8. Проверка корректности установки и функционирования ППО

4.8.1. Общие сведения

Для проверки корректности установки и функционирования ППО, а также среды функционирования ППО в состав сценариев установки включена утилита для формирования диагностического отчета.

Для формирования диагностического отчета необходимо перейти в каталог со сценариями установки (каталог: `install-<версия ППО>/install-<вариант поставки>`) 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 `report.html`.

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

- общая информация о статусе сервисов ППО;
- общая информация о статусе компонентов среды функционирования;
- разделы, содержащие детальную информацию об отдельных сервисах ППО

и компонентах среды функционирования.

4.8.2. Описание параметров диагностического отчета

4.8.2.1. Раздел «Disk Space»

Информация о полном и доступном объеме дискового пространства для ППО приведена на рисунке (Рисунок 41).

Disk Space			
Mount point	Size total, MiB	Size available, MiB	Availability, %
/boot	1014.00	864.34	85.24
/	51175.00	46308.92	90.49
/home	45729.66	43128.35	94.31

Рисунок 41

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 14).

Таблица 14

Название столбца	Описание	Возможные значения (примеры значений)
Mount points	Каталог, к которому монтируется файловое хранилище (точка монтирования)	Путь к каталогу, например: /home.
Size total, MiB	Размер файлового хранилища, примонтированного к заданному каталогу	Объем физической памяти в Мб, например: 45729,66
Size available, MiB	Объем свободного места в файловом хранилище, примонтированного к заданному каталогу	Объем физической памяти в Мб, например: 43128,35
Availability, %	Объем свободного места в файловом хранилище в процентном соотношении (к полному объему)	От 0 до 100, например: 94.31

В случае если объем свободного места в менее 15%, то поле закрашивается красным цветом

4.8.2.2. Раздел «Systemd Unit Status»

В данном разделе приведена общая информация о статусе сервисов ППО и компонентов среды функционирования и состоит из следующих подразделов:

4.8.2.2.1 OCS Targets

Информация об автозапуске сервисов ППО (наличии конфигурационных файлов запуска групп сервисов *.target в автозапуске) приведена на рисунке (Рисунок 42).

Systemd Unit Status	
Service name	Status
OCS Targets	
ocs-appstore-admin-api-gw.target	enabled
ocs-appstore-adminconsole-ui.target	enabled
ocs-appstore-applications-api.target	enabled
ocs-appstore-client-api-gw.target	enabled
ocs-appstore-dev-api-gw.target	enabled
ocs-appstore-devconsole-ui.target	enabled
ocs-appstore-egress-api-gw.target	enabled
ocs-appstore-settings-api.target	enabled
ocs-appstore.target	enabled

Рисунок 42

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 15).

Таблица 15

Название столбца	Описание	Возможные значения (примеры значений)
Service name	Имя конфигурационного файла запуска группы сервисов	Возможные значения определяются перечнем сервисов ППО и имеют следующий формат <имя группы сервисов>.target, например: ocs-appstore-admin-api-gw.target.
Status	Информация о присутствии конфигурационного файла запуска группы сервисов в автозапуске	enabled - присутствует в автозапуске disabled - отсутствует в автозапуске

4.8.2.2.2 OCS Services

Информация о статусе сервисов ППО приведена на рисунке (Рисунок 43).

OCS Services	
ocs-appstore-admin-api-gw@0.service	active (running)
ocs-appstore-adminconsole-ui@0.service	active (running)
ocs-appstore-applications-api@0.service	active (running)
ocs-appstore-client-api-gw@0.service	active (running)
ocs-appstore-dev-api-gw@0.service	active (running)
ocs-appstore-devconsole-ui@0.service	active (running)
ocs-appstore-egress-api-gw@0.service	active (running)
ocs-appstore-settings-api@0.service	active (running)
ocs-auth-accounts-applications-api@0.service	active (running)

Рисунок 43

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 16).

Таблица 16

Название столбца	Описание	Возможные значения (примеры значений)
Service name	Название сервиса ППО	Возможные значения определяются перечнем сервисов ППО и имеют следующий формат <имя группы сервисов>@<номер экземпляра сервиса в группе>.service, например: ocs-appstore-admin-api-gw@0.service.
Status	Информация о статусе сервиса	active (running) - сервис запущен и выполняется; activating - сервис запускается; deactivating - сервис выключается; inactive - сервис выключен; failed - при запуске сервиса произошла ошибка

4.8.2.2.3 Mandatory services

Информация о статусе сервисов – компонентов среды функционирования приведена на рисунке (Рисунок 44).

Mandatory services	
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 44

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 17).

Таблица 17

Название столбца	Описание	Возможные значения (примеры значений)
Service name	Название сервиса компонента среды функционирования	Возможные значения имеют следующий формат <имя сервиса>.service и определяются Разработчиком. Перечень возможных значений: consul-template.service consul.service nats-streaming-server.service nginx.service postgresql-11.service postgresql.service
Status	Информация о статусе сервиса	active (running) - сервис запущен и выполняется; activating - сервис запускается; deactivating - сервис выключается; inactive - сервис выключен; failed - при запуске сервиса произошла ошибка; enabled - сервис присутствует в автозапуске; disabled - сервис отсутствует в автозапуске; missed - компонент отсутствует

4.8.2.3. Раздел «OIDC Clients»

Информация об OIDC-клиентах приведена на рисунке (Рисунок 45).

OIDC Clients	
auth-admin-console	
Redirect URI:	<code>http://ocs-app.local:8009/auth/admin/</code>
Audience:	<code>ocs-auth-admin-api-gw</code>
Scopes:	<code>[openid] [offline] [account:read] [account:changePassword] [account:update] [account:delete] [audit:read] [session:read] [service:read]</code>
aps-admin-console	
Redirect URI:	<code>http://ocs-app.local:8009/appstore/admin/</code>
Audience:	<code>ocs-appstore-admin-api-gw</code>
Scopes:	<code>[openid] [offline] [account:read] [application:read] [dashboard:read] [dashboard:update] [release:read] [release:update] [icon:read] [category:read] [customerKeyPair:read] [customerKeyPair:update] [service:read]</code>

Рисунок 45

По каждому OIDC-клиенту приведена следующая информация:

- идентификатор OIDC-клиента (например, `emm-admin-console`);
- в поле «Scope» приведен перечень действий (прав) доступных OIDC-клиенту;
- в поле «Return/redirect URI» находится список URI для автоматического перехода для авторизованного и неавторизованного пользователя;
- в поле «Audience» указано название шлюза доступа, который и является OIDC-клиентом.

4.8.2.4. Раздел «Consul Services Registration»

На рисунке (Рисунок 46) отображается пример статуса регистрации сервисов в системе обнаружения сервисов (Consul).

Consul Services Registration		
Service name	Code	Status
<code>ocs-appstore-admin-api-gw</code>	200	passing
<code>ocs-appstore-client-api-gw</code>	200	passing
<code>ocs-appstore-dev-api-gw</code>	200	passing
<code>ocs-auth-admin-api-gw</code>	200	passing
<code>ocs-auth-public-api-gw</code>	200	passing
<code>ocs-emm-admin-api-gw</code>	200	passing
<code>ocs-emm-device-api-gw</code>	200	passing
<code>ocs-pkgrepo-admin-api-gw</code>	200	passing
<code>ocs-pkgrepo-device-api-gw</code>	200	passing

Рисунок 46

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 18).

Таблица 18

Название столбца	Описание	Возможные значения (примеры значений)
Service name	Название сервиса ППО	Возможные значения определяются перечнем сервисов ППО
Code	Код http-ответа	Возможные значения определяются протоколом HTTP
Status	Информация о статусе регистрации сервиса в системе обнаружения сервисов (Consul)	Возможные значения определяются Consul. Статус «passing» означает, что проверка пройдена успешно

4.8.2.5. Раздел «Consul Cluster Endpoints Availability»

Проверка доступности интерфейсных функций системы обнаружения сервисов (Consul) представлена на рисунке (Рисунок 47).

Consul Cluster Endpoints Availability	
Node:Port	Availability
inp1int03.omplcloud:8300	OPENED
inp1int03.omplcloud:8301	OPENED
inp1int03.omplcloud:8302	OPENED
inp1int03.omplcloud:8500	OPENED
inp1int02.omplcloud:8300	OPENED
inp1int02.omplcloud:8301	OPENED
inp1int02.omplcloud:8302	OPENED
inp1int02.omplcloud:8500	OPENED

Рисунок 47

Перечень интерфейсных функций Consul приведен в документации на Consul (<https://www.consul.io/docs/install/ports>). Информация по доступности интерфейсных функций Consul предоставляется только в случае кластерной (многонодовой) конфигурации.

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 19).

Таблица 19

Название столбца	Описание	Возможные значения (примеры значений)
Node:Port	Адрес функции	Адрес функции представлен в следующем формате: <имя хоста>:<порт>. Проверка выполняется только для функций доступных на следующих портах: 8300, 8301, 8302, 8500. Например: inp1int03.ompccloud:8300
Availability	Статус доступности функции	В случае доступности функции принимает значение «OPENED». В ином случае выводится код ошибки и сообщение, определяемое Consul

4.8.2.6. Раздел «Consul Service Health Check»

Статус регистрации сервисов ППО в системе обнаружения сервисов Consul представлен на рисунке (Рисунок 48).

Consul Service Health Check		
service_location		
ocs-appstore-admin-api-gw	200	http://ocs-app.local:80/ocs-appstore-admin-api-gw/admin/health/ocs-appstore-admin-api-gw
ocs-appstore-adminconsole-ui	200	http://ocs-app.local:80/ocs-appstore-adminconsole-ui/admin/health/ocs-appstore-adminconsole-ui
ocs-appstore-applications-api	200	http://ocs-app.local:80/ocs-appstore-applications-api/admin/health/ocs-appstore-applications-api
ocs-appstore-client-api-gw	200	http://ocs-app.local:80/ocs-appstore-client-api-gw/admin/health/ocs-appstore-client-api-gw
ocs-appstore-dev-api-gw	200	http://ocs-app.local:80/ocs-appstore-dev-api-gw/admin/health/ocs-appstore-dev-api-gw
ocs-appstore-devconsole-ui	200	http://ocs-app.local:80/ocs-appstore-devconsole-ui/admin/health/ocs-appstore-devconsole-ui
ocs-appstore-egress-api-gw	200	http://ocs-app.local:80/ocs-appstore-egress-api-gw/admin/health/ocs-appstore-egress-api-gw

Рисунок 48

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 20).

Таблица 20

Название столбца	Описание	Возможные значения (примеры значений)
Первый столбец	Название сервиса ППО	Возможные значения определяются перечнем сервисов ППО. Зеленый цвет названия сервиса говорит о том, что сервис функционирует в штатном режиме
Второй столбец	Код http-ответа	Возможные значения определяются протоколом HTTP
Третий столбец	url-адрес функции (endpoint) сервиса «healthcheck»	Содержит url-адрес функции «healthcheck», которая возвращает информацию о статусе сервиса

Перечисленные заголовки "service_location", "expose_location", "service_vhost", "expose_port" – это режимы работы consul-template.

4.8.2.7. Раздел «Cluster Nodes Reachability»

Результат проверки доступности серверов (нод) кластера представлен на рисунке (Рисунок 49).

Cluster Nodes Reachability	
Node	Reachable
ocs-app.local	OK

Рисунок 49

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 21).

Таблица 21

Название столбца	Описание	Возможные значения (примеры значений)
Node	Адрес сервера (хоста)	Определяется доменными именами хостов
Reachable	Информация о доступности сервера	Может принимать значения: «OK» (в случае доступности) или содержать сообщение об ошибке, которое вернет утилита ping

4.8.2.8. Раздел «Nginx Service Proxy»

Информация о проверке конфигурации балансировщика микросервисов Nginx Web Server для каждого сервиса ППО приведена на рисунке (Рисунок 50).

Nginx Service Proxy		
Service name	Upstreams	Virtual server
ocs-appstore-settings-api	1	OK
ocs-appstore-adminconsole-ui	1	OK
ocs-pkgrepo-egress-api-gw	1	OK
ocs-auth-idp-ui	1	OK
ocs-pkgrepo-pkg-repo-api	1	OK
ocs-auth-admin-api-gw	1	OK
ocs-auth-server-public	1	OK

Рисунок 50

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 22).

Таблица 22

Название столбца	Описание	Возможные значения (примеры значений)
Service name	Название сервиса ППО	Возможные значения определяются перечнем сервисов ППО
Upstreams	Количество экземпляров сервиса, заданных в конфигурационном файле Nginx	Целочисленные значения от 1 до n
Virtual server	Информация о наличии секции «server» для указанного сервиса ППО в конфигурационном файле Nginx. В данной секции заданы настройки «виртуального» сервиса ППО, который осуществляет перенаправление (проксирование) http-запросов на «реальные» экземпляры сервиса	«OK» - секция server присутствует «No server block found!» - секция отсутствует

4.8.2.9. Раздел «Filestorage Configuration»

Информация о конфигурации файловых хранилищ ПМ и ПООС представлена на рисунке (Рисунок 51).



Рисунок 51

Настройка «Filestorage location» содержит путь к каталогу и его статус.

В настройке «Configuration file» указан конфигурационный файл, в котором задан путь к файловому хранилищу.

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 резервную копию каталога «install-<версия ППО>/install-<вариант поставки>».

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 ПООС (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 пакетов ОС ПООС.

Для этого необходимо создать резервную копию каталога `/ocs/pkgrepo` на Сервере приложений ПООС, 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 также 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. ОПИСАНИЕ ОБНОВЛЕНИЯ 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 разделом 5.

6.2. Скопировать на управляющую ПЭВМ архив с новой версией ППО и распаковать его в соответствии с пп. 4.3.2.3 - 4.3.2.7.

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

Для этого необходимо перейти в каталог со сценариями установки новой версии ППО (каталог: `install-<новая версия ППО>/install-<вариант поставки>`) и выполнить команду:

```
ansible-playbook -i inventories/hosts.yml -u <имя пользователя>
release_upgrade/play-upgrade_to_release_2.5.0.yml -vv --diff
```

6.4. При обновлении СУБД PostgreSQL 11/12 до новой старшей версии¹² (major version), необходимо удалить СУБД (без удаления данных) выполнив команду:

```
ansible-playbook play-postgresql.yml -i "inventories/hosts.yml" -
vv --diff -u <имя пользователя> --extra-var "flush_all=true
skip_subsystems=true"
```

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

¹² Согласно спецификации SemVer 2.0.0.

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                1dd681d509a1c5e3aa1882aeb53ebeb504faeecf
nginx                 master                420ad871296855752ed3bb31e9958ecf0d68ad52
postgres             master                e7d2e67da97955d2440723a58dfb4510db3907b4
nats-streaming-server master                fb4a9b55308f29c8bcda3fc1804da92db84e90d6
server-provision-scripts master                cdcba455e074dd6bc2bcc519ebd842d36c3a29726
redis                 master                f4c6c300e7f9533652bb02008575ff009f8ef985
openssl               master                7ac23c1d67a6671e20785a9e1cc84d7d8b46103d
cert-distr-infra     branch                1ac040b2fff85ce3c9fbca42a914b34679303acc
```

6.6. Установить ППО в соответствии с подразделом 4.4.

7. УПРАВЛЕНИЕ СЕРВИСАМИ И НАСТРОЙКАМИ СЕРВИСОВ (ПОДСИСТЕМ) ППО

7.1. Управление сервисами ППО

Управление сервисами ППО заключается в их установке, запуске, остановке, перезапуске, изменении настроек и осуществляется с помощью скрипта `deploy-ac.sh` из каталога `install-<версия ППО>`, созданного на этапе развертывания управляющей ПЭВМ п. 4.3.2.

Формат команды управления сервисами имеет следующий вид:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh <параметры>
```

Описание параметров команды управления:

1) <имя пользователя>

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

2) `-s, --subsystems`

Данный параметр задает подсистему, для которой будет выполнена команда управления. Параметр может принимать следующие значения:

- `auth` (для ПБ);
- `appstore` (для ПМ);
- `emm` (для ПУ);
- `pkgrepo` (для ПООС).

В данном параметре может задаваться список подсистем, например:

```
--subsystems auth,appstore,emm,pkgrepo
```

По умолчанию (если параметр не задан) параметр имеет значение:

```
--subsystems auth,appstore,emm,pkgrepo
```


3) -a, --apps

Данный параметр задает перечень сервисов, для которых будет выполнена команда управления. Например:

```
--apps ocs-auth-adminconsole-ui,ocs-appstore-adminconsole-ui
```

Если необходимо выполнить команду сразу для всех сервисов подсистемы, то необходимо перечислить через запятую все сервисы подсистемы, либо задать значение параметра:

```
--apps all
```

По умолчанию (если параметр не задан), то параметр имеет значение «all».

В случае, если заданные в параметре «--apps» сервисы не соответствуют заданным в параметре «--subsystems» подсистемам, то управляющая команда к таким сервисам применена не будет. При этом управление шлюзами доступа (сервисами шлюзов доступа) осуществляется в рамках той подсистемы, для которой они предназначены. Состав подсистем приведен в таблице (Таблица 23).

Таблица 23

Значение параметра «--subsystems»	Сервисы (значение параметра «--apps»)
	ПБ
auth	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

Значение параметра «--subsystems»	Сервисы (значение параметра «--apps»)
ПМ	
appstore	ocs-appstore-applications-api
	ocs-appstore-settings-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	
emm	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
	ocs-emm-users-api
	ocs-emm-journal-api
	ocs-emm-jobs-api
	ocs-emm-adminconsole-ui
	ocs-emm-admin-api-gw
	ocs-emm-device-api-gw
	ocs-emm-egress-api-gw

Значение параметра «--subsystems»	Сервисы (значение параметра «--apps»)
ПООС	
pkgrepo	ocs-pkgrepo-pkg-repo-api
	ocs-pkgrepo-device-api-gw
	ocs-pkgrepo-admin-api-gw
	ocs-pkgrepo-egress-api-gw

4) -A, --action

Данный параметр задает действие, которое необходимо выполнить. Перечень допустимых действий и соответствующие им значения параметра приведены в таблице (Таблица 24).

Таблица 24

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

По умолчанию (если параметр не задан) параметр имеет значение «deploy».

5) -c, --clients

Данный параметр задает OIDC клиентов, для которых будет выполнена команда управления. Например:

```
--clients auth-admin-console, aps-admin-console
```

Если необходимо выполнить команду сразу для всех OIDC клиентов, то необходимо перечислить через запятую все OIDC клиенты, либо задать значение параметра:

```
--clients all
```

По умолчанию (если параметр не задан) параметр имеет значение «all».

6) -d, --database

Данный параметр задает СУБД, которая установлена на сервере БД. Параметр может принимать следующие значения:

- 11 (для СУБД PostgreSQL 11);
- 12 (для СУБД PostgreSQL 12);
- 11-pro (для СУБД Postgres Pro 11).

Например:

```
--database 11
```

По умолчанию (если параметр не задан) параметр имеет значение «11».

7) --help

Вывод справочной информации.

Примеры команд управления:

1) остановка всех сервисов ПМ:

```
ANSIBLE_USER=omp ./deploy-ac.sh --action stop
```

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

ПМ:

```
ANSIBLE_USER=omp ./deploy-ac.sh --apps ocs-appstore-applications-api,ocs-appstore-adminconsole --action start
```

3) получение справочной информации:

```
./deploy-ac.sh --help
```

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 приведено в подразделе 10.3.

7.2.1.2. Переустановить конфигурационные файлы с помощью следующей команды:

– ПБ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems auth -  
-action config
```

– ПМ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems  
appstore --action config
```

– ПУ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems emm --  
action config
```

– ПООС:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems  
pkgrepo --action config
```

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 приведено в разделе 10.

7.2.2.2. Перезапустить требуемые сервисы с помощью следующей команды:

– ПБ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems auth -  
-apps <перечень сервисов ПБ> --action restart
```

– ПМ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems  
appstore --apps <перечень сервисов ПМ> --action restart
```

– ПУ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems emm --  
apps <перечень сервисов ПУ> --action restart
```

– ПООС:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems  
pkgsrepo --apps <перечень сервисов ПООС> --action restart
```

8. ОПИСАНИЕ УДАЛЕНИЯ ППО

Для удаления сервисов ППО необходимо выполнить следующие действия:

8.1. Перейти в каталог со сценариями установки ППО;

8.2. Удалить сервисы ППО с помощью следующих команд:

– ПБ:

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

– ПМ:

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

– ПУ:

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

– ПООС:

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

8.3. Удалить компоненты среды функционирования ППО с помощью следующих команд:

– dnsmasq:

```
ansible-playbook play-dnsmasq.yml -i "inventories/hosts.yml" -vv -  
-diff -u <имя пользователя> --extra-vars "flush_all=true  
skip_subsystems=true"
```

– nginx:

```
ansible-playbook play-nginx.yml -i "inventories/hosts.yml" -vv --  
diff -u <имя пользователя> --extra-vars "flush_all=true  
skip_subsystems=true"
```

– consul:

```
ansible-playbook play-consul.yml -i "inventories/hosts.yml" -vv --diff -u <ИМЯ ПОЛЬЗОВАТЕЛЯ> --extra-vars "flush_all=true skip_subsystems=true"
```

– consul template:

```
ansible-playbook play-consul-template.yml -i "inventories/hosts.yml" -vv --diff -u <ИМЯ ПОЛЬЗОВАТЕЛЯ> --extra-vars "flush_all=true skip_subsystems=true"
```

– nats streaming server:

```
ansible-playbook play-nats-streaming-server.yml -i "inventories/hosts.yml" -vv --diff -u <ИМЯ ПОЛЬЗОВАТЕЛЯ> --extra-vars "flush_all=true skip_subsystems=true"
```

– redis:

```
ansible-playbook play-redis.yml -i "inventories/hosts.yml" -vv --diff -u <ИМЯ ПОЛЬЗОВАТЕЛЯ> --extra-vars "flush_all=true skip_subsystems=true"
```

– postgresql (без удаления данных):

```
ansible-playbook play-postgresql.yml -i "inventories/hosts.yml" -vv --diff -u <ИМЯ ПОЛЬЗОВАТЕЛЯ> --extra-vars "flush_all=true skip_subsystems=true"
```

– postgresql (с удалением данных):

```
ansible-playbook play-postgresql.yml -i "inventories/hosts.yml" -vv --diff -u <ИМЯ ПОЛЬЗОВАТЕЛЯ> --extra-vars "flush_all=true skip_subsystems=true pg_uninstall_delete_data=true"
```


9. КОНФИГУРАЦИОННЫЕ ФАЙЛЫ СЦЕНАРИЕВ УСТАНОВКИ СРЕДЫ ФУНКЦИОНИРОВАНИЯ

9.1. Конфигурационные файлы сценариев установки среды функционирования

9.1.1. 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 25).

Таблица 25

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

9.1.2. Настройки сценариев установки среды функционирования в конфигурационном файле `config/vars/_vars.yml`

В данном конфигурационном файле задаются настройки следующих компонентов среды функционирования ППО: Nats Streaming Server, Consul, СУБД Redis и СУБД PostgreSQL.

Описание секций конфигурационного файла, относящихся к сценариям установки среды функционирования, приведено в п. 10.3.2, 10.3.3, 10.3.4, 10.3.5.

9.1.3. Настройки сценариев установки среды функционирования в конфигурационном файле `config/vars/_vars_infra.yml`

В данном конфигурационном файле задаются настройки СУБД PostgreSQL.

Описание секций конфигурационного файла приведено в таблице (Таблица 26).

Таблица 26

Секция конфигурационного файла	Описание
<code>pg_settings.listen_addresses</code>	IP-адреса сетевых интерфейсов, по которым сервер будет принимать подключения
<code>pg_settings.timezone</code>	Часовой пояс для вывода и ввода значений времени
<code>pg_settings.log_timezone</code>	Часовой пояс для штампов времени при записи в журнал сервера
<code>pg_hba_settings.type</code>	Тип подключения
<code>pg_hba_settings.name</code>	Имя пользователя
<code>pg_hba_settings.database</code>	Имя БД
<code>pg_hba_settings.address</code>	IP-адрес хоста или IP-адрес подсети

Секция конфигурационного файла	Описание
pg_hba_settings.method	Метод аутентификации
pg_replication_user.type	Тип подключения пользователя с ролью «replication»
pg_replication_user.name	Имя пользователя с ролью «replication»
pg_replication_user.database	Имя БД
pg_replication_user.address	IP-адрес хоста или IP-адрес подсети
pg_replication_user.method	Метод аутентификации пользователя с ролью «replication»
pg_replication_user.password	Пароль пользователя с ролью «replication»

С подробным описанием параметров и возможными значениями параметров можно ознакомиться в документации на СУБД PostgreSQL или СУБД Postgres Pro

Конфигурационный файл `config/vars/_vars_infra.yml` может иметь следующий

ВИД:

```
pg_settings: # postgresql.conf parameters
  listen_addresses: "0.0.0.0"
  timezone: "UTC"
  log_timezone: "UTC"

pg_hba_settings: # pg_hba.conf settings
- type: local ## Unix-socket access
  name: all
  database: all
  method: trust
- type: host ## Localhost IPv4 access
  name: all
  database: all
  address: 127.0.0.1/32
  method: trust
- type: host ## DB hosts
```

```
    name: all
    database: all
    address: "{{ groups['postgresql'] }}"
    method: md5
- type: host ## Application hosts
    name: all
    database: all
    address: "{{ groups['app'] }}"
    method: md5
- type: host # Gitlab CI vbox-testing
    name: all
    database: all
    address: 172.17.0.0/16
    method: md5
- type: host # TODO: What's it local zone for?
    name: all
    database: all
    address: 172.28.0.0/16
    method: md5

pg_replication_user: # Replication access configuration
    type: host
    name: replication
    database: replication
    address: "{{ ansible_default_ipv4.network }}/24"
    method: md5
    password: 123Qwe!@#
```

10. КОНФИГУРАЦИОННЫЕ ФАЙЛЫ ППО (СЦЕНАРИЕВ УСТАНОВКИ ППО)

10.1. Конфигурационные файлы ППО (общая информация)

ППО содержит следующие типы конфигурационных файлов:

- конфигурационные файлы подсистем ППО (config.yml);
- конфигурационные файлы сервисов (модулей) ППО (<название сервиса>.yml).

В конфигурационных файлах подсистем содержатся настройки подсистем ППО. Также в конфигурационные файлы подсистем вынесены (могут быть вынесены) отдельные настройки сервисов ППО, которые может изменять администратор ППО. В данном случае в конфигурационном файле содержится секция с именем сервиса. Например, секция для сервиса `ocs-auth-accounts-users-api` выглядит следующим образом:

```
#-----  
-----  
# Parameters for user accounts  
#-----  
-----  
ocs-auth-accounts-users-api:  
  
##  
# The number of recently used passwords,  
# which system will store for forbidding use it for new password  
creating.  
##  
passwordHistoryDepth: 3  
  
##  
# Maximum inactivity period 45 days.
```

```
# If account not use system during this time, account will be
blocked.
# Must be greater or equal to OIDC refresh token lifetime.
##
maxAccountInactivityPeriod: "1080h"
```

Описание параметров конфигурационных файлов подсистем ППО приведено в п. 10.3.2, 10.3.3, 10.3.4, 10.3.5.

Конфигурационные файлы подсистем ППО располагаются по следующему пути:

```
/var/ocs/<название подсистемы>/config.yml
```

Например, конфигурационный файл ПБ:

```
/var/ocs/auth/config.yml
```

Конфигурационные файлы сервисов содержат настройки сервисов ППО и располагаются по следующему пути:

```
/var/ocs/<название подсистемы>/<название сервиса>/<название сервиса>.yml
```

Например, конфигурационный файл сервиса ocs-auth-idp-api ПБ:

```
/var/ocs/auth/ocs-auth-idp-api/ocs-auth-idp-api.yml
```

Описание параметров конфигурационных файлов сервисов приведено в самих конфигурационных файлах в виде комментариев.

ВНИМАНИЕ! Редактировать конфигурационные файлы сервисов ППО не рекомендуется.

10.2. Конфигурационные файлы сценариев установки ППО (общая информация)

Сценарии установки ППО содержат следующие типы конфигурационных файлов:

- конфигурационный файл inventories/hosts.yml;
- конфигурационные файлы config/vars/_vars.yml;

- конфигурационные файлы подсистем `config/subsystems/<название подсистемы>/vars/_vars.yml`;
- шаблоны конфигурационных файлов подсистем ППО (`config.yml.j2`);
- шаблоны конфигурационные файлы сервисов (модулей) ППО (`<название сервиса>.yml.j2`).

10.2.1. Конфигурационный файл `inventories/hosts.yml`

Конфигурационный файл `inventories/hosts.yml` содержит адреса серверов (имена хостов), на которые установлены (будут установлены) компоненты среды функционирования ППО и подсистемы ППО.

Описание параметров конфигурационных файлов `inventories/hosts.yml` приведено в п. 9.1.1.

10.2.2. Общий конфигурационный файл сценариев установки `config/vars/_vars.yml`

Конфигурационный файл `config/vars/_vars.yml` является общим для всех подсистем и модулей ППО. В нем содержится полный перечень общих параметров, относящихся к подсистемам и модулям ППО.

Описание параметров конфигурационного файла `config/vars/_vars.yml` приведено в п. 10.3.2, 10.3.3, 10.3.4, 10.3.5.

10.2.3. Конфигурационные файлы сценариев установки для подсистем ППО (файлы: `config/subsystems/<название подсистемы>/vars/_vars.yml`)

Конфигурационные файлы `vars.yml` подсистем содержат параметры, относящиеся к конкретной подсистеме. Также данные файлы могут быть дополнены параметрами из общего конфигурационного файла, значения которых надо переопределить для заданной подсистемы.

Конфигурационные файлы `_vars.yml` в большей части содержат настройки взаимодействия подсистем с компонентами среды функционирования. Располагаются данные конфигурационные файлы в каталоге со сценариями установки по следующему пути:

```
config/subsystems/<название подсистемы>/vars/_vars.yml
```

Например, конфигурационный файл `vars.yml` для ПБ:

```
config/subsystems/auth/vars/_vars.yml
```

Описание параметров конфигурационных файлов `_vars.yml` приведено в п. 10.3.2, 10.3.3, 10.3.4, 10.3.5.

10.2.4. Шаблоны конфигурационных файлов подсистем ППО

На основе данных файлов в процессе установки ППО формируются конфигурационные файлы подсистем ППО. Значения параметров в шаблонах конфигурационных файлов подсистем ППО задаются администратором, а также сценариями установки на основе значений, заданных администратором в конфигурационных файлах `_vars.yml`.

Располагаются данные конфигурационные файлы в каталоге со сценариями установки по следующему пути:

```
config/subsystems/<название подсистемы>/config/services/config.yml.j2
```

Например, шаблон конфигурационного файла ПБ:

```
config/subsystems/auth/config/services/config.yml.j2
```

Описание параметров шаблонов конфигурационных файлов подсистем ППО приведено в п. 10.3.2, 10.3.3, 10.3.4, 10.3.5.

10.2.5. Шаблоны конфигурационных файлов сервисов ППО

На основе данных файлов в процессе установки ППО формируются конфигурационные файлы сервисов ППО.

Шаблоны конфигурационных файлов сервисов располагаются в каталоге со сценариями установки по следующему пути:

```
config/subsystems/<название подсистемы>/config/services/<название сервиса>/<название сервиса>.yml.j2
```

Например, шаблон конфигурационного файла сервиса ocs-auth-adminconsole-ui ПБ:

```
config/subsystems/auth/config/services/ocs-auth-adminconsole-ui/ocs-auth-adminconsole-ui.yml.j2
```

Описание параметров шаблонов конфигурационных файлов сервисов приведено в самих конфигурационных файлах в виде комментариев.

ВНИМАНИЕ! Редактировать шаблоны конфигурационных файлов сервисов ППО не рекомендуется.

10.2.6. Конфигурационные файлы окружений

Данные конфигурационные файлы включают:

- общий конфигурационный файл сценариев установки ППО для заданного окружения (файл: `config/environments/<название окружения>/vars/_vars.yml`);
- конфигурационные файлы сценариев установки подсистем ППО для заданного окружения (файлы в каталоге: `config/environments/<название окружения>/<название подсистемы>/vars/`).

В данных конфигурационных файлах переопределяются параметры общего конфигурационного файла сценариев установки ППО и конфигурационных файлов сценариев установки подсистем ППО.

Для того чтобы переопределить параметр, необходимо:

- скопировать параметр (включая секцию, в которую входит параметр) из общего конфигурационного файла сценариев установки ППО или конфигурационного файла сценариев установки подсистем ППО;
- вставить скопированное значение в аналогичный конфигурационный файл для заданного окружения;

– задать требуемое значение параметра.

10.2.7. Порядок работы с конфигурационными файлами сценариев установки

ППО

В целях оптимизации настройки ППО, а также отдельных подсистем ППО и модулей ППО была реализована следующая структура конфигурационных файлов сценариев установки ППО, приведенная в таблице (Таблица 27).

Таблица 27

Каталог (имя файла)	Описание	Порядок применения параметров (приоритет параметров)
config/vars/_vars.yml	Общий (для всех подсистем и модулей ППО) конфигурационный файл сценариев установки ППО. В нем содержится полный перечень общих параметров, относящихся к подсистемам и модулям ППО	1 (самый низкий приоритет)
config/subsystems/<название подсистемы>/vars/ Например, config/subsystems/auth/vars/	Конфигурационные файлы сценариев установки подсистем ППО. В них содержатся параметры, относящиеся к конкретной подсистеме. Также данные файлы могут быть дополнены параметрами из общего конфигурационного файла, значения которых надо переопределить для заданной подсистемы	2
config/environments/<название окружения>/vars/_vars.yml Например, config/environments/release/vars/_vars.yml	Общий конфигурационный файл сценариев установки ППО для заданного окружения. В нем могут содержаться параметрами из общего конфигурационного файла, значения которых надо переопределить для заданного окружения	3

<code>config/environments/<окружение>/<название подсистемы>/vars/</code> Например, <code>config/environments/release/auth/vars/</code>	Конфигурационные файлы сценариев установки подсистем ППО для заданного окружения. В них могут содержаться параметры из общего конфигурационного файла или из конфигурационных файлов подсистем ППО, значения которых надо переопределить для заданного окружения	4 (самый высокий приоритет)
--	--	-----------------------------

При установке ППО параметры конфигурационных файлов применяются согласно порядку, приведенному в таблице (Таблица 27). Т.е. сценарий установки обрабатывает сначала конфигурационные файлы в каталоге «`config/vars/`», затем в каталоге «`config/subsystems/<название подсистемы>/vars/`» и т.д. Если, например, какой-либо параметр одновременно задан и в «`config/vars/`» и «`config/subsystems/<название подсистемы>/vars/`», то ППО будет установлено со значением параметра заданным в «`config/subsystems/<название подсистемы>/vars/`».

10.2.7.1. Правила обработки сценариями установки ППО параметров, массивов и списков, если они одновременно заданы в нескольких конфигурационных файлах

Правило обработки параметров: Значение параметра в конфигурационном файле с более высоким приоритетом переопределяет значение параметра в конфигурационном файле с более низким приоритетом.

Пример параметра:

```
redis_password: "example_redis_password"
```

Правило обработки массивов: массив в конфигурационном файле с более высоким приоритетом переопределяет массив в конфигурационном файле с более низким приоритетом.

Пример массива:

```
pg_hba_settings:
  - type: local # Unix-socket access
    name: all
```

```
database: all
method: trust
- type: host # Localhost IPv4 access
name: all
database: all
address: 127.0.0.1/32
method: trust
- type: host # Localhost IPv6 access
name: all
database: all
address: ::1/128
method: trust
- type: host # Gitlab CI vbox-testing
name: all
database: all
address: 172.17.0.0/16
method: md5
```

Правило обработки списков: если список в конфигурационном файле с более низким приоритетом содержит новые элементы (которых не было в конфигурационном файле с более высоким приоритетом), то они добавляются к исходному списку. Значение параметра в списке, содержащемся в конфигурационном файле с более высоким приоритетом, переопределяет значение параметра из списка содержащемся в конфигурационном файле с более низким приоритетом.

Пример списка:

```
postgresql:
  dbname: example_db_name # database name
  port: 5432 # port
  user: example_user # user
  password: ocs # password
  extensions: ["pg_partman_bgw", "pg_trgm", "pg_stat_statements",
"pgcrypto"] # necessary extensions
```

10.3. Описание конфигурационных файлов ППО (сценариев установки ППО)

10.3.1. Описание конфигурационного файла сценариев установки ППО hosts.yml (файл: inventories/hosts.yml)

10.3.1.1. Описание конфигурационного файла сценариев установки ППО hosts.yml (файл: inventories/hosts.yml) приведено в таблице (Таблица 28).

Таблица 28

Параметр	Описание	Добавлен/ Удален
all.children.ocs.children.app.hosts	Хосты, куда будут установлены серверные приложения ППО	2.2.0 / -
all.children.ocs.children.postgresql.children.postgresql_masters.hosts	Хосты, куда будет установлена СУБД PostgreSQL или Postgres Pro (master)	2.2.0 / -
all.children.ocs.children.postgresql.children.postgresql_slaves.hosts	Хосты, куда будет установлена СУБД PostgreSQL или Postgres Pro (slave)	2.2.0 / -
all.children.ocs.children.nginx.children.app	Хосты, куда будет установлен балансировщик микросервисов Nginx Web Server	2.2.0 / -
all.children.ocs.children.consul.children.consul_masters.children.app	Хосты, куда будет установлена система мониторинга сервисов Consul.(master)	2.2.0 / -
all.children.ocs.children.consul.children.consul_agents	Хосты, куда будет установлена система мониторинга сервисов Consul.(agent)	2.2.0 / -
all.children.ocs.children.consul_template.children.children.app	Хосты, куда будет установлен Consul Template	2.2.0 / -
all.children.ocs.children.nats_streaming_server.hosts	Хосты, куда будет установлен сервис гарантированной доставки сообщений Nats streaming server	2.2.0 / -
all.children.ocs.children.redis.children.redis_masters.hosts	Хосты, куда будет установлена СУБД Redis для хранения сессий (master)	2.2.0 / -

Параметр	Описание	Добавлен/ Удален
all.children.ocs.children.redis.children.redis_slaves.hosts	Хосты, куда будет установлена СУБД Redis для хранения сессий (slave)	2.2.0 / -
all.children.ocs.children.redis.children.redis.sentinel.hosts	Хосты, куда будет установлен Redis Sentinel, обеспечивающий высокую доступность СУБД Redis	2.2.0 / -

10.3.2. Описание конфигурационных файлов ПБ (сценариев установки ПБ)

10.3.2.1. Описание параметров конфигурационного файла ПБ (/var/ocs/auth/config.yml), шаблона конфигурационного файла ПБ (config/subsystems/auth/config/services/config.yml.j2) и конфигурационного файла сценариев установки ПБ _vars.yml (config/subsystems/auth/vars/_vars.yml) приведено в таблице (Таблица 29).

Таблица 29

Параметр в файлах: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено	
config.publicUri.auth.	publicUri	auth_public_uri	Полный адрес публичного API сервера авторизации	2.2.1 / -
config.publicUri.auth.	publicBasepath	auth_public_basepath	Префикс url публичного API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия	2.2.1 / -
config.publicUri.auth.	adminBasepath	auth_admin_basepath	Префикс url к API консоли подсистемы безопасности, используемый для внутреннего межподсистемного взаимодействия	2.2.1 / -

Параметр в файлах: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено	
config.publicUri.e mm.	adminUri	emm_admin_uri	Полный адрес API/UI консоли администратора EMM	2.2.1 / -
config.session.	rememberFor	session_remember_for	Время жизни сессии пользователя консоли	2.2.0 / -
config.session.	renewTimeout	session_renew_timeout	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.database.	host	Задается выражением: <pre>{% if postgresql_patroni_cluster is defined and postgresql_patroni_cluster bool %}localhost{% else %}{{ groups['postgresql_masters'] first }}{% endif %}</pre>	Адрес (хост) базы данных	2.2.0 / -
config.database.	port	postgresql.port	Порт базы данных	2.2.0 / -
config.database.	dbname	postgresql.dbname	Имя базы данных	2.2.0 / -
config.database.	user	postgresql.user	Имя пользователя базы данных	2.2.0 / -
config.database.	password	postgresql.password	Пароль базы данных	2.2.0 / -
config.consul.	token	consul_token	Секрет для аутентификации в consul	2.5.0 / -
config.redis.	sentinelAddresses	Задается выражением: <pre>{{ groups['sentinel'] map('regex_rep</pre>	Адрес модуля sentinel СУБД Redis	2.2.0 / -

Параметр в файлах: config.yml, config.yml.j2		Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
		lace', '^(.*)\$', '\\1:26379') join(', ')} с использованием параметров из hosts.yml		
config.redis.	sentinelPass word	redis_password	Пароль к модулю sentinel СУБД Redis	2.2.0 / -
config.redis.	masterName	redis_master_name	Идентификатор (имя) БД Redis	2.2.0 / -
config.redis.	password	redis_password	Пароль к СУБД Redis	2.2.0 / -
config.transport.	shutdownTime	transport_shutdown_time	Время на завершение открытых соединений перед тем, как сервис завершит работу	2.3.0 / -
config.transport.nats.	url	Задается выражением: {% for host in groups['nats_streaming_server'] %}nats://{{nats.auth_token}} @{{ host }}:4222{% if not loop.last %},{% endif %}{% endfor %} с использованием параметров из hosts.yml и vars.yml	Адрес сервера NATS	2.3.0 / -
config.transport.nats.	clusterID	nats.cluster_id	Идентификатор кластера NATS (https://docs.nats.io/)	2.3.0 / -
config.transport.nats.	redeliveryCount	-	Количество повторных отправок сообщений шиной при неудачной обработке сообщения	2.5.0 / -

Параметр в файлах: config.yml, config.yml.j2		Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.transport.ht tp.tls.	enabled	-	Флаг включения TLS протокола	2.2.0 / -
config.transport.ht tp.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.ht tp.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.ht tp.tls.	ca_certificate	-	Путь к файлу с доверенным сертификатом. При незаполненном значении формируется по принципу config_folder/ca.crt	2.2.0 / -
config.transport.ht tp.httpDebug.	address	-	[не используется] Адрес сервера (для служебных debug-эндпоинтов приложения)	2.4.0 / -
config.transport.ht tp.httpDebug.tls.	enabled	-	[не используется] Флаг включения TLS протокола (для служебных debug- эндпоинтов приложения)	2.2.0 / -
config.transport.ht tp.httpDebug.tls.	private_key	-	[не используется] Путь к файлу с приватным ключом (для служебных debug-эндпоинтов приложения)	2.2.0 / -

Параметр в файлах: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено	
config.transport.ht tp.httpDebug.tls.	certificate	-	[не используется] Путь к файлу с сертификатом (публичный ключ) (для служебных debug- эндпоинтов приложения)	2.2.0 / -
config.transport.ht tp.httpDebug.tls.	ca_certificat e	-	[не используется] Путь к файлу с доверенным сертификатом (для служебных debug- эндпоинтов приложения)	2.2.0 / -
config.ttl.	login_conse nt_request	ttl_login_consent _request	Время жизни запроса на авторизацию	2.2.0 / -
config.ttl.	access_toke n	ttl_access_token	Время жизни access_token	2.2.0 / -
config.ttl.	refresh_tok en	ttl_refresh_token	Время жизни refresh_token. При значении «-1» считается бесконечным	2.2.0 / -
config.ttl.	id_token	ttl_id_token	Время жизни id_token	2.2.0 / -
config.ttl.	auth_code	ttl_auth_code	Время жизни auth_code	2.2.0 / -
config.	passwordEx pirationTim e	-	Максимальное время действия пароля.	2.2.0 / -
config.passwordSe ttings.	minLength	-	Минимальная длина пароля. Значение: 8. Если указать значение меньше, чем 8, то система должна считать, что minLength = 8.	2.2.0 / -
config.passwordSe ttings.	maxLength	-	Максимальная длина пароля. Значение: 255. Если указать значение меньше, чем minPasswordLength (минимальная длина пароля), то система	2.2.0 / -

Параметр в файлах: config.yml, config.yml.j2		Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
			должна считать, что maxPasswordLength = minPasswordLength	
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 TUVWXYZ	2.2.0 / -
config.passwordSettings.	lowerLetters	-	Допустимые для пароля символы нижнего регистра abcdefghijklmnopqrstuvwxyz wxyz	2.2.0 / -
config.passwordSettings.	specialChars	-	Допустимые для пароля специальные символы !@#\$%^&*()_+	2.2.0 / -
config.	failedLoginTries	-	Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки учетной записи Значение: "3"	2.2.0 / -

Параметр в файлах: config.yml, config.yml.j2		Параметр в файле _vars.yml	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.	loginGraceTime	-	Время, в течение которого считаются неуспешные попытки аутентификации перед блокировкой	2.2.0 / -
config.	privilegedSessionsLimit	privileged_sessions_limit	Допустимое количество одновременно запущенных сессий у привилегированной учетной записи	2.2.0 / -
config.	unprivilegedSessionsLimit	unprivileged_sessions_limit	Допустимое количество одновременно запущенных сессий у непривилегированной учетной записи	2.2.0 / -
config.	insecureUri	insecure_uri	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 / -

Параметр в файлах: config.yml, config.yml.j2		Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.	expose_internal_errors	expose_internal_errors	Флаг отображения расширенной информации в ошибках. По умолчанию выключен, так как информация может содержать данные, нежелательные к раскрытию. Используется для отладки	2.5.0 / -
config.	insecureRedirectUris	<p>Задается выражением</p> <pre>[{% if insecure_uri is defined and insecure_uri %} "{{ emm_admin_uri }}/", "{{ aps_admin_uri }}/", "{{ aps_dev_uri }}/", "{{ auth_admin_uri }}/", "{{ push_admin_uri }}/", {% endif %}]</pre> <p>с использованием параметров из vars.yml</p>	Список url на которые сервер авторизации разрешает делать редирект по протоколу http в процессе аутентификации. Конфиг можно заполнять только при включенной опции config.insecureUri	2.2.0 / -
config.secrets.	system	-	Ключи для шифрования системной информации	2.2.0 / -
config.secrets.	cookie	-	Ключи для шифрования cookie, передаваемые в браузер	2.2.0 / -

Параметр в файлах: config.yml, config.yml.j2		Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.	allowTerminationFrom	<p>Задается выражением</p> <pre>[{% if allow_termination_from is defined %} {% for host in allow_termination_from %} "{{ host }}", {% endfor %} {% endif %} {% for host in groups['app'] %} "{{ hostvars[host]['ansible_default_ipv4']['address'] }}" {% endfor %}]</pre> <p>с использованием параметров из vars.yml и hosts.yml</p>	<p>Список ip адресов, с которых можно делать запросы на сервер авторизации по протоколу http</p>	2.2.0 / -
config.ocs-auth-accounts-users-api.	passwordHistoryDepth	-	<p>Число последних использованных паролей, которые запрещено использовать при создании новых паролей. Новый пароль не должен совпадать с паролями из истории в рамках заданного значения. Используется для учетных записей пользователей.</p>	2.2.0 / -

Параметр в файлах: config.yml, config.yml.j2		Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.ocs-auth-accounts-users-api.	maxAccountInactivityPeriod	-	Максимальный срок неактивности учетной записи, после которого она должна быть заблокирована. Используется для учетных записей пользователей	2.2.0 / -
config.ocs-auth-accounts-devices-api.	passwordHistoryDepth	-	Число последних использованных паролей, которые запрещено использовать при создании новых паролей. Новый пароль не должен совпадать с паролями из истории в рамках заданного значения. Используется для учетных записей с ролью МП «Аврора Центр»	2.2.0 / -
config.ocs-auth-accounts-devices-api.	maxAccountInactivityPeriod	-	Максимальный срок неактивности учетной записи, после которого она должна быть заблокирована. Используется для учетных записей с ролью МП «Аврора Центр»	2.2.0 / -
config.	gatewayTimeout	gateway_timeout	Таймаут запросов на шлюзы	2.2.0 / -
config.	hashWorkers	-	Количество воркеров, вычисляющих хэши паролей. По умолчанию 16.	2.4.0 / -

Параметр в файлах: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.oidcClients. authAdminConsole	scope	<p>Задается выражением:</p> <pre> {{ oidc_clients[' auth-admin-console'].scope }} </pre> <p>с использованием параметров из oidc.yml</p>	<p>Скопы для oidc клиента, который используется для аутентификации в консоли ПБ</p> <p>2.2.0 / -</p>
config.oidcClients. authAdminConsole	returnUri	<p>Задается выражением:</p> <pre> {{ oidc_clients[' auth-admin-console'].redirect_uris first }} </pre> <p>с использованием параметров из oidc.yml</p>	<p>Адрес, на который сервер авторизации сделает редирект после аутентификации в консоли ПБ</p> <p>2.2.0 / -</p>
config.logger.	level	logger_level	<p>Уровень детализации сообщений логирования.</p> <p>Возможные значения: debug, info, warn, error</p> <p>2.2.0 / -</p>
config.logger.	caller	logger_caller	<p>Флаг включения в сообщение лога названия функции и номера строки, в которой происходит логирование события</p> <p>2.2.0 / -</p>
config.logger.	humanReadable	logger_human_readable	<p>Флаг включения форматирования сообщений лога в обычный текст (не json)</p> <p>2.4.0 / -</p>
config.tracing.	enabled	tracing_enabled	<p>Флаг включения трассировки</p> <p>2.2.0 / -</p>

Параметр в файлах: config.yml, config.yml.j2		Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.tracing.	sample_rate	tracing_sample_rate	Частота дискретизации трассировки	2.2.0 / -
config.tracing.	reporting_period	tracing_reporting_period	Отчетный период трассировки	2.2.0 / -
config.tracing.	jaeger_agent_endpoint	-	Адрес подключения к Jaeger	2.2.0 / -
config.jaeger.	address	-	Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/)	2.2.0 / -
config.	enablePprof	enable_pprof	Флаг включения отладочного профилировщика	2.2.0 / -

10.3.3. Описание конфигурационных файлов ПМ (сценариев установки ПМ)

10.3.3.1. Описание параметров конфигурационного файла ПМ (/var/ocs/appstore/config.yml), шаблона конфигурационного файла ПМ (config/subsystems/appstore/config/services/config.yml.j2) и конфигурационного файла сценариев установки ПМ _vars.yml (config/subsystems/appstore/vars/_vars.yml) приведено в таблице (Таблица 30).

Таблица 30

Параметр в файлах: config.yml, config.jml.j2		Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
config.publicUri s.auth.	publicUri	auth_public_uri	Полный адрес публичного API сервера авторизации *	2.2.1 / -
-	-	auth_public_address	Адрес публичного API сервера авторизации	2.4.0 / -
-	-	auth_public_basepath	Basepath публичного API сервера авторизации	2.4.0 / -
config.publicUri s.auth.	adminUri	auth_admin_uri	Полный адрес API/UI консоли ПБ *	2.2.1 / -

Параметр в файлах: config.yml, config.jml.j2		Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
-	-	auth_admin_addresses	Адрес API/UI консоли ПБ	2.4.0 / -
-	-	auth_admin_basepath	Basepath API/UI консоли ПБ	2.4.0 / -
config.publicUri s.aps.	adminUri	aps_admin_uri	Полный адрес API/UI административной консоли Аврора Маркет	2.5.0 / -
-	-	aps_admin_address	Адрес API/UI административной консоли Аврора Маркет	2.5.0 / -
-	-	aps_admin_basepath	Basepath API/UI административной консоли Аврора Маркет	2.5.0 / -
config.publicUri s.aps.	devUri	aps_dev_uri	Полный адрес API/UI Консоли разработчика ПМ *	2.2.1 / -
-	-	aps_dev_address	Адрес API/UI консоли Разработчика	2.4.0 / -
-	-	aps_dev_basepath	Basepath API/UI Консоли разработчика ПМ	2.4.0 / -
config.publicUri s.aps.	devBasepath	aps_dev_basepath	Префикс API/UI Консоли разработчика ПМ	2.2.1 / -
config.publicUri s.aps.	adminBasepath	aps_admin_basepath	Префикс в url для Консоли администратора ПМ	2.2.1 / -
config.publicUri s.aps.	marketUri	aps_market_uri	Полный адрес API клиентского шлюза	2.5.0 / -
-	-	aps_market_address	Адрес API клиентского шлюза	2.5.0 / -
-	-	aps_market_basepath	Basepath API клиентского шлюза	2.5.0 / -
-	-	aps_client_address		2.4.0 / 2.5.0

Параметр в файлах: config.yml, config.jml.j2	Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
-	-	aps_client_basepath	2.4.0 / 2.5.0
-	-	aps_client_uri	2.4.0 / 2.5.0
config.publicUri s.emm.	adminUri	emm_admin_uri	Полный адрес API/UI Консоли администратора ПУ 2.2.1 / -
-	-	emm_admin_addresses	Адрес API/UI Консоли администратора ПУ 2.4.0 / -
-	-	emm_admin_basepath	Basepath API/UI Консоли администратора ПУ 2.4.0 / -
config.systemU ris.auth.	publicAddress	"http://ocs-auth- public-api-gw." + domain	Адрес публичного API авторизации - для межсистемного взаимодействия 2.2.1 / -
config.systemU ris.auth.	publicBasepath	-	Префикс публичного API авторизации - для межсистемного взаимодействия 2.2.1 / -
config.systemU ris.auth.	adminAddress	"http://ocs-auth- admin-api-gw." + domain	Адрес административного API авторизации - для межсистемного взаимодействия 2.2.1 / -
config.systemU ris.auth.	adminBasepath	-	Префикс административного API авторизации - для межсистемного взаимодействия 2.2.1 / -
config.session.	rememberFor	session_remember_ for	Время жизни сессии пользователя консоли 2.2.0 / -
config.session.	renewTimeout	session_renew_time out	Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а

Параметр в файлах: config.yml, config.jml.j2	Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено	
		один раз за данный интервал)		
config.oidcClients.apsDevConsole.	scope	oidc_clients['aps-dev-console'].scope из hosts.yml	Скопы для oidc клиента, который используется для аутентификации в Консоли разработчика ПМ	2.2.0 / -
config.oidcClients.apsDevConsole.	returnUri	oidc_clients['aps-dev-console'].redirect_uri из hosts.yml	Адрес, на который сервер авторизации сделает редирект после аутентификации в Консоли разработчика ПМ	2.2.0 / -
config.oidcClients.apsAdminConsole.	scope	oidc_clients['aps-admin-console'].scope из hosts.yml	Скопы для oidc клиента, который используется для аутентификации в Консоли администратора ПМ	2.2.0 / -
config.oidcClients.apsAdminConsole.	returnUri	oidc_clients['aps-admin-console'].redirect_uri из hosts.yml	Адрес, на который сервер авторизации сделает редирект после аутентификации в Консоли администратора ПМ	2.2.0 / -
config.database.	host	<p>формируется из</p> <ul style="list-style-type: none"> – postgresql_patroni_cluster; – groups['postgresql_masters'] <p>из hosts.yml</p> <pre>{% if postgresql_patroni_cluster is defined and postgresql_patroni_cluster </pre>	Адрес (хост) БД	2.2.0 / -

Параметр в файлах: config.yml, config.jml.j2		Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
		<pre>bool %}localhost{% else %}{{ groups['postgres sql_masters'] first }}{% endif %}</pre>		
config.databases. e.	port	postgresql.port	Порт базы данных	2.2.0 / -
config.databases. e.	dbname	postgresql.dbname	Имя базы данных	2.2.0 / -
config.databases. e.	user	postgresql.user	Имя пользователя БД	2.2.0 / -
config.databases. e.	password	postgresql.password	Пароль БД	2.2.0 / -
config.consul.	token	consul_token	Токен для доступа к Consul	2.5.0 / -
config.redis.	sentinelAddresses	<pre>формируется из - groups['sentinel'] из hosts.yml groups['sentinel '] map('regex_repla ce', '^(.*)\$', '\1:26379') join(',')</pre>	Адрес модуля sentinel СУБД Redis	2.2.0 / -
config.redis.	sentinelPassword	redis_password	Пароль к модулю sentinel СУБД Redis	2.2.0 / -
config.redis.	masterName	redis_master_name	Идентификатор (имя) БД Redis	2.2.0 / -
config.redis.	password	redis_password	Пароль к СУБД Redis	2.2.0 / -
config.transport. t.	shutdownTime	transport_shutdown_time	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.3.0 / -
config.transport.nats.	url	<pre>формируется из - groups['nats_strea ming_server'] из hosts.yml</pre>	Адрес сервера NATS	2.3.0 / -

Параметр в файлах: config.yml, config.jml.j2		Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
		<pre>{% for host in groups['nats_str eaming_server'] %}nats://{{nats. auth_token}}@{{ host }}:4222{% if not loop.last %},{% endif %}{{% endfor %}</pre>		
config.transpor t.nats.	clusterID	nats.cluster_id	Идентификатор кластера NATS (https://docs.nats.io/)	2.3.0 / -
config.transpor t.nats.	redeliveryCoun t	-	Максимальное количество попыток обработать событие. По умолчанию количество попыток - 3.	2.5.0 / -
config.transpor t.http.tls.	enabled	-	Флаг включения TLS протокола	2.3.0 / -
config.transpor t.http.tls.	private_key	-	Путь к файлу с приватным ключом. При незаполненном значении формируется по принципу config_folder/app_nam e/app_name.key	2.2.0 / -
config.transpor t.http.tls.	certificate	-	Путь к файлу с сертификатом (публичный ключ). При незаполненном значении формируется по принципу config_folder/app_nam e/app_name.crt	2.2.0 / -

Параметр в файлах: config.yml, config.jml.j2		Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
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.tls.	enabled	-	[не используется] Флаг включения TLS протокола (для служебных debug-эндпоинтов приложения)	2.2.0 / -
config.transport.httpDebug.tls.	private_key	-	[не используется] Путь к файлу с приватным ключом (для служебных debug-эндпоинтов приложения)	2.2.0 / -
config.transport.httpDebug.tls.	certificate	-	[не используется] Путь к файлу с сертификатом (публичный ключ) (для служебных debug-эндпоинтов приложения)	2.2.0 / -
config.transport.httpDebug.tls.	ca_certificate	-	[не используется] Путь к файлу с доверенным сертификатом (для служебных debug-эндпоинтов приложения)	2.2.0 / -
config.	insecureUri	insecure_uri	Флаг использования незащищенного соединения. Этот параметр надо задавать в true если	2.2.0 / -

Параметр в файлах: config.yml, config.jml.j2		Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
			используется незащищенное соединение (http протокол). Он влияет на формирование Cookie заголовков, проверку редиректов	
config.	gatewayTimeout	gateway_timeout	Таймаут запросов при взаимодействии со шлюзами	2.3.0 / -
config.	clientTimeout	client_timeout	Таймаут запросов при межсервисном взаимодействии	2.3.0 / -
config.logger.	level	logger_level	Уровень детализации сообщений логирования. Возможные значения: debug, info, warn, error	2.2.0 / -
config.logger.	caller	logger_caller	Флаг включения в сообщение лога названия функции и номера строки, в которой происходит логирование события	2.2.0 / -
config.logger.	humanReadable	logger_human_readable	Флаг включения форматирования сообщений лога в обычный текст (не json)	2.4.0 / -
config.tracing.	enabled	tracing_enabled	Флаг включения трассировки	2.2.0 / -
config.tracing.	sample_rate	tracing_sample_rate	Частота дискретизации трассировки	2.2.0 / -
config.tracing.	reporting_period	tracing_reporting_period	Отчетный период трассировки	2.2.0 / -
config.tracing.	jaeger_agent_endpoint	-	Адрес подключения к Jaeger	2.2.0 / -

Параметр в файлах: config.yml, config.jml.j2		Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
config.jaeger.	address	-	Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/)	2.2.0 / -
config.	enablePprof	enable_pprof	Флаг включения отладочного профилировщика	2.2.0 / -
config.publishedReleaseRequiredFields.	changelog	-	Требуется ли заполнение поля «Что нового» для публикации второго и последующих релизов	2.4.0 / -
config.publishedReleaseRequiredFields.	description	-	Требуется ли заполнение поля «Описание приложения» для публикации релиза	2.4.0 / -
config.publishedReleaseRequiredFields.	icon	-	Требуется ли заполнение поля «Иконка» для публикации релиза	2.4.0 / -
config.publishedReleaseRequiredFields.	keywords	-	Требуется ли заполнение поля «Ключевые слова» для публикации релиза	2.4.0 / -
config.publishedReleaseRequiredFields.	minScreenshotCount	-	Количество скриншотов, требуемое для публикации релиза. 0 - не требуются.	2.4.0 / -
config.publishedReleaseRequiredFields.	policyUrl	-	Требуется ли заполнение поля «URL политики конфиденциальности» для публикации релиза	2.4.0 / -

Параметр в файлах: config.yml, config.jml.j2		Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
config.publishedReleaseRequiredFields.	secondCategory	-	Требуется ли заполнение поля «Категория 2» для публикации релиза	2.4.0 / -
config.publishedReleaseRequiredFields.	supportEmail	-	Требуется ли заполнение поля «email поддержки» для публикации релиза	2.4.0 / -
config.publishedReleaseRequiredFields.	webSiteUrl	-	Требуется ли заполнение поля «Сайт приложения» для публикации релиза	2.4.0 / -
config.	secrets	-	Список секретов для механизма шифрования приватных ключей. Первый в списке - актуальный секрет. Остальные нужны для расшифровки зашифрованных данных (с последующим шифрованием с актуальным секретом)	2.3.0 / -
config.smtp.	from	-	Почта и имя отправителя	3.0.0 / -
config.smtp.	address	-	Адрес почтового сервера	3.0.0 / -
config.smtp.	authType	-	Тип аутентификации	3.0.0 / -
config.smtp.	host	-	Имя хоста для аутентификации	3.0.0 / -
config.smtp.	username	-	Имя пользователя для аутентификации	3.0.0 / -
config.smtp.	password	-	Пароль для аутентификации	3.0.0 / -

Параметр в файлах: config.yml, config.jml.j2		Параметр в файле _vars.yml	Описание (* помечены поля, которые запрещено редактировать)	Добавлено / Удалено
config.smtp.	identity	-	identity для аутентификации обычно совпадает с username или пустая строка	3.0.0 / -
config.smtp.	secret	-	Ключ для подписи сообщений с помощью md5 hmac	3.0.0 / -

10.3.4. Описание конфигурационных файлов ПУ (сценариев установки ПУ)

10.3.4.1. Описание параметров конфигурационного файла ПУ (/var/ocs/emm/config.yml), шаблона конфигурационного файла ПУ (config/subsystems/emm/config/services/config.yml.j2) и конфигурационного файла сценариев установки ПУ _vars.yml (config/subsystems/emm/vars/_vars.yml) приведено в таблице (Таблица 31).

Таблица 31

Параметр файла: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.insecureUri	insecure_uri	Использование незащищенного соединения. Этот параметр необходимо задавать в true если используется незащищенное соединение (http протокол). Он влияет на формирование Cookie заголовков, проверку редиректов.	2.2.0 / -
config.publicUri.emm.mobileUri	emm_mobile_uri	Полный адрес API для МП «Аврора Центр»	2.2.0 / -
config.publicUri.emm.adminBasepath	emm_admin_basepath	Префикс админского API/UI ПУ	2.2.0 / -

Параметр файла: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.publicUri.auth. .publicUri	auth_public_uri	Полный адрес публичного API сервера авторизации	2.2.0 / -
config.publicUri.auth. .adminUri	auth_admin_uri	Полный адрес админского API/UI сервера авторизации	2.2.0 / -
config.publicUri.aps. adminUri	aps_admin_uri	Полный адрес админского API/UI подсистемы «Маркет»	2.2.0 / -
config.systemUri.auth. h.publicAddress	-	Хост публичного API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия	2.2.0 / -
config.systemUri.auth. h.publicBasepath	-	Префикс публичного API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия	2.2.0 / -
config.systemUri.auth. h.adminAddress	-	Хост админского API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия	2.2.1 / -
config.systemUri.auth. h.adminBasepath	-	Префикс к админскому API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия	2.2.1 / -
config.systemUri.aps. .marketAddress	-	Хост API подсистемы «Маркет», используемый для внутреннего межподсистемного взаимодействия	2.2.0 / -
config.systemUri.aps. .marketBasepath	-	Префикс к API подсистемы «Маркет», используемый для внутреннего межподсистемного взаимодействия	2.2.0 / -

Параметр файла: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.systemUris.pkg Repo.adminAddress	-	Хост админского API подсистемы обновлений, используемый для внутреннего межподсистемного взаимодействия	2.2.1 / -
config.systemUris.pkg Repo.adminBasepath	-	Префикс к админскому API подсистемы обновлений, используемый для внутреннего межподсистемного взаимодействия	2.2.1 / -
config.systemUris.push. adminAddress	-	Хост админского API подсистемы Push-уведомлений, используемый для внутреннего межподсистемного взаимодействия	2.3.0 / -
config.systemUris.push. adminBasepath	-	Префикс к админскому API подсистемы Push-уведомлений, используемый для внутреннего межподсистемного взаимодействия	2.3.0 / -
config.systemUris.push. publicAddress	-	Хост публичного API подсистемы Push-уведомлений, используемый для внутреннего межподсистемного взаимодействия	2.4.0 / -
config.systemUris.push. publicBasepath	-	Префикс к публичному API подсистемы Push-уведомлений, используемый для внутреннего межподсистемного взаимодействия	2.4.0 / -
config.redis.sentinelA ddress	формируется из groups['sentinel'] из hosts.yml	Адрес модуля sentinel СУБД Redis	2.2.0 / -
config.redis.sentinelP assword	redis_passw ord	Пароль к модулю sentinel СУБД Redis	2.2.0 / -
config.redis.masterNa me	-	Идентификатор (имя) БД Redis	2.2.0 / -
config.redis.password	redis_passw ord	Пароль к СУБД Redis	2.2.0 / -

Параметр файла: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.session.rememberFor	session_remember_for	Время жизни сессии	2.2.0 / -
config.session.renewTimeout	session_renew_timeout	Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаются не на каждую активность, а один раз за данный интервал)	2.2.0 / -
config.oidcClients.emmAdminConsole.scope	формируется из oidc_clients['emm-admin-console'].scope из hosts.yml	Скопы для oidc клиента, который используется для аутентификации в Консоли администратора ПУ	2.2.1 / -
config.oidcClients.emmAdminConsole.returnUri	oidc_clients['emm-admin-console'].returnUri из hosts.yml	Адрес, на который сервер авторизации сделает редирект после аутентификации в Консоли администратора ПУ	2.2.1 / -
config.database.host	формируется из - postgresql_patroni_cluster - groups['postgresql_masters'] из hosts.yml <pre>{% if postgresql_patroni_cluster is defined and postgresql_patroni_cluster bool %}localhost{% else %}{{ groups['postgresql_masters'] first }}{% endif %}</pre>	Адрес (хост) БД ПУ	2.2.0 / -
config.database.port	postgresql.port	Порт БД ПУ	2.2.0 / -
config.database.user	postgresql.user	Имя пользователя БД ПУ	2.2.0 / -
config.database.dbname	postgresql.dbname	Имя БД ПУ	2.2.0 / -

Параметр файла: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
me			
config.database.password	postgresql.password	Пароль БД ПУ	2.2.0 / -
config.consul.token	consul_token	Токен для доступа к Consul	2.5.0 / -
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	transport_shutdown_time	Время на завершение открытых соединений, перед тем, как сервис завершит работу	2.2.0 / -
config.transport.nats.url	формируется из – groups['nats_streaming_server'] из hosts.yml – auth_token {% for host in groups['nats_streaming_server'] }%nats://{{nats_auth_token}}@{{ host }}:4222{% if not loop.last %},{% endif %}}{% endfor %}	Адрес сервера NATS	2.2.0 / -
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 / -

Параметр файла: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.tracing.jaeger_agent_endpoint	-	Адрес подключения к Jaeger	2.2.1 / -
config.jaeger.address	-	Адрес подключения к Jaeger, см. https://www.jaegertracing.io/docs/1.17/	2.4.0 / -
config.enablePprof	enable_pprof	Флаг включения pprof, используется для отладки кода	2.4.0 / -
config.logger.level	logger_level	Уровень детализации сообщений логирования. Возможные значения: – debug; – info; – warning; – error.	2.2.0 / -
config.logger.caller	logger_caller	Признак включения в лог дополнительных полей (имя файла, название функции): – false; – true	2.2.0 / -
config.logger.gateway_gin_log_enabled	gateway_gin_log_enabled	Флаг включения логирования входящего запроса на шлюзе (url запроса и http-статус ответа)	2.2.1 / 2.4.0
config.logger.humanReadable	logger_human_readable	Флаг управления редактированием логгера	2.4.0 / -
config.smtp.from	-	Адрес эл. почты, с которой отправляются письма	2.2.0 / -
config.smtp.address	-	Адрес сервера эл. почты	2.2.0 / -
config.smtp.AuthType	-	Тип авторизации. Может принимать значения CRAM-MD5, PLAIN, LOGIN, либо не заполняться	2.4.0 / -

Параметр файлов: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.smtp.Identity	-	Идентификатор учетной записи пользователя, обычно совпадает с Username Заполняется для типа авторизации PLAIN	2.4.0 / -
config.smtp.Username	-	Логин пользователя Заполняется для типа авторизации PLAIN, CRAM-MD5, LOGIN	2.4.0 / -
config.smtp.Password	-	Пароль пользователя Заполняется для типа авторизации PLAIN, LOGIN	2.4.0 / -
config.smtp.Host	-	Адрес (хост) почтового сервера. Заполняется для типа авторизации PLAIN	2.4.0 / -
config.smtp.Secret	-	Ключ, с помощью которого подписываются hmac.md5 данные между сервером и клиентом. Заполняется для типа авторизации CRAM-MD5	2.4.0 / -
config.smtp.tls	-	Доступность неявного TLS для SMTP при необходимости: – true; – false. Значение зависит от конфигурации сервера	2.4.0 / -
config.qrCodeTtl	-	Время жизни QR-кода	2.2.0 / -
config.jobService.url	-	Внутренний адрес сервиса Jobs	2.3.0 / -
config.ldapServer.address	ldap_server.address	Адрес LDAP сервера пример: "ldap://msk1pdc.omp.ru"	2.3.0 / -
config.ldapServer.userCN	ldap_server.user_cn	Логин от технической учетной записи от LDAP сервера	2.3.0 / -
config.ldapServer.password	ldap_server.password	Пароль от технической учетной записи от LDAP сервера	2.3.0 / -

Параметр файла: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
config.ldapServer.parentGroup	ldap_server.parent_group	Название группы, с которой будет происходить импорт данных орг. структуры из LDAP сервера	2.3.0 / -
config.ldapServer.pageSize	ldap_server.page_size	Количество элементов, которое будет импортировано за одну итерацию. Максимальное значение: 1000	2.3.0 / -
-	project_name	Имя проекта	2.2.1 / -
-	download_mode	Модуль для скачивания исходников	2.2.1 / -
-	repository_dir	Директория для скачивания исходников	2.2.1 / -
-	postgresql.extensions	Необходимые расширения для Postgres	2.2.1 / -
-	postgres_password	Пароль для подключения к БД Postgres	2.2.1 / -
-	nats.auth_token	Используется для формирования config.transport.nats.url	2.2.1 / -
-	redis_password	Используется для формирования config.redis.sentinelPassword, config.redis.password	2.2.1 / -
-	auth_public_address	Используется для: – для генерации oidc клиентов; – формирования переменных *_uri	2.2.1 / -
-	auth_admin_address		2.2.1 / -
-	aps_admin_addresses		2.2.1 / -
-	aps_market_addresses		2.2.1 / -
-	emm_admin_addresses		2.2.1 / -
-	emm_mobile_addresses		2.2.1 / -

Параметр файла: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
	pkgrepo_admin_address		2.2.1 / -
	push_admin_address		2.3.0 / -
	auth_public_basepath		2.2.1 / -
	auth_admin_basepath		2.2.1 / -
	emm_admin_basepath		2.2.1 / -
	emm_mobile_basepath		2.2.1 / -
	aps_admin_basepath		2.2.1 / -
	aps_market_basepath		2.2.1 / -
	pkgrepo_admin_basepath		2.2.1 / -
-	emm_admin_console_client_secret	Используется для генерации OIDC клиентов	2.2.1 / -
-	same_site_mode	Определяет параметр sameSite для csrf-куки (допустимые значения: "strict", "lax", "none", "")	2.3.0 / 2.5.0
-	krakendcsrf_enabled	Использование CSRF на гейтвеях, принимает значения: – true; – false	2.3.0 / -
-	expose_internal_errors	Используется для управления внутренней ошибкой в ответах запросов к сервисам, принимает значения: – true; – false	2.5.0 / -
aurora_mobility_management_client_secret	-		2.2.1 / -

Параметр файлов: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
emm_integration_account_client_secret	-		2.2.1 / -
domain	http://ocs-appstore-admin-api-gw.{{ domain }}/api/categories		2.2.1 / -
pushNotificationSystem.enabled	Push_notification_system.enabled	Используется для удобного включения и отключения функции отправки настроек Push-уведомлений (на бэкэнде)	2.4.0 / -
pushNotificationSystem.hostname		IP-адрес или имя хоста сервиса Push-уведомлений	2.4.0 / -
pushNotificationSystem.port		Порт сервиса Push-уведомлений	2.4.0 / -
pushNotificationSystem.applicationID		Идентификатор приложения, с которым регистрируется МП в сервисе Push-уведомлений	2.4.0 / -
pushNotificationSystem.mobileHostname	push_mobile_hostname	IP-адрес или имя хоста сервиса Push-уведомлений для МП	2.4.0 / -
pushNotificationSystem.mobilePort	push_mobile_port	Порт сервиса Push-уведомлений для МП	2.4.0 / -
pushNotificationSystem.messageTTL	Push_notification_system.messageTTL	Время жизни Push-уведомления	2.4.0 / -
pushNotificationSystem.projectId	Push_notification_system.project_id	Идентификатор проекта для отправки Push-уведомлений	2.4.0 / -
pushNotificationSystem.clientId	Push_notification_system.client_id	Идентификатор клиента технической учетной записи	2.4.0 / -
pushNotificationSystem.privateKey	Push_notification_system.private_key	Приватный ключ технической учетной записи	2.4.0 / -
pushNotificationSystem.keyId	Push_notification_system.key_id	Приватный ключ технической учетной записи, указывает, какой ключ используется на сервисе авторизации	2.4.0 / -
pushNotificationSystem.audience	Push_notification_system.audience	Audience в понятии OAuth2	2.4.0 / -

Параметр файлов: config.yml, config.yml.j2	Параметр в файле _vars.yml	Описание	Добавлено/ Удалено
		https://tools.ietf.org/id/draft-tschofenig-oauth-audience-00.html	
pushNotificationSystem.scopes	Push_notification_system.scopes	Скопы для oidc клиента, которые используются для аутентификации в ПУ	2.4.0 / -
pushNotificationSystem.tokenURL	Push_notification_system.token_url	URL для получения токена авторизации	2.4.0 / -

10.3.5. Описание конфигурационных файлов ПООС (сценариев установки ПООС)

10.3.5.1. Описание параметров конфигурационного файла ПООС (/var/ocs/pkgrepo/config.yml), шаблона конфигурационного файла ПООС (config/subsystems/pkgrepo/config/services/config.yml.j2) и конфигурационного файла сценариев установки ПООС _vars.yml (config/subsystems/pkgrepo/vars/_vars.yml) приведено в таблице (Таблица 32).

Таблица 32

Параметр в общем конфигурационном файле config.yml.j2	Параметр в конфигурационном файле vars.yml	Описание	Добавлено/ Удалено
config.publicUri.auth.publicUri	auth_public_uri	Полный адрес публичного API сервера авторизации	2.2.0 / - 2.4.0 / - 2.4.0 / -
config.database.host	формируется из: – postgresql_patroni_cluster; – groups['postgresql_masters'] {% if postgresql_patroni_cluster is defined and	Адрес (хост) БД ПООС	2.2.0 / -

Параметр в общем конфигурационном файле config.yml.j2	Параметр в конфигурационном файле vars.yml	Описание	Добавлено/ Удалено
	<pre>postgresql_patron i_cluster bool %}localhost{% else %} {{ groups['postgresq l_masters'] first }}{% endif %}</pre>		
config.database.port	postgresql.port	Порт БД ПООС	2.2.0 / -
config.database.user	postgresql.user	Имя пользователя БД ПООС	2.2.0 / -
config.database.dbname	postgresql.dbname	Имя БД ПООС	2.2.0 / -
config.database.password	postgresql.password	Пароль БД ПООС	2.2.0 / -
config.redis.sentinelAddress	формируется из groups['sentinel']	Адрес модуля sentinel СУБД Redis	2.2.0 / -
config.redis.sentinelPassword	redis_password	Пароль к модулю sentinel СУБД Redis	2.2.0 / -
config.redis.masterName	-	Идентификатор (имя) БД Redis	2.2.0 / -
config.redis.password	redis_password	Пароль к СУБД Redis	2.2.0 / -
config.transport.tls.enabled	-	Доступность TLS протокола	2.2.0 / -
config.transport.shutdownTime	transport_shutdown_time	Время на завершение открытых соединений перед тем, как сервис завершит работу	2.2.0 / -
config.transport.nats.url	<pre>формируется из: - groups['nats_streaming_server'] - auth_token {% for host in groups['nats_streaming_server'] %}nats://{{nats.auth_token}}@{{ host }}:4222 {% if not</pre>	Адрес сервера NATS	2.2.0 / -

Параметр в общем конфигурационном файле config.yml.j2	Параметр в конфигурационном файле vars.yml	Описание	Добавлено/ Удалено
	<code>loop.last %}, {% endif %}{% endfor %}</code>		
<code>config.transport.nats.clusterID</code>	-	Идентификатор кластера NATS	2.2.0 / -
<code>config.zipkin.address</code>	-	Адрес подключения к Zipkin	2.2.0 / 2.2.1
<code>config.tracing.enabled</code>	-	Доступность трейсера	2.2.1 / -
<code>config.tracing.sample_rate</code>	-	Частота дискретизации трассировки	2.2.1 / -
<code>config.tracing.reporting_period</code>	-	Отчетный период трассировки	2.2.1 / -
<code>config.tracing.jaeger_agent_endpoint</code>	-	Адрес подключения к Jaeger	2.2.1 / -
<code>config.jaeger.address</code>	-	Адрес подключения к Jaeger, см. https://www.jaegertracing.io/docs/1.17/	2.4.0 / -
<code>config.enablePprof</code>	<code>enable_pprof</code>	Флаг включения pprof, используется для отладки кода	
<code>config.logger.level</code>	<code>logger_level</code>	Уровень детализации сообщений логирования. Возможные значения: – debug; – info; – warning; – error.	2.2.0 / -
<code>config.logger.caller</code>	-	Признак включения в лог дополнительных полей (имя файла, название функции) – false; – true	2.2.0 / -

Параметр в общем конфигурационном файле config.yml.j2	Параметр в конфигурационном файле vars.yml	Описание	Добавлено/ Удалено
config.logger.gateway_gin_log_enabled	gateway_gin_log_enabled	Флаг включения логирования входящего запроса на шлюзе (url запроса и http-статус ответа)	2.2.1 / -
config.logger.humanReadable	logger_human_readable	Флаг управления редактированием логгера	2.4.0 / -
-	project_name	Имя проекта	2.2.0 / -
-	download_mode	Режим загрузки. Доступные типы: – `http`: загружать артефакты из внешнего HTTP-хранилища напрямую на управляемый узел; – `httplocal`: загрузить артефакты из внешнего http-хранилища на управляющий узел, затем скопировать на управляемый узел; – `local`: не загружать артефакты из внешнего http-хранилища, они должны каким-то образом существовать на контрольном узле, копировать локальные артефакты с контрольного узла на управляемый узел.	2.2.0 / -
-	repository_dir	Путь к локальному хранилищу артефактов кэша	2.2.0 / -
-	postgresql.extensions	Необходимые расширения	2.2.0 / -
-	postgres_password	Пароль от postgres	2.2.0 / -

Параметр в общем конфигурационном файле config.yml.j2	Параметр в конфигурационном файле vars.yml	Описание	Добавлено/ Удалено
-	nats.auth_token	Используется для формирования config.transport.nats.url	2.2.0 / -
-	redis_password	Используется для формирования: config.redis.sentinelPassword, config.redis.password	2.2.0 / -
-	auth_public_address	Используется для: – для генерации oidc клиентов; – формирования переменных *_uri	2.2.0 / -
	auth_admin_address		2.2.0 / -
	auth_public_basepath		2.2.0 / -
	auth_admin_basepath		2.2.0 / -
	pkgrepo_mobile_address		2.2.0 / -
	pkgrepo_mobile_basepath		2.2.0 / -
-	updateServers.address	Адрес обращения МУ к репозиторию с обновлением ОС	2.5.0 / -
	retrieveReleasesPeriod	Период времени для перечитывания метафайла релизов	2.2.0 / -
-	pkgrepo_integration_account_client_secret	Используется для генерации OIDC клиентов	2.2.0 / -
-	pkgrepo_mobile_uri	Полный адрес репозитория с обновлениями ОС для МУ	2.2.0 / -
			2.4.0 / -
			2.4.0 / -
-	auth_admin_uri	Полный адрес админского API/UI сервера авторизации	2.2.0 / -
			2.4.0 / -
			2.4.0 / -

11. СООБЩЕНИЯ ОБ ОШИБКАХ

В ходе работы с компонентами ПБ пользователям могут выдаваться сообщения об ошибках, приведенные в таблице (Таблица 33).

Таблица 33

№	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 34).

Таблица 34

Термин/ Сокращение	Расшифровка
БД	База данных
Воркер	Потоки, принадлежащие браузеру, которые можно использовать для выполнения JS-кода без блокировки цикла события
ГИС	Государственная информационная система
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»
ПООС	Подсистема обновления ОС
ППО	Прикладное программное обеспечение «Аврора Центр»
Предприятие-изготовитель	Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа»)
ПУ	Подсистема Платформа управления
ПЭВМ	Персональная электронно-вычислительная машина
СЗИ	Средство защиты информации
СЗИ НСД	Средство защиты информации от несанкционированного доступа

Термин/ Сокращение	Расшифровка
СПО	Специальное программное обеспечение
СУА	Сервис уведомлений Аврора
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"> – МП «Аврора Центр» - роль назначается учетным записям МП «Аврора Центр» (сервис/процесс без участия пользователей, который управляет МУ); – Администратор учетных записей - роль позволяет осуществлять управление учетными записями; – Оператор аудита – роль позволяет осуществлять действия по работе с журналом регистрации событий ППО; – Администратор Платформы Управления - роль позволяет осуществлять все действия по управлению ПУ через интерфейс ППО; – Администратор Аврора Маркет - роль позволяет осуществлять все действия по управлению ПМ через интерфейс системы; – Разработчик - роль позволяет осуществлять добавление новых и обновление ранее загруженных приложений в ПМ, а также получать информацию о приложениях;

Термин/ Сокращение	Расшифровка
	– Пользователь Аврора Маркет - роль 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
FQDN	Fully Qualified Domain Name — «полностью определенное имя домена», иногда сокращается до «полное имя домена»
HEALTH-запрос	Запрос проверки доступности API

Термин/ Сокращение	Расшифровка
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

