

**УТВЕРЖДАЮ:**

**Директор ООО «АЙДЕНТИКА»**

**Абрамович Михаил Леонидович**



**М.П.**

**Осторус**

**Руководство пользователя**

ООО «АЙДЕНТИКА»

город Москва, 2024 год

**Octopus**

**Руководство пользователя**

**(система управления учетными записями и контроля доступа)**

## Содержание

1. О программе для ЭВМ Octopus
  - 1.1. Общие сведения
  - 1.2. Функции
2. Установка Octopus
  - 2.1. Системные требования
  - 2.2. Подготовка и установка
3. Запуск Octopus
  - 3.1. Авторизация пользователя
4. Интерфейс Octopus
  - 4.1. Меню «Обзор»
  - 4.2. Меню «Штат»
    - 4.2.1. Рабочая зона «Сотрудники»
      - 4.2.1.1. Карточка сотрудника
      - 4.2.1.2. Добавление нового сотрудника
    - 4.2.2. Рабочая зона «Организационная структура»
  - 4.3. Меню «Доступы»
    - 4.3.1. Рабочая зона «Аккаунты»
    - 4.3.2. Рабочая зона «Группы/роли»
  - 4.4. Меню «Профили»
  - 4.5. Меню «Политики»
  - 4.6. Меню «Запросы»
  - 4.7. Меню «Ресертификация (аттестация)»
  - 4.8. Меню «Конфигурация»
    - 4.8.1. Рабочая зона «Приложения»
    - 4.8.2. Рабочая зона «Маршруты»
    - 4.8.3. Рабочая зона «Плагины»
    - 4.8.4. Рабочая зона «Автоматические доступы»

## 1. О программе для ЭВМ Ostorus

### *Общие сведения*

Ostorus представляет собой автоматизированную систему управления учетными записями сотрудников и правами доступа к информационным системам организации и включает в себя компоненты каталога сотрудников и ресурсов, сценариев жизненного цикла сотрудников в организации, контроля политик и процедур управления доступом, портала самообслуживания, аудита.

### *Функции*

Ostorus позволяет решать следующие задачи:

- Управление идентификационными данными пользователей в организации
- Управление учетными записями пользователей, включая процедуры создания/удаления и активации/деактивации учетных записей.
- Применение политик управления доступом к информационным системам организации
- Управление назначениями ролей
- Организация процесса запроса прав пользователями через портал самообслуживания

## 2. Установка Ostorus

### *Системные требования*

Для установки Ostorus необходимы:

- аппаратные ресурсы (сервер не хуже: 4 CPU, 16 RAM, 128GB Storage)
- системные программные ресурсы: Debian 12
- прикладные программные ресурсы: -
- сеть: доступ в интернет на порты 443 (любые адреса), 22 (github.com)
- доменные имена: 1. для idm, 2. для idm-worker

### **Порядок установки**

Методы установки зависят от требований к Проекту и наличия технологической базы. Варианты установки включают в себя: Deployment на Kubernetes, на пустую операционную систему через docker compose или ansible galaxy.

## 3. Запуск Ostorus

### *3.1. Авторизация пользователя*



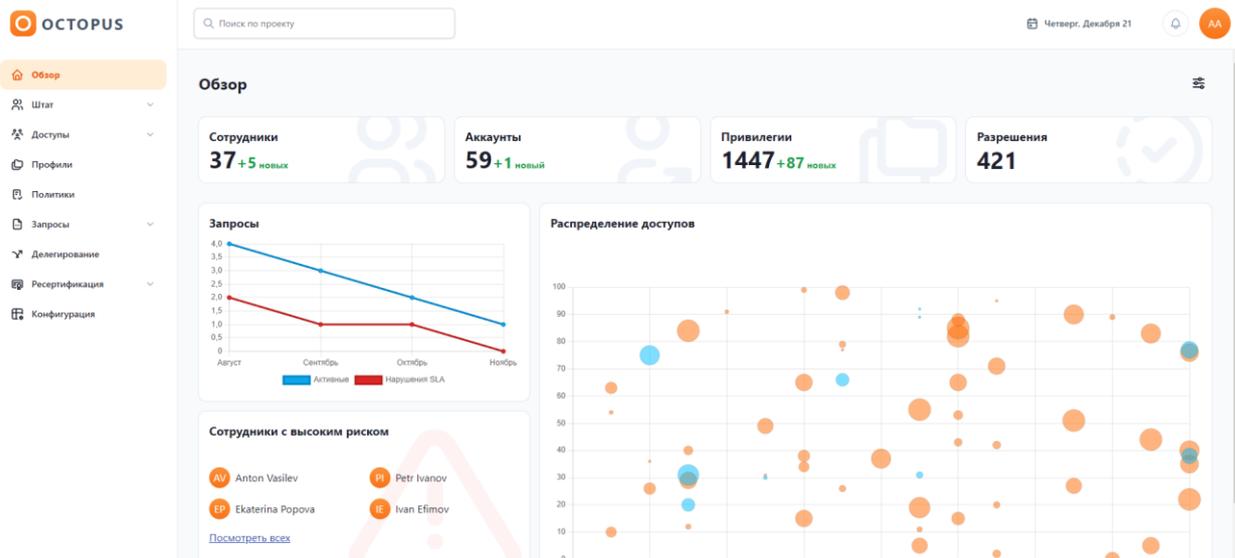
Yandex 360

Для входа следует использовать учетную запись (связку логин и пароль), созданную Администратором программы, либо выбрать один из предложенных способов авторизации.

#### **4. Описание интерфейса.**

##### *4.1. Меню «Обзор»*

Главное окно интерфейса Администратора системы представлено в следующем виде:



Центральная часть консоли (Меню «Обзор») представляет собой набор конфигурируемых виджетов, позволяющих настраивать дэшборд в соответствии с задачами пользователя. По умолчанию представлены базовые наборы таких виджетов – сводная информация по данным о сотрудниках, их аккаунтах, привилегиях и разрешениях; график со статистикой по заявкам пользователей; информация по сотрудникам, имеющим потенциально высокий коэффициент риска для Компании; схема, отображающая информацию по накоплению доступов сотрудников за время их работы в организации.

#### 4.2. Меню «Штаб»

| ID  | Имя                           | E-mail                        | Орг. структура | Тип-но аккаунта | Статус       | Действия |
|-----|-------------------------------|-------------------------------|----------------|-----------------|--------------|----------|
| 404 | Семенова Наталья Семеновна    | natalya.semenova@company.com  | ПДО            | 2               | Активен      | Иконки   |
| 393 | Серебря Николас Анатольевич   | nikolay.sirota@company.com    | Пользователи   | 2               | Активен      | Иконки   |
| 927 | Ситников Сергей Викторович    | sergey.sitnikov@company.com   | ДП             | 2               | Активен      | Иконки   |
| 785 | Склад СМ                      | skladsm@company.com           | Ид_User        | 2               | Активен      | Иконки   |
| 943 | Скрябин Кирилл Геннадьевич    | kirill.skrabin@company.com    | КНС-М          | 2               | Активен      | Иконки   |
| 547 | Слестукина Ана Васильевна     | anna.slustukina@company.com   | УТ             | 2               | Активен      | Иконки   |
| 278 | Смирнова Елена Александровна  | elena.a.smirnova@company.com  | ДСМ            | 2               | Активен      | Иконки   |
| 681 | Смирнов Алексей Александрович | aleksey.a.smirnov@company.com | Ид_User        | 2               | Заблокирован | Иконки   |
| 671 | Смирнов Алексей Сергеевич     | aleksey.smirnov@company.com   | Ид_User        | 2               | Заблокирован | Иконки   |
| 246 | Смирнов Андрей Михайлович     | andrey.smirnov@company.com    | InfSec         | 2               | Активен      | Иконки   |

Меню содержит информацию о сотрудниках, заведенных в систему, а также об организационно-штатной структуре Компании и, соответственно, представлено двумя разделами – «сотрудники» и «структура».

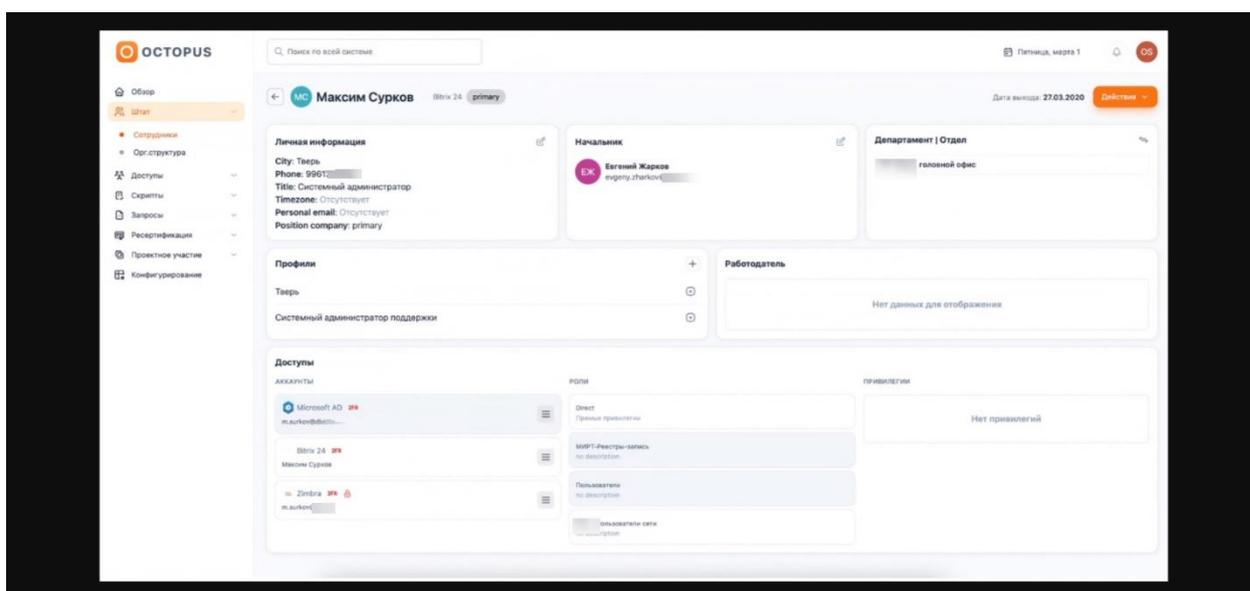
##### 4.2.1. Рабочая зона раздела «Сотрудники»

Представлена в виде списка сотрудников, содержащего информацию:

- ФИО
- рабочий e-mail
- место/принадлежность в организационной структуре Компании
- количество подключенных (ассоциированных с учетной записью) аккаунтов в ИС предприятия

По списку можно осуществлять поиск нужного сотрудника по ФИО, ставить фильтр по типу занятости сотрудника (штатная единица (трудовой договор), внешний подрядчик, внешний аудитор)

#### 4.2.1.1. Карточка сотрудника



Карточка представляет собой отображение сводной информации по сотруднику и логически делится на две части:

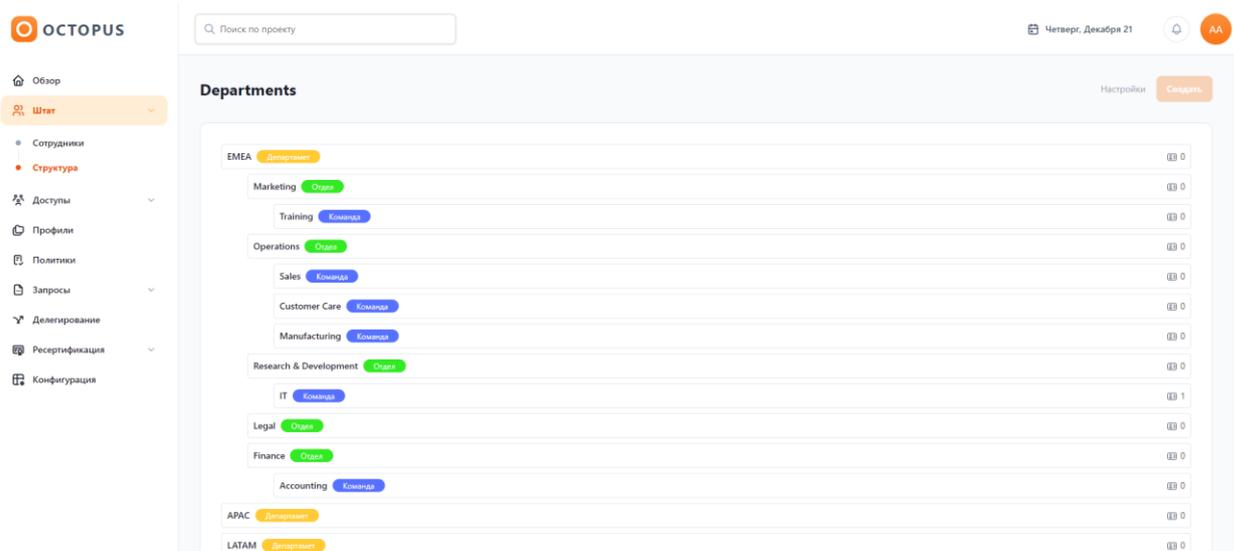
Первая часть содержит информацию о контактных данных, локации, должности и месте в организационно-штатной структуре (Департамент/отдел/ Работодатель).

Вторая часть содержит информацию о доступах: подключенных аккаунтах, ролях, на которые назначен пользователь (используется принцип ролевой модели: в соответствии с занимаемой должностью и обязанностями пользователю назначается определенный набор доступов и полномочий в ИС организации).

#### 4.2.1.2. Добавление нового сотрудника

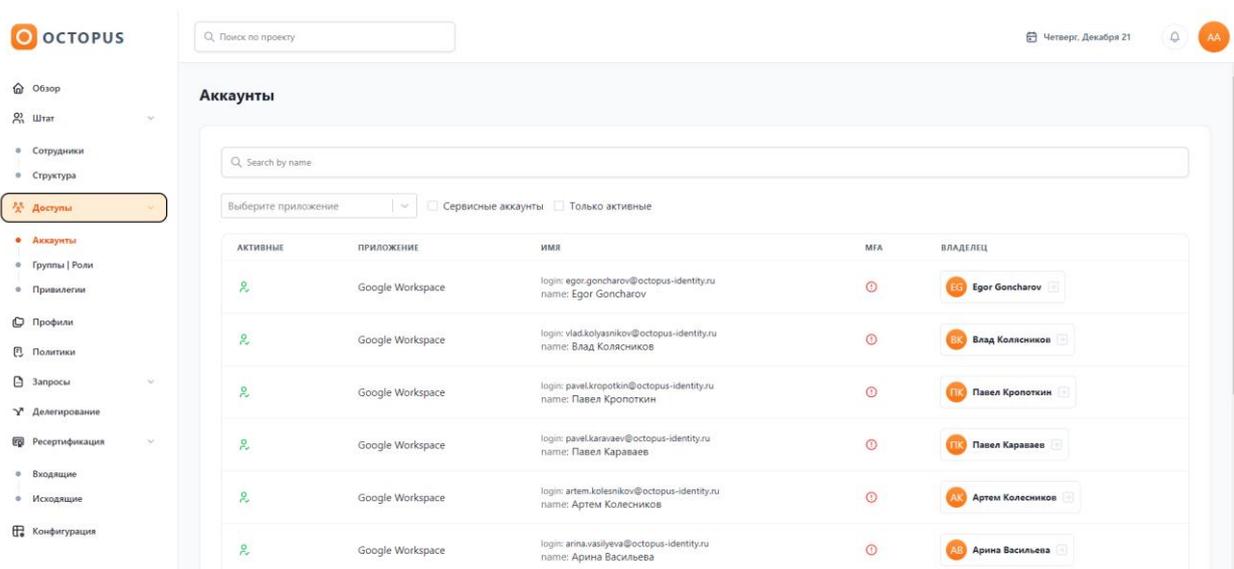
Система, при наличии у пользователя соответствующих прав, предоставляет возможность вручную добавлять нового сотрудника (кнопка «добавить сотрудника» в правой верхней части экрана), введя необходимую информацию: e-mail, дату найма, выбрав департамент, указав непосредственного руководителя, тип сотрудника (штатный сотрудник/внешний подрядчик/аудитор).

## 4.2.2. Рабочая зона меню «Организационная структура»



Представлена в виде списка элементов организационно-штатной структуры Компании, каждый из которых содержит список относящихся к нему сотрудников. Эти элементы гибко конфигурируются в самой системе, включая возможность создавать новые при наличии соответствующих прав.

## 4.3. Меню «Доступы»

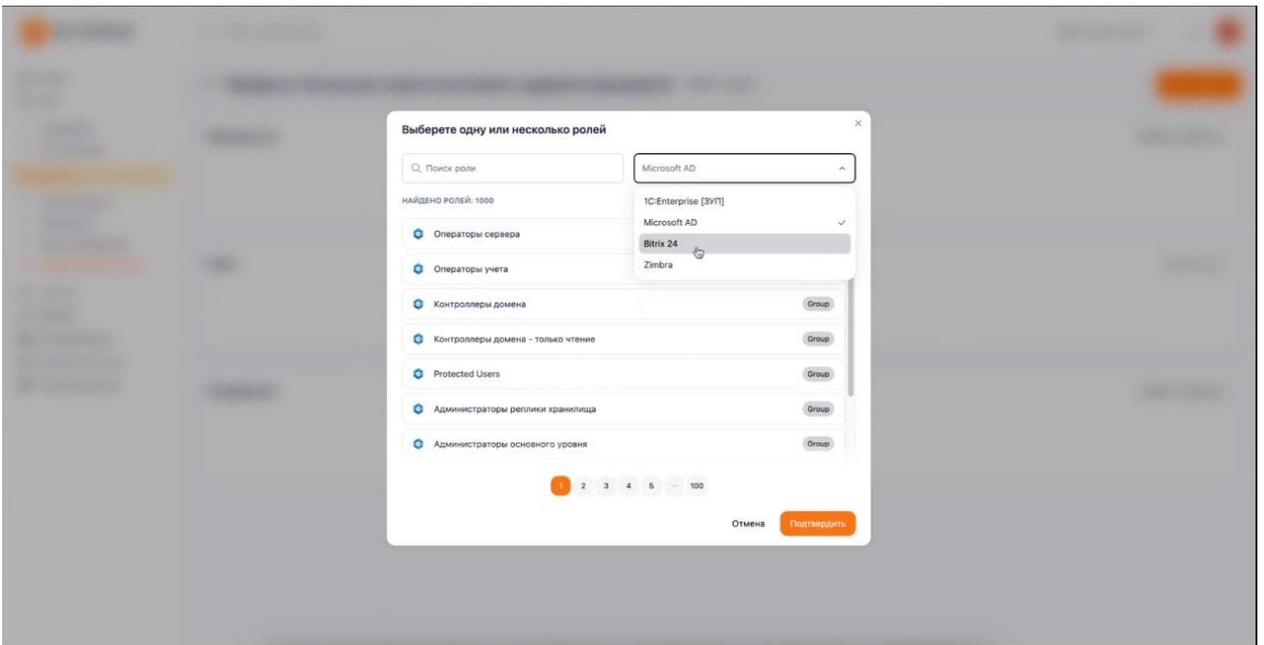


Рабочая область меню представлена тремя подпунктами – «аккаунты», «группы/роли», «привилегии».

### 4.3.1. Рабочая зона «Аккаунты»

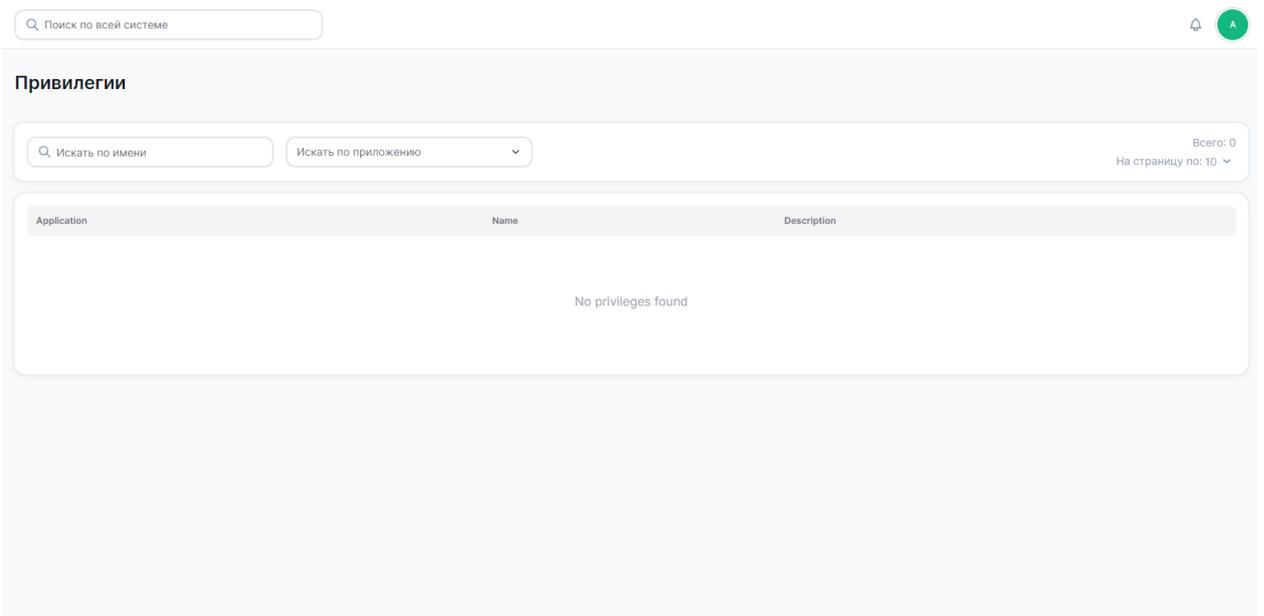
Рабочая зона подпункта содержит информацию об аккаунтах, закрепленных за конкретным пользователем в конкретных ИС компании. Отображается информация о владельце (со ссылкой на его карточку), наименовании приложения. Реализована возможность поиска по списку пользователей, по приложению, а также фильтрации по различным признакам (активный/неактивный, сервисный/обычный).

### 4.3.2. Рабочая зона «Группы/роли»



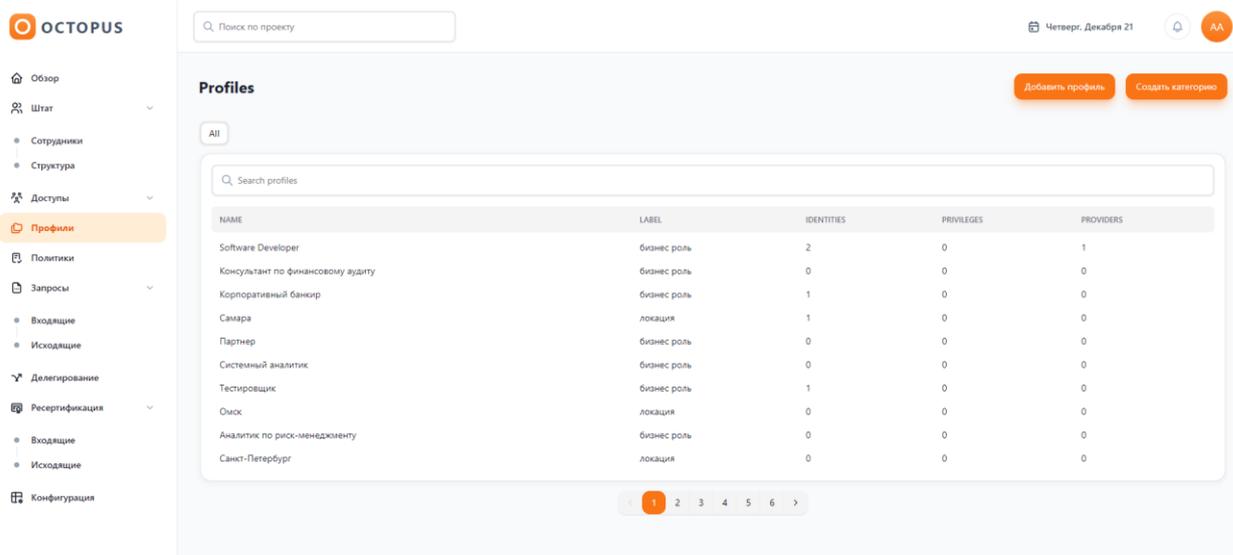
Доступен поиск по ролям, фильтры по управляемым системам.

#### 4.3.3. Рабочая зона «Привилегии»



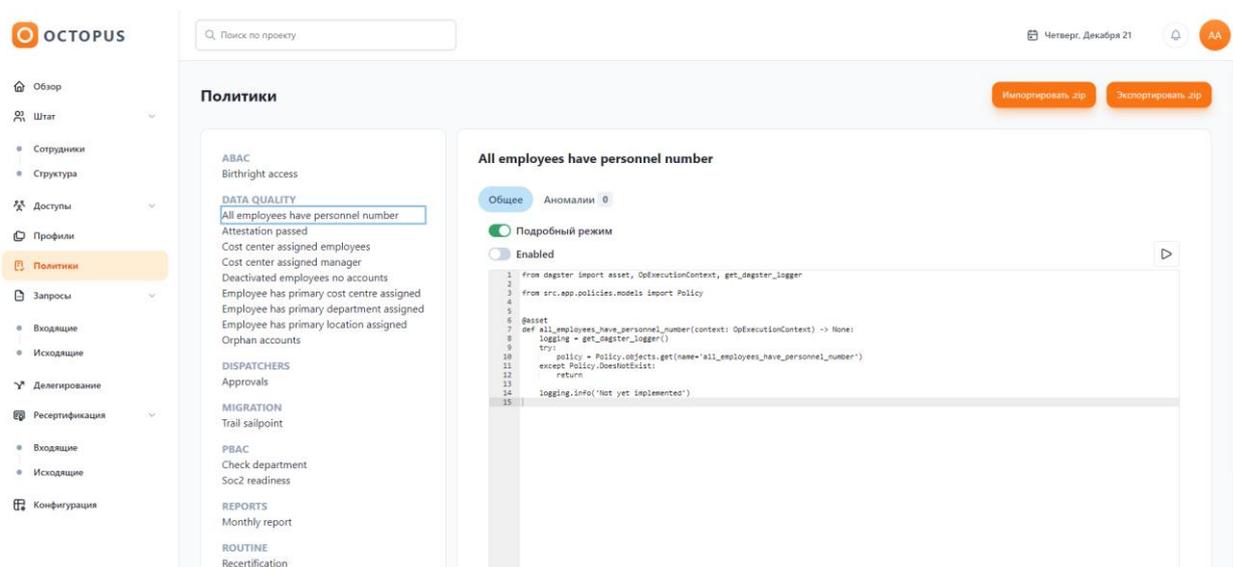
Доступен поиск по точечным привилегиям в конкретных приложениях.

#### 4.4. Меню «Профили»



Профилем могут выступать бизнес-роли (должности, функциональные обязанности), локации (географически распределенные офисы). Предусмотрена возможность заведения пользовательских категорий профилей.

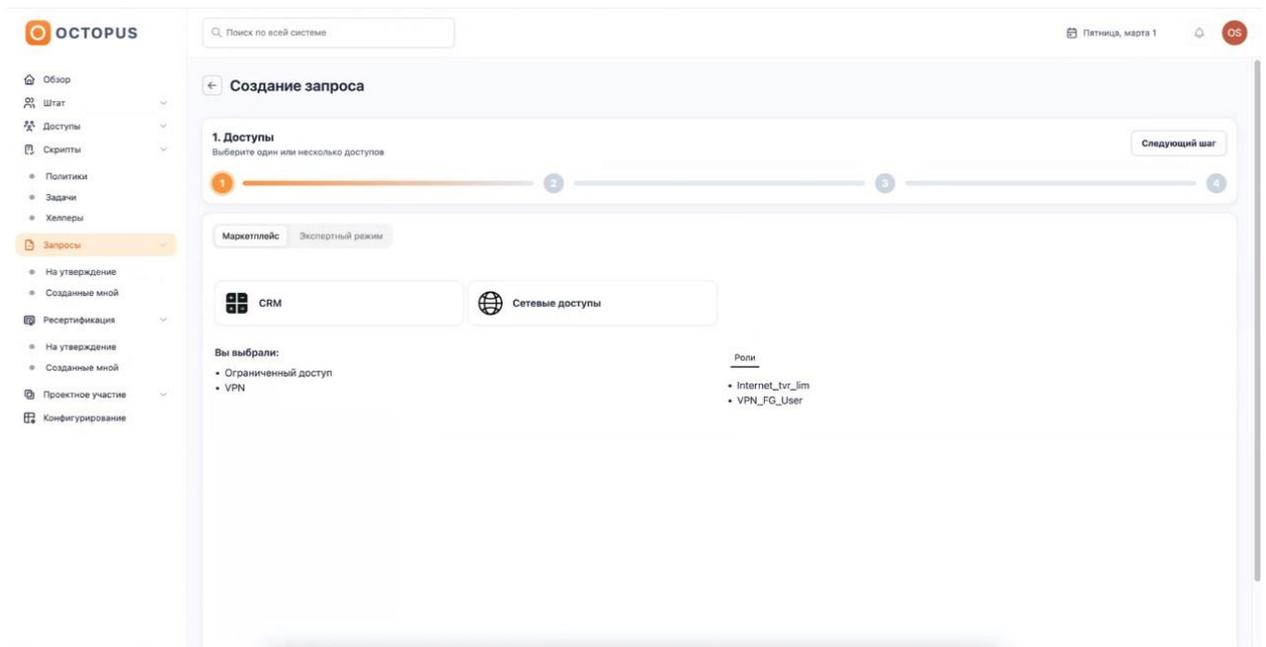
#### 4.5. Меню «Политики»



Рабочая область меню представлена списком политик, при выборе которых вызывается форма для ее редактирования посредством внесения изменений в код.

Также предусмотрена возможность импорта/экспорта политик, предоставленных пользователем.

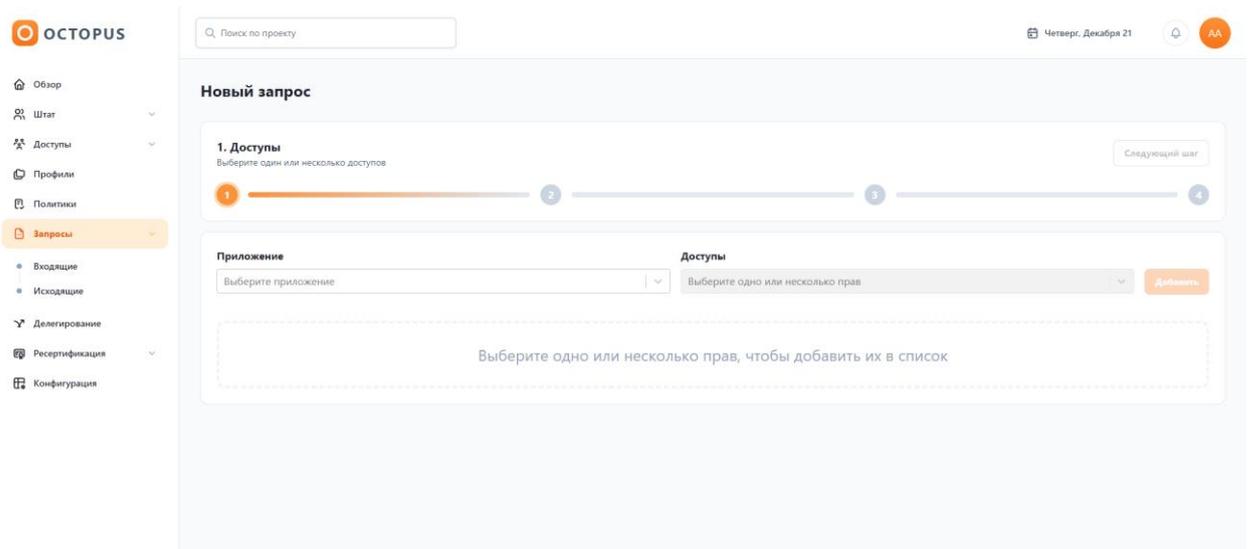
#### 4.6. Меню «Запросы»

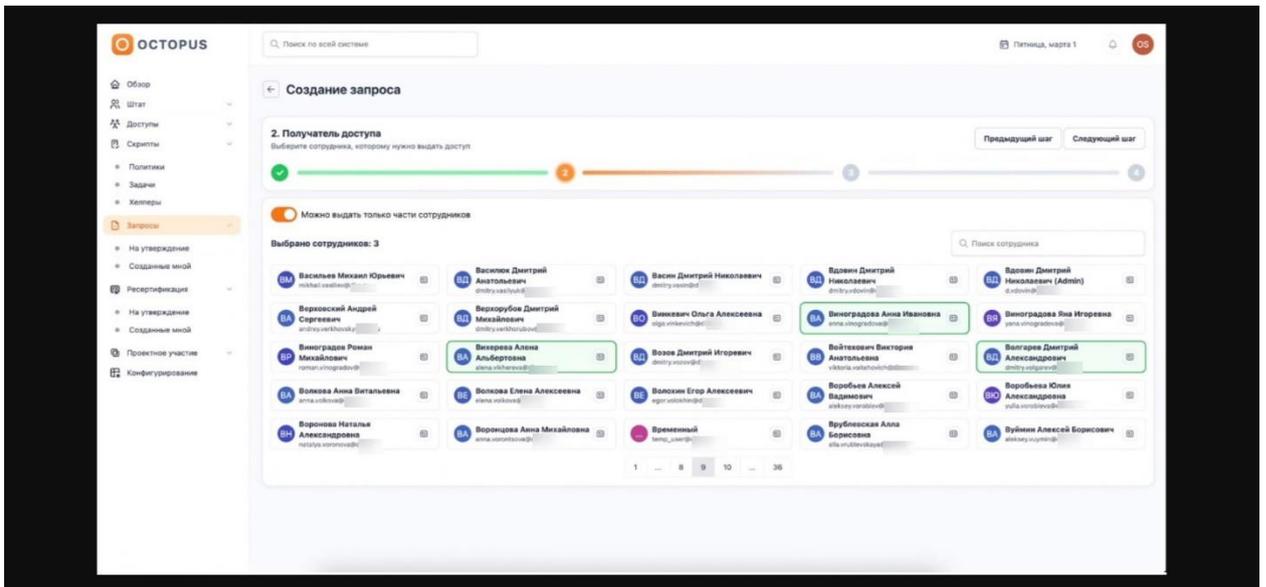


Раздел имеет вид портала самообслуживания и состоит из двух подпунктов: «на утверждение» и «созданные мной».

Меню «на утверждение» содержит список заявок, поступивших пользователю, как участнику согласования. В данном разделе пользователь может выполнять следующие действия:

- Согласование/отклонение запроса;
- Частичное согласование запроса;
- Запрос дополнительной информации.



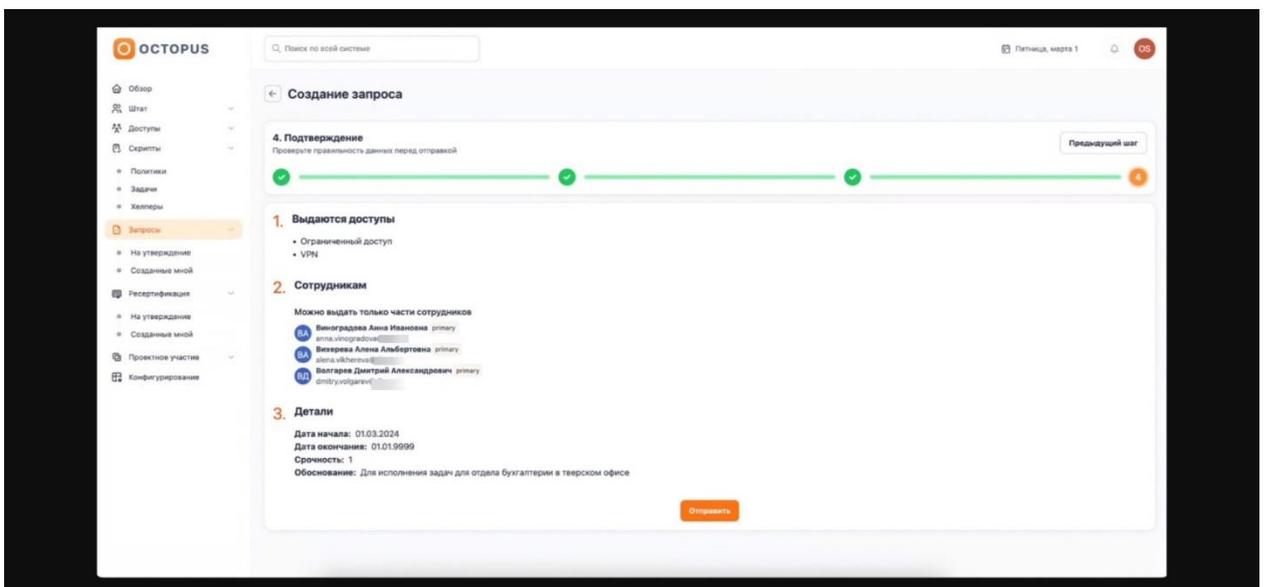


Меню «созданные мной» позволяет создать заявку на предоставление доступа.

При создании нового запроса, на первом шаге пользователь выбирает из выпадающего списка приложение, к которому ему необходим доступ, и одно или несколько требуемых прав. Предусмотрена возможность выбирать несколько приложений в одной заявке.

На втором шаге указывается получатель доступа – сотрудник, которому нужно выдать доступ. По умолчанию системой предлагается сам создатель заявки, и опционально предлагается выбрать другого сотрудника, для которого запрашивается доступ.

На третьем шаге указываются детали: обоснование, важность и сроки действия прав, признак важности заявки.



Четвертый шаг подразумевает проверку правильности данных перед отправкой – пользователь видит сводную информацию о запросе и отправляет заявку на согласование.

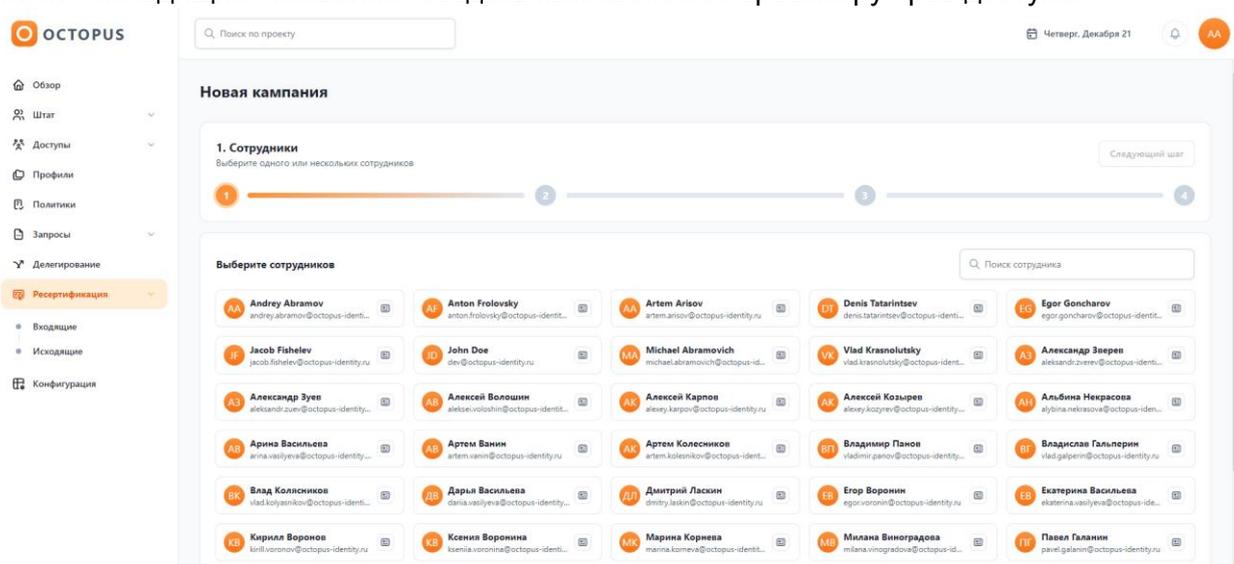
#### 4.7. Меню «Ресертификация (аттестация)»

Это меню позволяет вызывать создание кампаний по пересмотру прав доступа. Оно состоит из двух подпунктов: «входящие» и «исходящие».

Меню «входящие» содержит список заявок, поступивших пользователю, как участнику согласования. В данном разделе пользователь может выполнять следующие действия:

- Согласование/отклонение прав доступа;
- Частичное согласование доступа;
- Запрос дополнительной информации.
- Перевод заявки на другого согласующего.

Меню «исходящие» позволяет создать кампанию по пересмотру прав доступа.



На первом шаге доступен выбор сотрудников для проведения пересмотра их прав доступов.

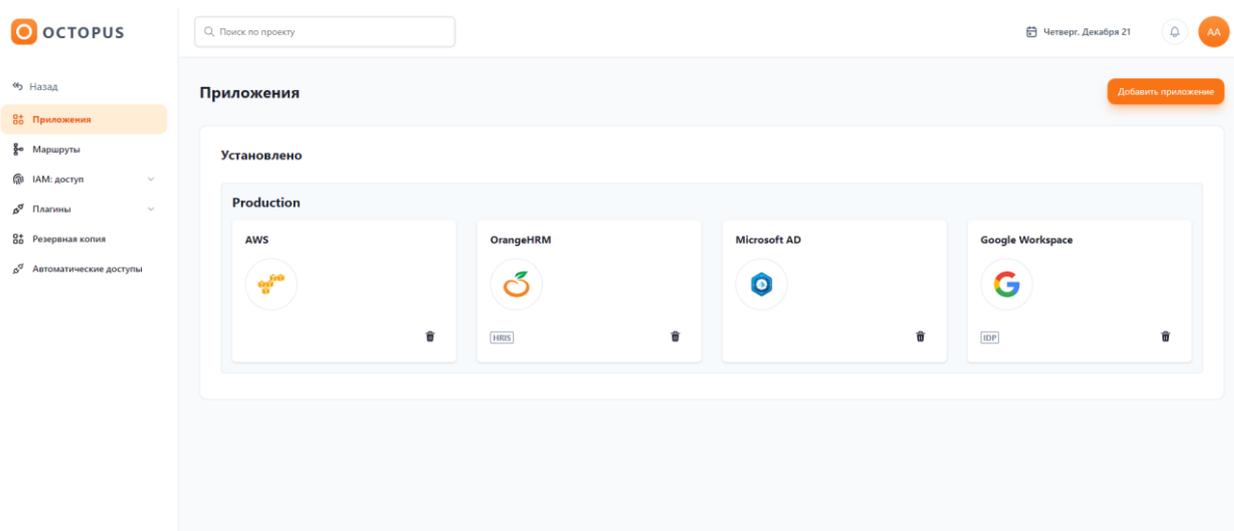
На втором шаге предлагаются доступы для ревизии прав, имеющихся у выбранных сотрудников.

На третьем шаге вводится дополнительная информация по Кампании: ее наименование, дата и сотрудник, который будет выступать исполнителем в системе.

Четвертый шаг предоставляет сводную информацию по заявке и отправляет заявку в работу.

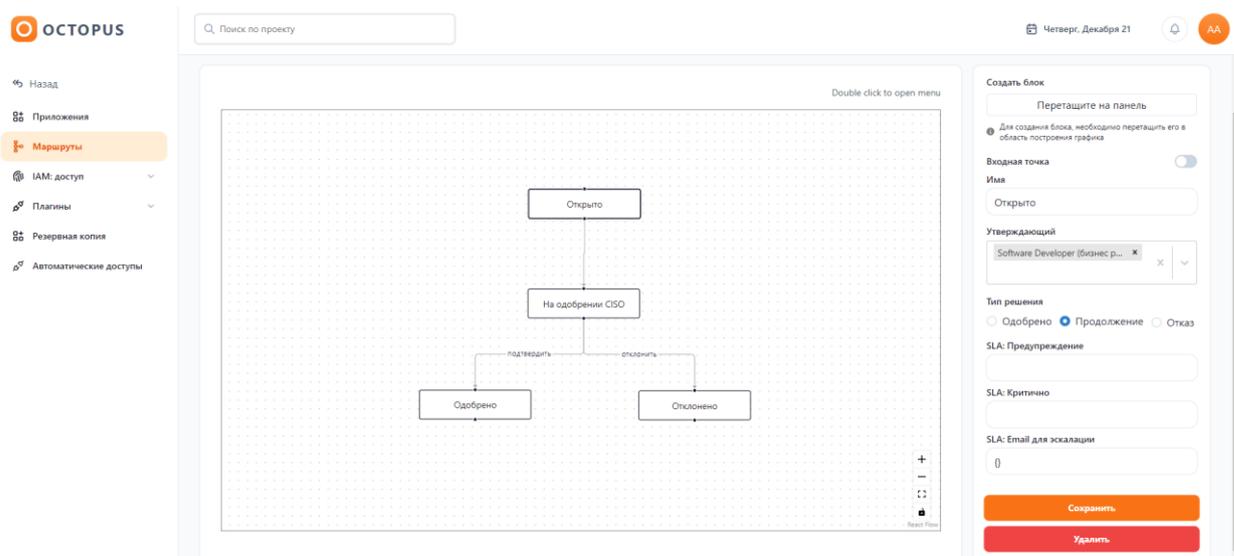
## 4.8. Меню «Конфигурация»

### 4.8.1. Рабочая зона «Приложения»



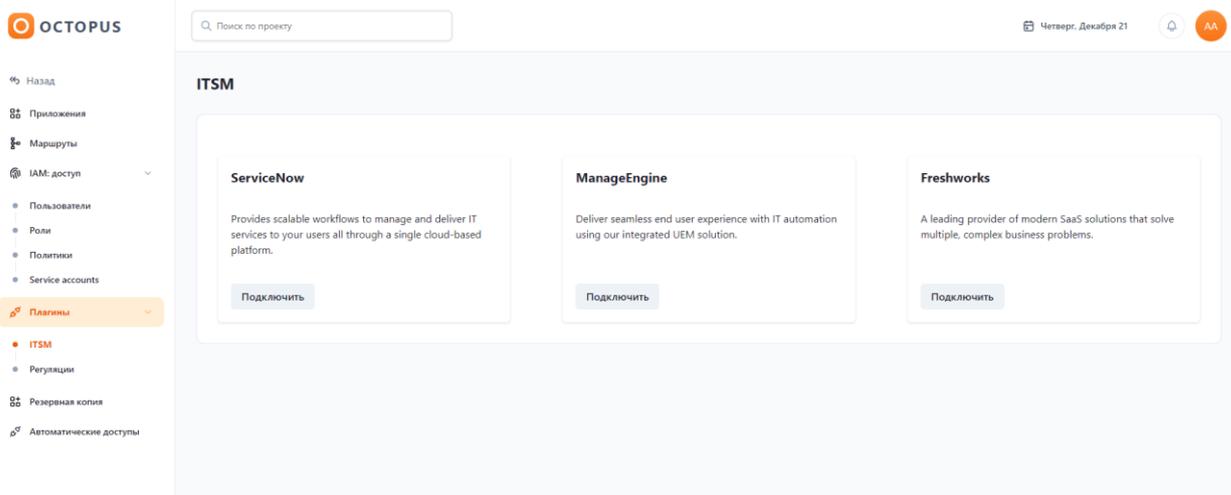
Содержит информацию о приложениях и целевых системах, подключенных к Octopus. Предусмотрена возможность добавить новое приложение.

### 4.8.2. Рабочая зона «Маршруты»



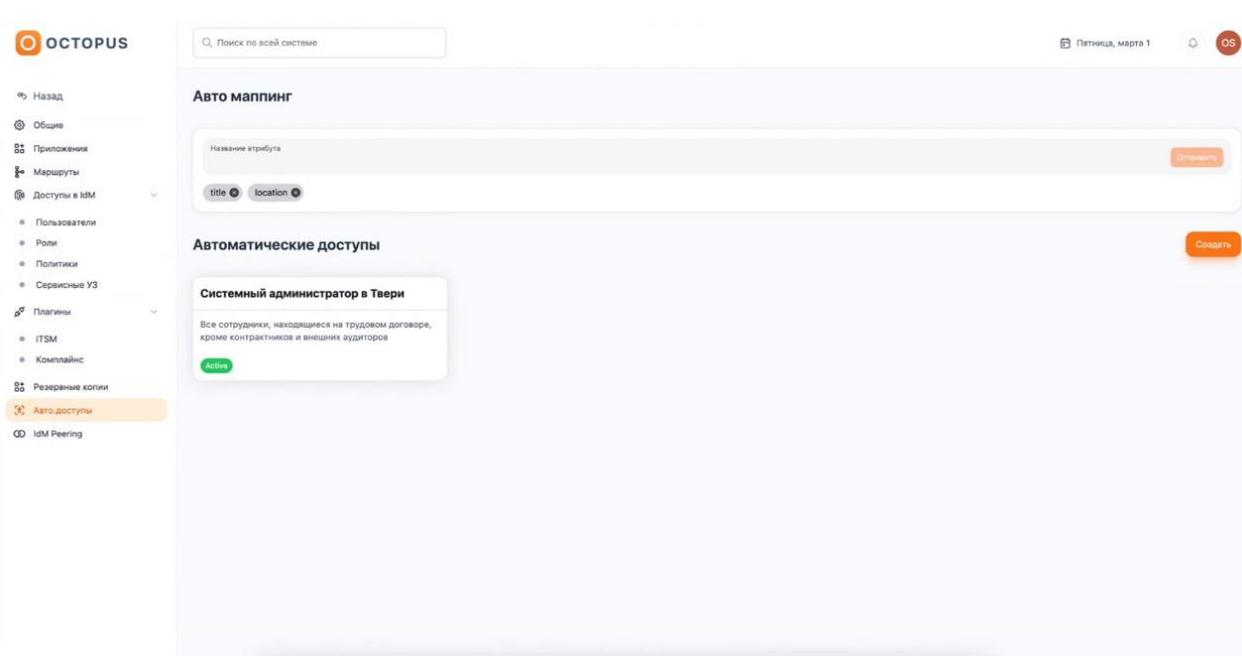
Реализована возможность настраивать маршруты согласования запросов, включая использование дополнительных триггеров, таких, как пользовательские политики, эскалации в случае нарушения SLA.

### 4.8.3. Рабочая зона «Плагины»



Позволяет подключать сторонние системы для работы в т.ч. с их внутренней бизнес-логикой для выполнения рабочих задач IDM – например, интеграции с ITSM-системами или для выполнения требований регуляторных органов.

#### 4.8.4. Рабочая зона «Автоматические доступы»



Раздел позволяет настраивать связки атрибутов, относящихся к роли, и автоматически предоставлять доступы на их основе.