**ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СИСТЕМЫ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ХРАНЕНИЯ И ВЫДАЧИ ИМУЩЕСТВА**

г. Москва

2024

**ОГЛАВЛЕНИЕ**

[1 ОБЩИЕ СВЕДЕНИЯ 3](#_Toc175167287)

[1.1 Цели создания системы 3](#_Toc175167288)

[1.2 Назначение системы 3](#_Toc175167289)

[2 АРХИТЕКТУРА ПРОЕКТА 3](#_Toc175167290)

[3 ПЕРЕЧЕНЬ ПОДСИСТЕМ, ИХ НАЗНАЧЕНИЕ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ 5](#_Toc175167291)

[3.1 Подсистема авторизации пользователей 5](#_Toc175167292)

[3.2 Подсистема навигации пользователя в боковом меню 5](#_Toc175167293)

[3.3 Подсистема управления данными сервисов 6](#_Toc175167294)

[3.4 Подсистема управления пользователями 9](#_Toc175167295)

[3.5 Подсистема работы с заказами пользователей 11](#_Toc175167296)

[4 ТРЕБОВАНИЯ К РАЗГРАНИЧЕНИЮ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ 14](#_Toc175167297)

[4.1 Требования к контейнеризации 16](#_Toc175167298)

[4.2 Требования к программному обеспечению 17](#_Toc175167299)

[4.3 Требования к техническому обеспечению системы 19](#_Toc175167300)

[5 ТРЕБОВАНИЯ К НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 19](#_Toc175167301)

# ОБЩИЕ СВЕДЕНИЯ

Полное наименование: Программное обеспечение системы автоматизации процессов хранения и выдачи имущества (далее Система).

## Цели создания системы

Система создана с целью автоматизации процессов хранения, выдачи и утилизации предметов

## Назначение системы

Система предназначена для предоставления услуг хранения багажа, личных вещей и предметов пользователей. Веб-сервис позволяет получать данные о заказах, принимать на хранение и выдавать имущество, администрировать учётные записи сотрудников и управлять данными сервисов

# АРХИТЕКТУРА ПРОЕКТА

Система разработана в рамках микросервисной архитектуры с использованием современных технологий и фреймворков для обеспечения эффективности, масштабируемости и удобства в поддержке. Архитектура состоит из следующих ключевых компонентов:

1. Backend (FastAPI):

* Фреймворк FastAPI используется для разработки серверной части приложения, обеспечивает удобное создание API для взаимодействия с Frontend-частью Системы.

1. База данных (PostgreSQL):

* PostgreSQL выбрана в качестве системы управления базами данных для обеспечения высокой надежности и поддержки сложных запросов.
* SQL Alchemy ORM используется для удобного взаимодействия с базой данных, создания моделей данных и выполнения запросов.
* Внедрение миграций Liquibase обеспечивает контроль версий схемы базы данных и упрощает процесс обновления структуры данных.

1. Frontend (ReactJS):

* Frontend разработан с использованием фреймворка ReactJS для создания динамичного пользовательского интерфейса.
* Используются компоненты Material UI для создания модульной структуры приложения.
* Для управления состоянием приложения используется Redux.
* Маршрутизация реализована с использованием React-Router-Dom для навигации по страницам.
* Интерактивные элементы интерфейса обеспечивают приятный пользовательский опыт.

1. Безопасность:

* Аутентификация и авторизация обеспечиваются средствами посредством Keycloack.

1. Контейнеризация:

* Применение Docker-контейнеров для сервисов Системы обеспечивает легкость развертывания, масштабирования и управления зависимостями приложения.
* Openshift используется для управления многоконтейнерными приложениями.

Эта архитектура предоставляет гибкую и масштабируемую основу для развертывания, обеспечивая эффективное взаимодействие между всеми сервисами проекта.

# ПЕРЕЧЕНЬ ПОДСИСТЕМ, ИХ НАЗНАЧЕНИЕ И ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

## Подсистема авторизации пользователей

Подсистема авторизации пользователей представляет собой компонент Системы, который отвечает за управление доступом пользователей к различным ресурсам и функциям. Она обеспечивает проверку прав пользователя на выполнение определённых действий и доступ к информации. Основные функции подсистемы авторизации включают:

1. Аутентификация;
2. Авторизация;
3. Контроль и управление сессиями;
4. Логирование и мониторинг;
5. Интерфейс управления;
6. Интеграция с иными системами (KeyCloack).

Окно авторизации пользователя и его основные элементы *(поле ввода логина и пароля, кнопки входа и смены пароля)* представлены на рисунке 1.

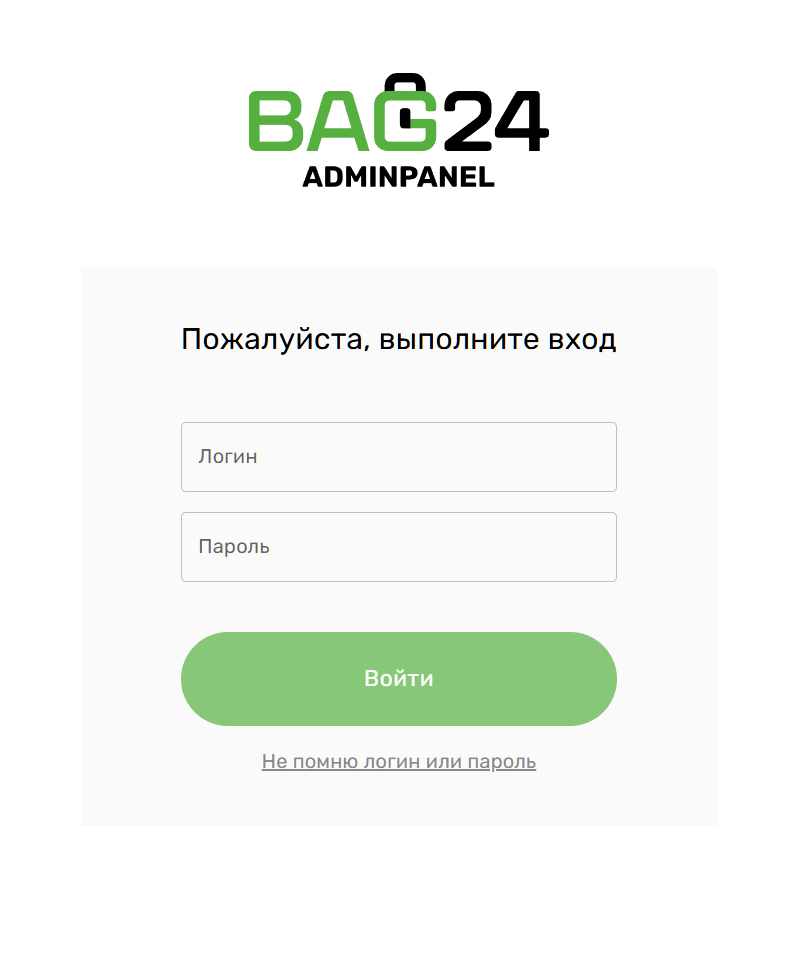


Рисунок 1 – Окно авторизации пользователя

## Подсистема навигации пользователя в боковом меню

Подсистема навигации пользователя в боковом меню позволяет пользователю перемещаться по разделам Системы и представляет собой набор данных о:

1. пользователе;
2. доступных пользователю сервисах (с учетом разграничения доступа);
3. доступных пользователю возможностях управлениями системой (с учетом разграничения доступа).

Интерфейс бокового меню в развернутом (слева) и свернутом (справа) видах представлен на рисунке 2.

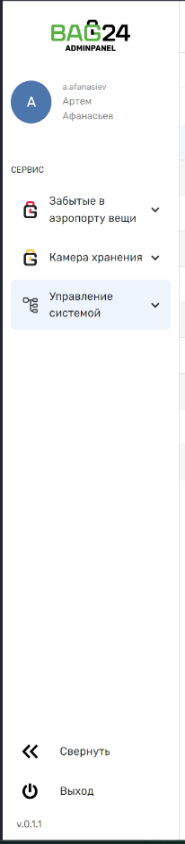


Рисунок 2 – Боковое меню в различных состояниях

## Подсистема управления данными сервисов

После успешной авторизации пользователю в боковом меню необходимо выбрать пункт "Управление системой" → «Управление данными».

Управление данными представляет собой сервис для администрирования сервисов Системы и включает в себя процессы, процедуры и инструменты, используемые для обеспечения надежного и безопасного функционирования информационной системы и обработки данных. Цель управления данными – обеспечение целостности, доступности и конфиденциальности информации.

Интерфейс управления данными представлен на рисунке 3, содержит несколько разделов категории данных (Страны, Города, Аэропорты). Для добавления новых объектов (сущностей) в верхней части страницы раздела категорий данных необходимо найти и нажать кнопку "Добавить". Для редактирования категории данных предназначена кнопка, представленная на рисунке 4, за удаление категории на рисунке 5.

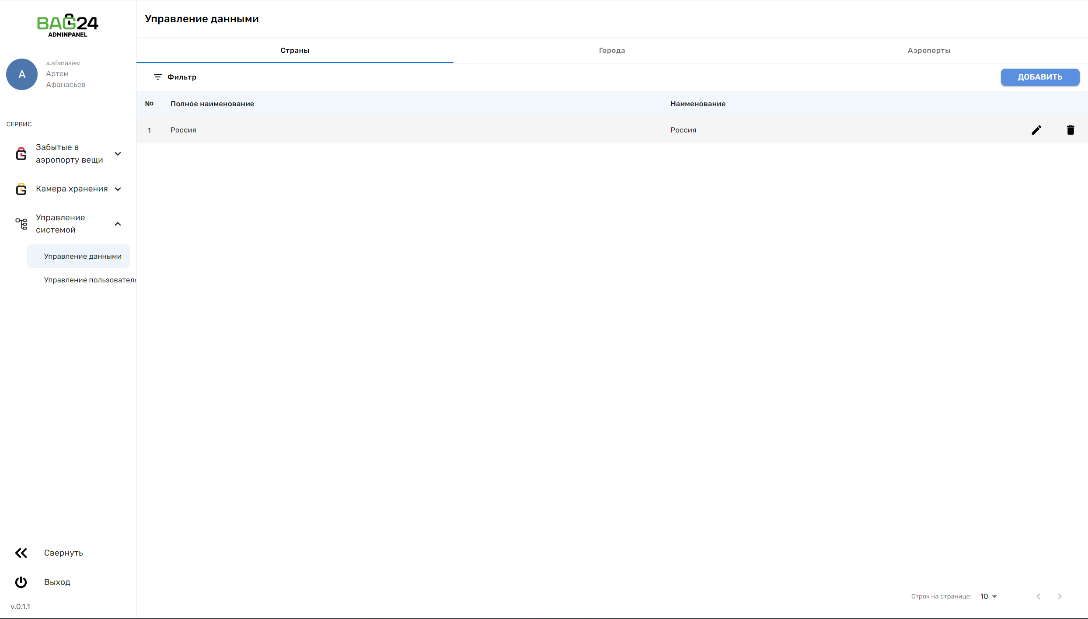


Рисунок 3 – Окно управления данными



Рисунок 4 – Кнопка редактирования



Рисунок 5 – Кнопка удаления

При добавлении новой категории данных появится форма для ввода информации о новой категории данных и редактирования, представленная на рисунках 6а, 6б, 6в.

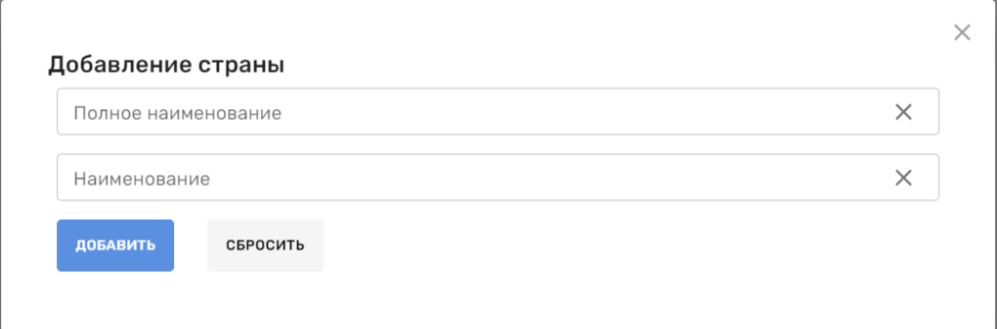


Рисунок 6а – Форма заполнения категории «Страна»



Рисунок 6б – Форма заполнения категории «Город»

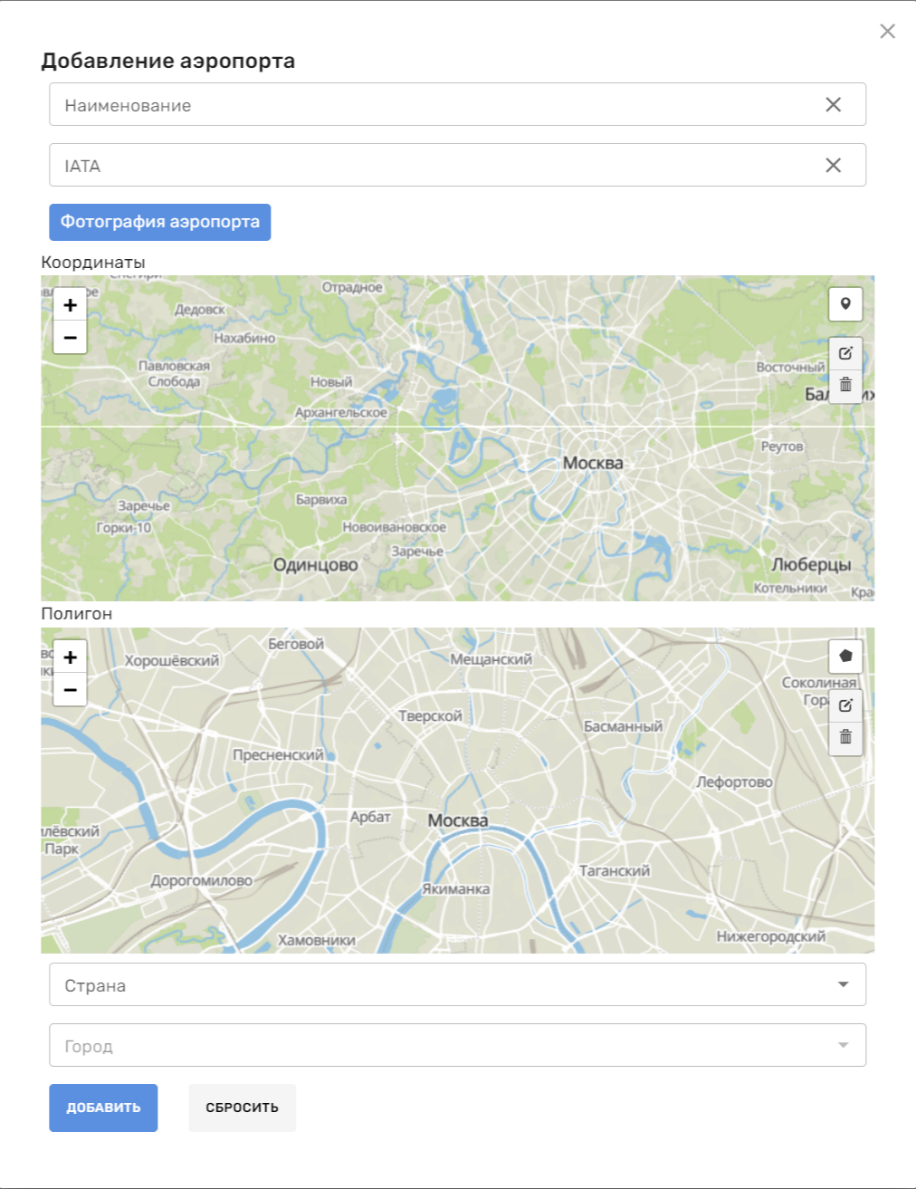


Рисунок 6в – Форма заполнения категории «Аэропорт»

После проверки правильности ввода информации пользователь нажимает на кнопку «Добавить». При необходимости очистить поля ввода данных пользователю необходимо нажать кнопку «Сбросить».

## Подсистема управления пользователями

Для перехода в Подсистему управления пользователями необходимо в боковом меню выбрать пункт "Управление системой" → «Управление пользователями». Подсистема отвечает за управление учетными записями пользователей, контролем доступа и обеспечением безопасности данных в информационной системе.

Основные функции управления пользователями:

1. Регистрация, редактирование и удаление учетных записей пользователей.
2. Аутентификация пользователей.
3. Авторизация и управление правами доступа.
4. Управление паролями.

Интерфейс управления пользователями представлен на рисунке 7 и содержит информацию о пользователях. Для добавления новых пользователей и управления правами доступа в верхней части страницы раздела необходимо найти и нажать кнопку "Добавить".

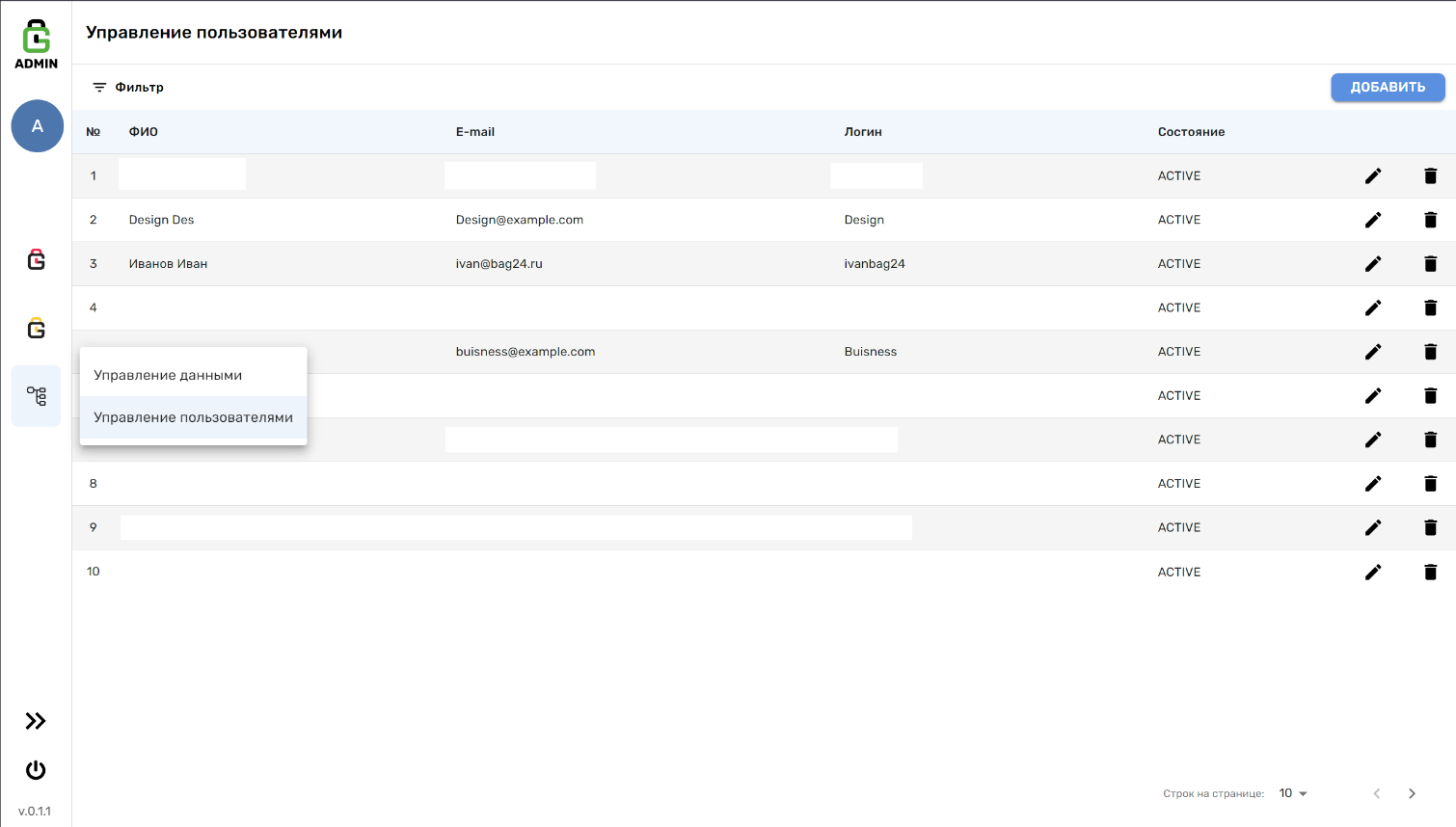


Рисунок 7 – Окно управления пользователями

Перечень данных их описание и функциональные возможности, указанных на странице «Управление пользователями» представлены в таблице № 1.

Таблица № 1 – Данные пользователей

|  |  |  |  |
| --- | --- | --- | --- |
| Сервис | Параметры сущности | Примечание | Возможности |
| Управление пользователями админ панели | ФИО | До 250 символов | Добавление / Изменение / Удаление\* |
| EMAIL | Валидация по латинским буквам и специальным символам |
| Логин | Уникально |
| Состояние | Активен (ACTIVE), если пользователь неактивен (INACTIVE), то не отображается системой |

При добавлении нового пользователя появится форма для ввода информации, представленная на рисунке 8.



Рисунок 8 – Форма добавления пользователя

При заполнении вышеуказанной формы следует учитвать требования к данным, заполняемым в соответствующих полях, которые представлены в таблице № 2.

Таблица № 2 – Требования к данным пользователя

|  |  |
| --- | --- |
| ФИО | До 250 символов |
| EMAIL | Валидация по латинским буквам и специальным символам |
| Логин | До 250 символов |
| Пароль | Требования к регистру (одна буква в верхнем регистре минимум), не менее 8 символов и один специальный символ |
| Права доступа | Выдаются в соответствии с ролью пользователя |

После проверки правильности ввода информации пользователь нажимает на кнопку «Добавить» если все поля заполонены корректно и кнопку «Сбросить» если необходимы правки.

После успешного добавления и корректности ввода данных новый в Системе отобразится новый пользователь с выданными правами доступа.

## Подсистема работы с заказами пользователей

Подсистема работы с заказами в аэропорту предоставляет пассажирам услугу временного безопасного хранения их багажа и продления срока хранения   
(с возможностью оплаты через мобильные устройства), упаковки, обеспечивая удобство и защиту на протяжении всего периода хранения и включает несколько ключевых компонентов и этапов работы:

* + - 1. Прием багажа на хранение
      2. Регистрация багажа
      3. Хранение багажа
      4. Выдача багажа
      5. Продление хранения:

5.1 Пассажир может продлить срок хранения, оплатив дополнительное время.

5.2 Информация об обновленном сроке хранения заносится в систему.

Преимущества для пассажиров:

* удобство и экономия времени, в частности, при долгих пересадках или транзитах.
* возможность безопасного хранения багажа на время пребывания в городе.
* гибкость и дополнительные опции для различных потребностей пассажиров.

Таким образом подсистема по хранению багажа обеспечивает удобство, безопасность и иные возможности для пассажиров, что делает путешествие более комфортным и менее стрессовым.

Для перехода в Подсистему «работы с заказами» необходимо в боковом меню выбрать пункт "Камера хранения" → «Заказы», после чего откроется интерфейс главной страницы с таблицей заказов, представленный на рисунке 9.

***Примечание:*** *Список отображаемых элементов может отличаться в зависимости от роли пользователя в соответствии с правилами разграничения доступа.*

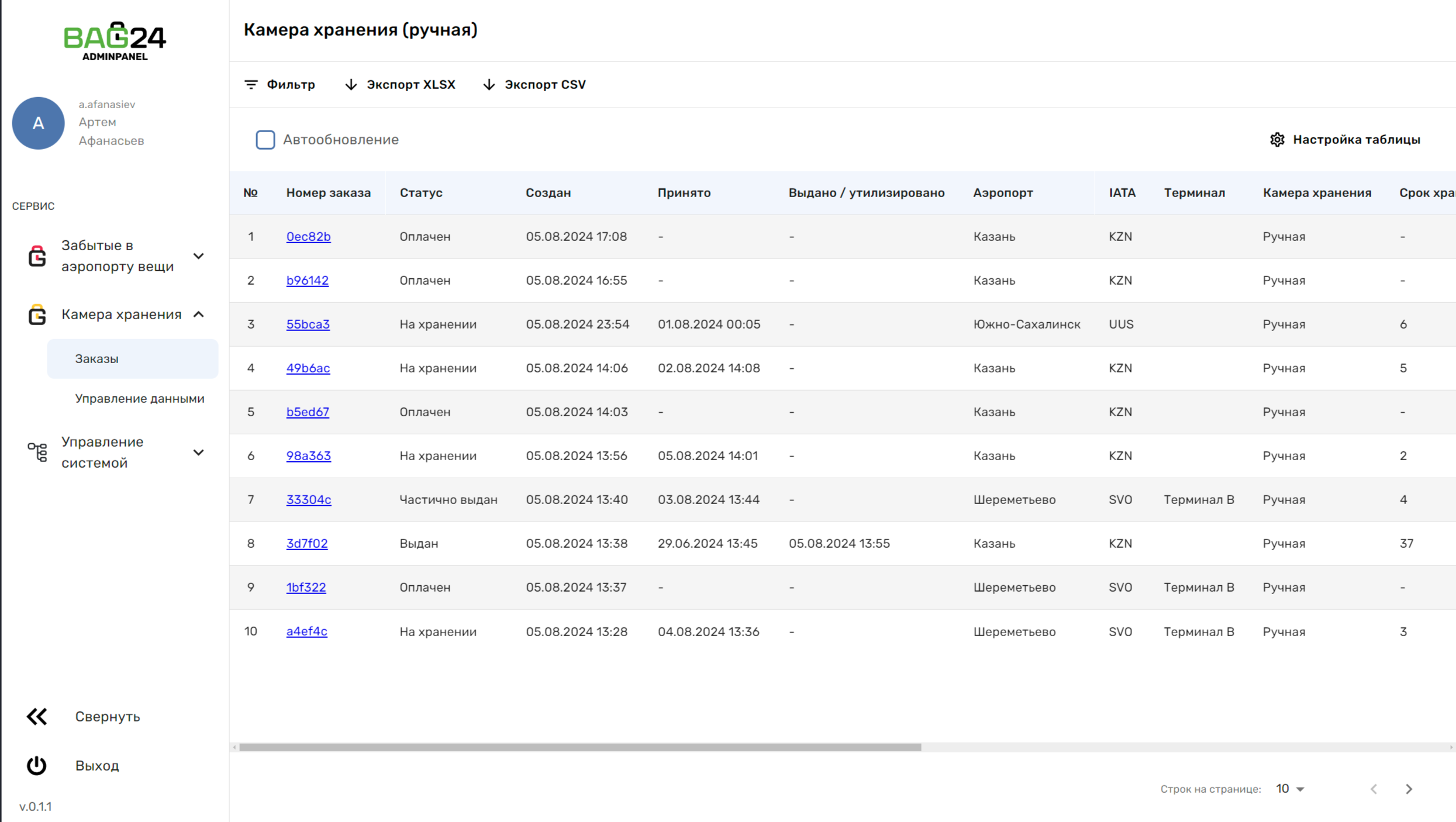


Рисунок 9 – Окно работы с заказами

Раздел подсистемы предназначен для выполнения следующих задач:

- просмотр истории операций с заказами;

- просмотр истории операций оплаты заказа;

- просмотр остатка имущества, находящего на хранении в КХ.

В целях обеспечения функциональности подсистемы существует раздел «Управление данными», для перехода в который необходимо выбрать соответствующий пункт в боковом меню. Интерфейс данного раздела представлен на рисунке 10 и содержит несколько категорий данных – «Камера хранения», «Тарифы», а также «Push-уведомления». Раздел «Push-уведомления» обеспечивает возможность отправки уведомлений клиентам. Для добавления новых объектов (сущностей) в верхней части страницы раздела категорий данных необходимо нажать кнопку "Добавить".

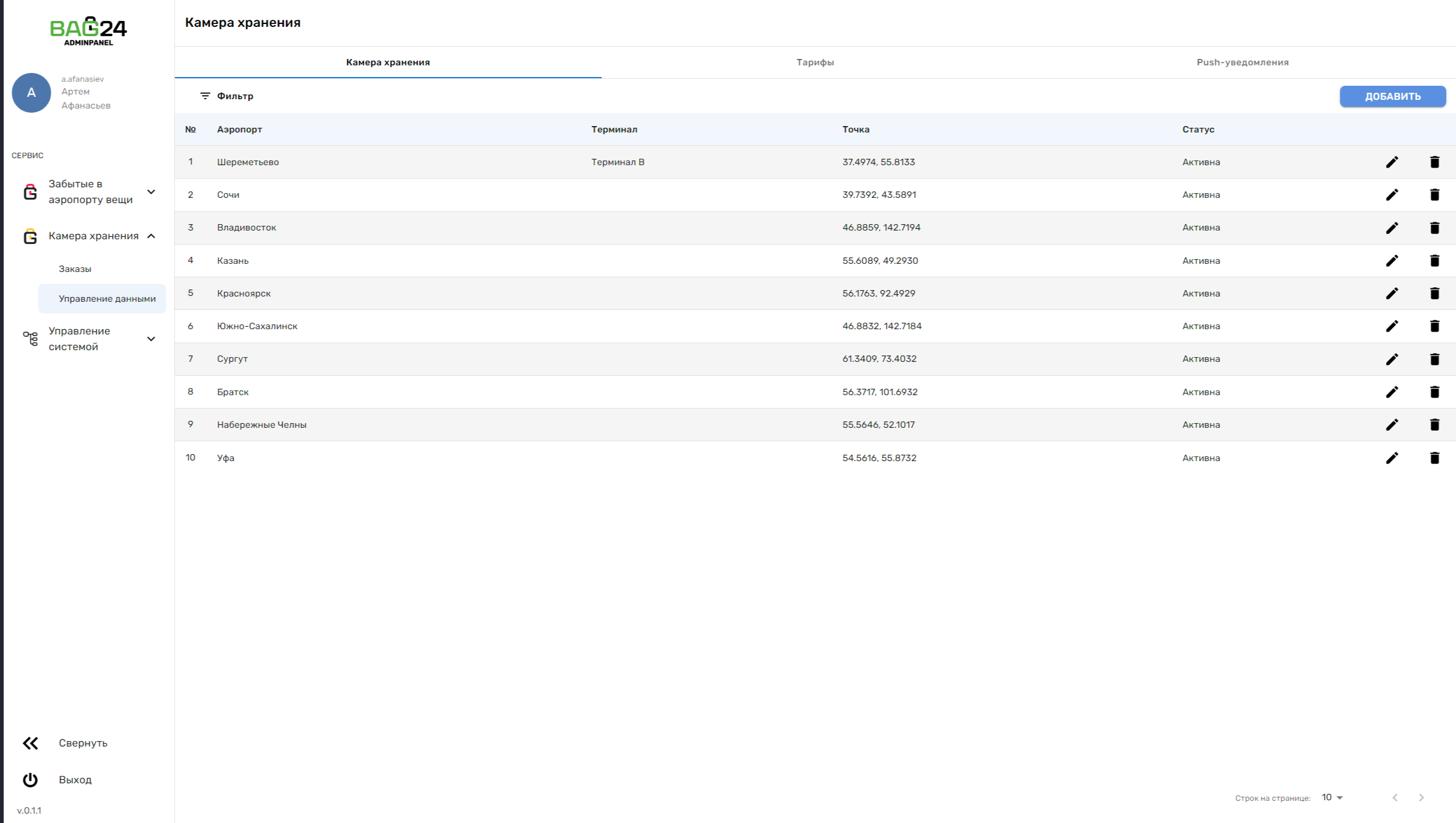


Рисунок 10 – Окно «Управления данными» подсистемы работы с заказами

Перечень данных, описание и функциональные возможности подсистемы работы с заказами представлены в таблице № 3.

Таблица № 3 – Работа с заказами

|  |  |  |  |
| --- | --- | --- | --- |
| Сущность | Параметры сущности | Примечание к значению | Возможности |
| Камера хранения | Аэропорт | Уникально | Добавление / Изменение / Удаление\* |
| Терминал | Уникально в рамках аэропорта |
| API-key (ключ доступа к кассовому оборудованию и КХ) | Требования к регистру (одна и более буква в верхнем регистре), не менее 16 и специальные символы |
| Фотография КХ | В формате JPG, PGEG, PNG, HEIC для мобильных устройств Apple |
| Точка | В формате WGS84 |
| Статус | Активна (если не активна, то не отображается) |
| Тарифы | Наименование | Уникально | Добавление / Изменение / Удаление\* |
| Описание | До 250 символов |
| Стоимость 1 суток | Только цифры (в копейках) |
| Стоимость продления | Только цифры (в копейках) |
| Аэропорт | Выбор из ранее добавленных |
| Терминал | Выбор из ранее добавленных |
| Push-уведомления | Дата и время | В формате дд.мм.гг | Отправка текста и эмодзи |
| Заголовок | До 250 символов |
| Текст уведомления | До 250 символов |

# ТРЕБОВАНИЯ К РАЗГРАНИЧЕНИЮ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ

В Системе доступны следующие роли:

* + - * **Владелец бизнеса** – пользователь системы с функциями управления данными, выдачи доступов сотрудникам, а также просмотра сведений о заказе в рамках **всех сервисов** в пределах **всех аэропортов**. Обладает следующими правами в Системе:

1. Управление доступов сотрудников;
2. Просмотр истории операций с заказами;
3. История операций по оплате заказа;
4. Возможность фильтрации;
5. Выгрузка отчетов (в csv/xlsx форматах).

***Примечание****: с учетом вышеуказанных ограничений по зоне ответственности*

* + - * **Управляющий** – пользователь системы с функциями управления данными, выдачи доступов сотрудникам, а также просмотра сведений о заказе в рамках **одного** или **нескольких** **сервисов** в пределах **одного или нескольких аэропортов**. Обладает следующими правами в Системе:

1. Управление доступов сотрудников;
2. Просмотр истории операций с заказами;
3. Просмотр истории операций по оплате;
4. Возможность фильтрации;
5. Выгрузка отчетов (в csv/xlsx форматах).

***Примечание****: с учетом вышеуказанных ограничений по зоне ответственности*

* + - * **Администратор** – пользователь системы с функциями управления данными, выдачи доступов сотрудникам, а также просмотра сведений о заказе в рамках **одного** или **нескольких** **сервисов** в пределах **одного аэропорта**. Обладает следующими правами в Системе:

1. Управление доступов сотрудников;
2. Просмотр истории операций с заказами;
3. Просмотр истории операций по оплате;
4. Возможность фильтрации сущностям;
5. Выгрузка отчетов (в csv/xlsx форматах).

***Примечание****: с учетом вышеуказанных ограничений по зоне ответственности*

* + - * **Представитель аэропорта –** пользователь системы с функциями просмотра сведений о заказе в рамках одного или нескольких **сервисов** в пределах **одного или нескольких** аэропортов. Обладает следующими правами в Системе:

1. Установка статуса работы КХ.
2. Просмотр истории операций с заказами.
3. Просмотр истории операций по оплате.
4. Возможность фильтрации.
5. Выгрузка отчетов (в csv/xlsx форматах).

Для данной роли в Web-панели отсутствуют столбцы с персональными данными пассажиров, а также отсутствует функционал по дабл-клику.

**ТРЕБОВАНИЯ К СЕРВЕРНОЙ ИНФРАСТРУКТУРЕ**

## Требования к контейнеризации

Контейнеризация приложений в OpenShift требует соблюдения ряда принципов и стандартов, чтобы гарантировать эффективную работу и управление контейнерами. Вот основные требования:

1. Изоляция приложений: Контейнеры должны быть изолированы друг от друга и от хост-системы.

2. Использование образов контейнеров: Приложения должны быть упакованы в образы контейнеров, которые могут быть созданы с использованием Dockerfile или других инструментов сборки. Эти образы должны быть доступны в реестре контейнеров.

3. Поддержка многопоточности и масштабируемости: Приложения должны быть спроектированы для работы в распределенной среде, что включает возможность горизонтального масштабирования.

4. Сетевые настройки: Приложения должны использовать сетевые политики OpenShift для управления сетевым трафиком и обеспечения безопасности.

5. Хранение данных: для хранения данных необходимо использовать постоянные тома (Persistent Volumes) и соответствующие классы хранения (Storage Classes).

6. Мониторинг и логирование: Приложения должны быть настроены для интеграции с системами мониторинга и логирования, такими как Prometheus и Elasticsearch.

7. Безопасность: следует учитывать безопасность на всех уровнях, включая использование Security Contexts, ограничение прав доступа и применение политик безопасности.

8. Конфигурация и секреты: Конфигурационные данные и секреты должны храниться в ConfigMaps и Secrets соответственно, чтобы обеспечить безопасное управление конфиденциальной информацией.

9. CI/CD интеграция: рекомендуется интегрировать приложения с CI/CD пайплайнами для автоматизации сборки, тестирования и развертывания.

10. Соблюдение стандартов и практик DevOps: важно следовать лучшим практикам DevOps при разработке, развертывании и управлении приложениями.

Соблюдение этих требований поможет обеспечить стабильную и безопасную работу приложений в среде OpenShift.

## Требования к программному обеспечению

Требования к программному обеспечению для хранения багажа и вещей в аэропортах:

1. Введение

Программное обеспечение (ПО) для хранения багажа и вещей в аэропортах должно обеспечивать безопасность, эффективность и удобство управления процессами хранения. Оно должно быть способно обрабатывать различные типы багажа, предоставлять актуальную информацию и интегрироваться с другими системами аэропорта.

2. Функциональные требования

2.1. Регистрация и идентификация багажа

- Осмотр: осмотр багажа на предмет запрещенных веществ.

- Выдача квитанций: автоматическая выдача квитанций пассажирам при сдаче багажа.

- Фотографирование багажа: система должна поддерживать фотографирование багажа для фиксации его состояния при приеме.

2.2. Хранение и отслеживание багажа

- Местоположение: учет местоположения каждого багажа в системе хранения.

- Уведомления: автоматические уведомления для сотрудников о необходимости перемещения или выдачи багажа.

- Статус хранения: отслеживание статуса багажа (например, сдан, на хранении, готов к выдаче, выдан).

2.3. Управление доступом и безопасностью

- Права доступа: Разграничение прав доступа для различных категорий пользователей.

- Журналирование действий: Ведение журнала всех действий пользователей для последующего аудита.

- Шифрование данных: Шифрование данных о багаже для обеспечения конфиденциальности.

2.4. Интеграция с другими системами

- Интеграция с системами аэропорта: Взаимодействие с системами управления рейсами, системами безопасности и другими релевантными системами.

- API: Наличие API для интеграции с внешними системами и сервисами.

2.5. Пользовательский интерфейс

- Удобство использования: интуитивно понятный интерфейс для сотрудников КХ и клиентов.

- Многоязычность: поддержка нескольких языков для удобства иностранных пассажиров.

- Мобильное приложение: возможность использования мобильного приложения для сотрудников и клиентов.

3. Нефункциональные требования

3.1. Производительность

- Скорость обработки: быстрая регистрация и обработка информации о багаже.

- Масштабируемость: способность системы обрабатывать большое количество багажа в периоды пиковых нагрузок.

3.2. Надежность и отказоустойчивость

- Резервное копирование: регулярное резервное копирование данных.

- Восстановление после сбоев: способность системы быстро восстанавливаться после сбоев.

3.3. Безопасность

- Защита данных: защита данных от несанкционированного доступа и утечки.

- Аутентификация и авторизация: надежные механизмы аутентификации и авторизации пользователей.

3.4. Поддержка и обслуживание

- Техническая поддержка: круглосуточная поддержка пользователей системы.

- Обновления и улучшения: регулярные обновления ПО для улучшения функциональности и безопасности.

## Требования к техническому обеспечению системы

Система должна поддерживать типовые конфигурации программно-аппаратных комплексов, которые включают различные технические решения для хранения, обработки, передачи и защиты данных.

Подрядчик должен определить состав, схему подключения и конфигурации технических средств, которые будут согласованы с Заказчиком при проектировании и разработке системы.

Проведение развертывания среды в инфраструктуре, предоставленной и сконфигурированной Заказчиком, включает:

* конфигурацию серверов и сетевого оборудования;
* конфигурацию системного программного обеспечения;
* конфигурацию сервисов администрирования для управления правами доступа.

Подрядчик должен:

1. Установить разработанное программное обеспечение на технические средства Заказчика.
2. Выполнить настройку программного обеспечения.
3. Выполнить частичное наполнение Системы тестовыми данными для наглядной визуализации процесса обучения.
4. Обеспечить доступ к Системе.

# ТРЕБОВАНИЯ К НАДЕЖНОСТИ И БЕЗОПАСНОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Требования к надежности технических средств и программного обеспечения включают в себя несколько аспектов, целью которых является обеспечение стабильности и бесперебойной работы системы, а именно:

1. Доступность: системы должны быть доступны пользователям в любое время, согласно установленным уровням обслуживания (SLA). Это включает в себя минимизацию времени простоя.

2. Отказоустойчивость: системы должны быть спроектированы так, чтобы продолжать функционировать даже в случае сбоев отдельных компонентов. Это может включать резервирование, дублирование и автоматическое переключение на резервные системы.

3. Устойчивость к нагрузке: программное обеспечение должно быть способно обрабатывать ожидаемую и даже повышенную нагрузку без снижения производительности.

4. Поддержка и обслуживание: надежные системы должны иметь возможность для легкого обновления, исправления ошибок и масштабирования без значительных перебоев в работе.

5. Тестирование и валидация: тестирование (включая нагрузочные и стресс-тесты) должно проводиться для выявления потенциальных проблем до их появления в рабочей среде.

Требования к безопасности включают в себя следующие основные пункты:

1. Аутентификация и авторизация: необходимо обеспечить надежные механизмы аутентификации пользователей и контроля доступа к системам и данным.

2. Шифрование данных: данные должны быть защищены как в состоянии покоя, так и при передаче. Использование протоколов шифрования (например, TLS) является обязательным.

3. Защита от угроз: системы должны иметь средства защиты от различных угроз, таких как вирусы, вредоносное ПО, атаки DDoS и другие виды кибератак.

4. Мониторинг и аудит: необходимо внедрить системы мониторинга для отслеживания подозрительной активности и ведения журналов для последующего анализа.

5. Обновления и патчи: регулярное применение обновлений безопасности и исправлений для программного обеспечения и операционных систем.

6. Обучение пользователей: пользователи должны быть обучены основам безопасности, включая распознавание фишинга и безопасное использование систем.

7. Политики безопасности: разработка и внедрение документированных политик безопасности, которые определяют правила и процедуры для защиты информации.

8. Резервное копирование данных: регулярное создание резервных копий критически важных данных для обеспечения их восстановления в случае потери или повреждения.

Соблюдение этих требований поможет обеспечить как надежность, так и безопасность технических средств и программного обеспечения, что, в свою очередь, повысит доверие пользователей и снизит риски для бизнеса.