ЦИФРОВЫЕ ТЕРРИТОРИИ

ООО «Цифровые территории»
Юридический адрес: Московская область, Г.О. Дубна,
г Дубна, ул Программистов, д 4, стр.4, офис 226
info@it-dt.ru www.it-dt.ru ИНН: 5010061548

РУКОВОДСТВО АДМИНИСТРАТОРА

Система ГеоБИМ.

Цифровой двойник территорий и объектов капитального строительства.

2026

Аннотация

Настоящий документ предназначен для организации и выполнения работ по развертыванию, настройке, сопровождению и восстановлению работоспособности Системы «ГеоБИМ. Цифровой двойник территорий и объектов капитального строительства» (далее – «ГеоБИМ»). В документе описаны действия администратора при подготовке окружения, запуске сервисов, настройке доступа, управлении слоями и источниками данных, использовании аналитических функций, резервном копировании и действиях в аварийных ситуациях.

Документ состоит из следующих разделов:

– раздел «Общие сведения» содержит сведения об области применения, описании возможностей, уровне подготовки администратора и перечне эксплуатационной документации;

– раздел «Назначение и условия применения» содержит сведения о назначении системы, ее компонентах и условиях эксплуатации;

– раздел «Подготовка к работе» содержит сведения о составе дистрибутива, предварительных требованиях, настройке окружения и порядке проверки работоспособности;

– раздел «Описание операций» содержит сведения о штатных административных операциях, конфигурации, мониторинге, архивировании и резервном копировании;

– раздел «Аварийные ситуации» содержит описание основных отказов и действий администратора по локализации и восстановлению;

– раздел «Рекомендации по освоению» содержит рекомендуемые действия для освоения задач системного администрирования Системы «ГеоБИМ».

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ....3
1 ОБЩИЕ СВЕДЕНИЯ....5
1.1 Наименование системы....5
1.2 Область применения....5
1.3 Краткое описание возможностей....5
1.4 Уровень подготовки пользователей....6
1.5 Перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю....6
2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ....7
2.1 Назначение....7
2.2 Компоненты Системы....7
2.3 Условия применения....7
3 ПОДГОТОВКА К РАБОТЕ....8
3.1 Состав и содержание дистрибутивного носителя данных....8
3.2 Порядок загрузки данных и программ....8
3.3 Порядок проверки работоспособности....11
4 ОПИСАНИЕ ОПЕРАЦИЙ....14
4.1 Операции в рамках Системы....14
4.2 Общесистемные задачи и процедуры администрирования....17
5 АВАРИЙНЫЕ СИТУАЦИИ....20
5.1 Отказ в доступе....20
5.2 Не загружается главная страница....20
5.3 Действия в случае несоблюдения условий выполнения технологического процесса, в том числе при длительных отказах технических средств....20
5.4 Действия по восстановлению программ и/или данных при отказе магнитных носителей или обнаружении ошибок в данных....20
5.5 Действия в случаях обнаружении несанкционированного вмешательства в данные....20
5.6 Действия в других аварийных ситуациях....20
5.7 Backend не запускается после обновления версии....21
5.8 Backend завершается с сигналом «Illegal instruction»....21
6 РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ....24

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и основные понятия области автоматизированных систем определены в ГОСТ Р 59853-2021 «Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения». Также в настоящий документ введены следующие термины и специальные сокращения на русском и английском языках (Таблица 1).

Таблица 1 – Перечень принятых терминов и сокращений

Термин	Значение
Администратор	Пользователь, выполняющий настройку, сопровождение и контроль работоспособности GeoBIM.
АРМ	Автоматизированное рабочее место администратора или конечного пользователя системы.
API	Программный интерфейс backend-сервиса GeoBIM, доступный по HTTP.
GeoBIM	Геоинформационная Система для работы с картой, слоями, аналитикой и 3D-объектами.
Backend	Серверное приложение на FastAPI, реализующее бизнес-логику и API системы.
Frontend	Клиентское веб-приложение на Angular 21.
Docker Compose	Средство оркестрации контейнеров, используемое для штатного развертывания системы.
Gateway	Контейнер Nginx, проксирующий frontend, backend и Keycloak.
Keycloak	Провайдер аутентификации и управления пользователями/realm системы.
PostgreSQL, Postgres pro/PostGIS	СУБД и расширение пространственных данных, используемые GeoBIM.
Слой	Логическая единица пространственных данных, отображаемая на карте.
Каталог слоев	Иерархическая структура папок и слоев, отображаемая в интерфейсе.
Источник данных	Описанный в системе набор полей и геометрии для создания и наполнения слоя.

Термин	Значение
Seed-профиль	Набор стартовых данных и конфигурации, применяемый при первичном развертывании.
GLTF/GLB	Форматы 3D-моделей, поддерживаемые для загрузки в GeoBIM.
Дашборд	Набор виджетов для визуализации показателей по данным слоев.
Аудит	Журнал действий пользователей и история изменения объектов/прав доступа.

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Наименование системы

Полное наименование Системы: Система «ГеоБИМ».

Условное обозначение Системы: Система.

1.2 Область применения

Настоящее Руководство администратора предназначено для специалистов, выполняющих развертывание, эксплуатацию, сопровождение и восстановление работоспособности Системы GeoBIM.

Документ содержит набор правил и инструкций по работе с инфраструктурными и прикладными компонентами системы, а также описание операций, выполняемых в административном интерфейсе.

1.3 Краткое описание возможностей

Система «ГеоБИМ» обеспечивает выполнение технологических процессов сбора, хранения, обработки, публикации и анализа пространственных данных, в том числе:

- отображение 2D- и 3D-данных на веб-карте с использованием MapLibre GL JS;
- ведение иерархического каталога слоев и папок;
- импорт геоданных из форматов SHP, GeoJSON, JSON, TAB, GPKG, KML, GML, DWG и DXF;
- создание, редактирование и удаление объектов слоя, а также изменение их геометрии;
- ведение истории изменений объектов и журнала аудита действий пользователей;
- управление внешними картографическими источниками и загрузка 3D-моделей GLTF/GLB;
- администрирование пользователей, ролей, feature-флагов и матрицы прав на слои;
- построение дашбордов и выполнение AI-аналитики с доступом к БД только на чтение;
- экспорт и импорт конфигурации слоев и каталога для переноса между инстансами.

1.4 Уровень подготовки пользователей

Для успешной работы с системой администраторы должны обладать базовыми навыками работы с персональным компьютером, интернет-браузером и средствами информационной безопасности.

Системные администраторы должны обладать знаниями и навыками администрирования ОПО и ППО, включая:

- операционные системы Linux, macOS или Windows в части эксплуатации Docker;
- Docker Engine и Docker Compose v2;
- PostgreSQL, Postgres Pro и основы резервного копирования баз данных;
- Keycloak и общие принципы OIDC/RBAC;
- Nginx и проксирование HTTP-трафика;
- работу с логами контейнеров, переменными окружения и JSON-конфигурацией.

Системные администраторы должны:

- уметь выполнять резервное копирование и восстановление данных;
- проводить первичную диагностику недоступности сервисов по логам и HTTP-проверкам;
- проверять корректность прав доступа пользователей и ролей в административном интерфейсе.

1.5 Перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю

Перед эксплуатацией системы администратору необходимо ознакомиться с настоящим документом.

Дополнительно рекомендуется использовать официальную документацию производителей следующего ПО:

- Docker Engine и Docker Compose;
- PostgreSQL, Postgres Pro и расширение PostGIS;
- Keycloak;
- FastAPI и SQLAlchemy;
- Angular CLI и Node.js;
- Nginx;
- MapLibre GL JS;
- Fiona/GDAL и Shapely для работы с геоданными.

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1 Назначение

Система предназначена для автоматизации хранения, публикации, редактирования, анализа и визуализации пространственных данных в двухмерном и трехмерном представлении.

Система в текущем составе обеспечивает следующие функциональные возможности:

- доступ к карте, слоям и аналитике через единый веб-интерфейс;
- управление каталогом слоев, справочниками источников данных и 3D-моделями;
- разграничение прав доступа по ролям и feature-флагам;
- подготовку и экспорт дашбордов, а также экспорт/импорт конфигурации инстанса.

2.2 Компоненты Системы

Компоненты Системы:

- модуль пользовательского интерфейса – Angular 21 SPA;
- серверное приложение – FastAPI + SQLAlchemy (async);
- подсистема хранения данных – PostgreSQL, Postgres Pro 16 + PostGIS 3.4;
- подсистема аутентификации и авторизации – Keycloak (OIDC/RBAC);
- веб-шлюз – Nginx gateway;
- профили развертывания и стартовые seed-данные;
- опциональная AI-интеграция с Yandex Foundation Models.

2.3 Условия применения

Система разворачивается на узле, где установлены Docker Engine и Docker Compose v2. Для штатного запуска должны быть свободны порты 80 (gateway), 4200 (frontend), 5432 (PostgreSQL, Postgres Pro) и 8080 (Keycloak). Значения переопределяются переменными окружения согласно таблице 6.

Клиентское веб-приложение системы функционирует в следующих браузерах:

- Яндекс.Браузер и иные Chromium-совместимые браузеры актуальной стабильной версии;
- Microsoft Edge актуальной стабильной версии;
- Mozilla Firefox актуальной стабильной версии;
- Safari 16 и выше.

3 ПОДГОТОВКА К РАБОТЕ

3.1 Состав и содержание дистрибутивного носителя данных

Для эксплуатации Системы на автоматизированных рабочих местах пользователей установка дополнительного программного обеспечения не требуется; достаточно поддерживаемого браузера и сетевого доступа к инстансу системы.

Дистрибутив включает директории backend, frontend, infra, deploy, а также docker-compose.yml и файлы шаблонов переменных окружения .env.example и backend/.env.example.

3.2 Порядок загрузки данных и программ

Для функционирования системы требуется общесистемное и прикладное программное обеспечение, указанное в таблице 2.

Таблица 2 – Общесистемное и прикладное программное обеспечение системы

Оборудование	**Вид ПО**	**Программный продукт**
Серверное оборудование	Контейнерная среда	Docker Engine, Docker Compose v2
Серверное оборудование	СУБД	PostgreSQL, Postgres Pro 16 + PostGIS 3.4
Серверное оборудование	Провайдер идентификации	Keycloak 24.0.5, образ собственной сборки на базе debian:bookworm-slim и OpenJDK 17
Серверное оборудование	Веб-шлюз	nginx:bookworm (Debian 12)
Серверное оборудование	Backend API	Python 3.12, FastAPI, SQLAlchemy, Alembic
Серверное оборудование	Frontend SPA	Node.js 24, Angular 21, MapLibre GL JS, TerraDraw
Внешняя интеграция	AI-аналитика	Yandex Foundation Models API (опционально)

Для установки системы необходимо подготовить следующую инфраструктуру:

- хост с установленными Docker Engine и Docker Compose v2;
- доступные сетевые порты для gateway, frontend, PostgreSQL, Postgres Pro и Keycloak;
- тома хранения для данных PostgreSQL, Postgres Pro и Keycloak;

– учетные данные Yandex Cloud, если требуется AI-аналитика.

3.2.1 Подготовка Docker-хоста

Установка Docker Engine и Docker Compose v2 выполняется в соответствии с документацией производителя. Перед запуском рекомендуется убедиться в отсутствии конфликтов по портам и наличии свободного места на дисках.

– cp .env.example .env

В корневом файле .env задаются COMPOSE_PROJECT_NAME, GATEWAY_PORT, FRONT_PORT, DB_PORT, KEYCLOAK_PORT, SEED_PROFILE и параметры AI-аналитики. Назначение и значения по умолчанию приведены в таблице 6.

3.2.2 Настройка переменных окружения

Корневой файл .env используется docker-compose.yml и является основным местом конфигурации для штатного запуска.

Значение GATEWAY_PORT по умолчанию изменено с 82 на 80. При конфликте портов значения переопределяются в корневом файле .env; одновременное развертывание нескольких стендов выполняется комбинацией уникальных портов и COMPOSE_PROJECT_NAME.

Файл backend/.env применяется только при локальном запуске backend вне Docker и может содержать DATABASE_READONLY_URL и переменные Yandex Cloud.

– cp backend/.env.example backend/.env

Пароли учетных записей СУБД и администратора Keycloak заданы в docker-compose.yml. До передачи в эксплуатацию требуется перенос значений в защищенный файл переменных окружения и ротация паролей.

3.2.3 Запуск контейнеров и инициализация базы данных

При запуске backend entrypoint ожидает готовность PostgreSQL, Postgres Pro, применяет миграции Alembic и, если задан SEED_PROFILE, выполняет загрузку стартовых данных. Ревизия 001_initial рассчитана на пустую базу данных; перед первым запуском необходимо выполнить требования пункта 3.2.8. Порядок сборки образа Keycloak приведен в пункте 3.2.7.

– docker compose up -d --build

– docker compose ps

В базе создаются схемы auth и audit, прикладные таблицы слоев, объектов, ролей, дашбордов, журналов действий и история AI-аналитики.

3.2.4 Настройка профиля развертывания

Для брендирования и начальной карты используется файл frontend/public/assets/config.json. Допускается копирование готового профиля из каталога deploy/<profile>/config.json.

– cp deploy/geobim/config.json frontend/public/assets/config.json

Если требуется собственный профиль, необходимо подготовить конфигурацию фронтенда и, при необходимости, реализовать backend/seeds/<profile>.py с добавлением имени профиля в backend/seeds/__main__.py.

3.2.5 Настройка AI-аналитики

Для включения AI-аналитики в .env необходимо указать YANDEX_FOLDER_ID и YANDEX_API_KEY. Дополнительно может быть задан YANDEX_MODEL; по умолчанию используется yandexgpt/rc.

Пользователь также может временно указать собственные значения ключа и Folder ID в интерфейсе модуля AI-аналитики; такие значения хранятся только в sessionStorage браузера.

3.2.6 Локальный запуск backend вне Docker (опционально)

При локальной отладке backend без Docker используется backend/.env, а приложение запускается как uvicorn app.main:app. Данный режим не заменяет штатный сценарий docker compose.

3.2.7 Сборка образа провайдера идентификации

Образ Keycloak не загружается из внешнего реестра, а собирается на узле развертывания из infra/keycloak/Dockerfile. Основой образа является debian:bookworm-slim с пакетом openjdk-17-jre-headless; официальный дистрибутив Keycloak 24.0.5 загружается с github.com с резервным источником repo1.maven.org, после чего выполняется обязательная проверка контрольной суммы SHA1. Служба запускается от непривилегированного пользователя с UID 1000.

При подготовке узла необходимо учитывать следующие требования:

– на время сборки узлу требуется сетевой доступ к github.com либо к repo1.maven.org;

– образ тегируется как geobim-keycloak:24.0.5 и во внешних реестрах отсутствует, поэтому команда docker compose pull возвращает по нему ошибку; это не является отказом и не препятствует запуску;

– при изменении infra/keycloak/Dockerfile образ необходимо пересобрать явно.

– docker compose up -d --build keycloak

В контуре без доступа к сети общего пользования адрес дистрибутива переопределяется аргументом сборки на внутреннее зеркало:

– docker compose build --build-arg KEYCLOAK_DIST_URL=https://<зеркало>/keycloak-24.0.5.tar.gz keycloak

3.2.8 Требование пустой базы данных при первичном запуске

История миграций сведена к единственной ревизии 001_initial, которая создает схему целиком: расширения postgis и btree_gist, схемы auth и audit, прикладные таблицы, индексы и роли только для чтения. Обновление баз данных, созданных предыдущими версиями Системы, данной ревизией не поддерживается.

Перед первым запуском новой версии на узле, где ранее разворачивались предыдущие версии, необходимо подтвердить отсутствие ценных данных либо снять резервную копию согласно пункту 4.2.5, затем удалить тома данных и выполнить повторное развертывание:

– docker compose down -v

– docker compose up -d --build

Признак нарушения этого требования: контейнер backend завершается с кодом 255, в журнале присутствует запись «Can't locate revision identified by '036'», при этом контейнеры gateway, frontend, keycloak и db остаются в состоянии Up. Порядок действий приведен в пункте 5.7.

При восстановлении из резервной копии дамп разворачивается в пустую базу данных, после чего повторный запуск ревизии не требуется — версия схемы содержится в самом дампе.

3.3 Порядок проверки работоспособности

3.3.1 Диагностирование и контроль работоспособности инфраструктурных сервисов

Проверка Docker-хоста и контейнеров проводится в соответствии с таблицей 3. Проверка выполняется через порт веб-шлюза, по умолчанию 80. Если GATEWAY_PORT переопределен в .env, в адресах контрольных запросов таблиц 3 и 4 следует указать выбранный порт.

Таблица 3 - Проверка Docker-хоста и контейнеров

Проверка	Описание действий	Ожидаемый результат
Состояние контейнеров	Выполнить команду docker compose ps	Пять сервисов в состоянии Up, для db и frontend — Healthy
Доступность backend API	Выполнить запрос curl http://localhost/api/health	HTTP 200 и тело {"status":"ok","service":"geobim-api"}
Готовность БД	Проверить docker compose logs db или выполнить pg_isready -U geobim	PostgreSQL, Postgres Pro принимает подключения
Миграции и завершение старта backend	Просмотреть docker compose logs backend	Присутствуют записи «Application startup complete» и применения ревизии 001. Ошибки Alembic отсутствуют, импорт seed завершается успешно. Остановка журнала на записи «Started reloader process» означает аварию по пункту 5.8
Свободное место	Проверить df -h и docker system df	Свободное место достаточно для журналов, томов БД и Keycloak
Доступность Keycloak	Открыть http://localhost:8080/auth или настроенный порт	Страница авторизации/администрирования Keycloak открывается

Проверка gateway, frontend и identity-provider проводится в соответствии с Таблицей 4.

Таблица 4 - Проверка gateway, frontend и identity-provider

Проверка	Описание действий	Ожидаемый результат
Главная страница	Открыть http://localhost/; выполнить curl -o /dev/null -w "%{http_code}" http://localhost/	HTTP 200, открывается страница входа GeoBIM

Проверка	Описание действий	Ожидаемый результат
Прямой frontend	Открыть http://localhost:4200 или порт FRONT_PORT, заданный в .env	Angular-приложение отвечает и обновляется при изменении исходников
Keycloak realm	Войти в realm geobim под администратором Keycloak	Открывается консоль с импортированным realm geobim
Статические ресурсы	Проверить загрузку логотипа и config.json через frontend	Брендинг и карта инициализируются без ошибок 404
Работа контроля доступа	Выполнить запрос к http://localhost/api/layers без токена	HTTP 403 — признак корректной работы авторизации, а не отказа сервиса
Конфигурация realm	Выполнить curl http://localhost/auth/realms/geobim/.well-known/openid-configuration	HTTP 200, возвращается конфигурация realm geobim

3.3.2 Проверка работоспособности ППО

После входа в приложение необходимо убедиться, что в зависимости от назначенных ролей пользователю доступны модули «Карта», «Аналитика» и «Слои». Для администратора дополнительно должен открываться раздел /admin.

– в каталоге слоев присутствуют стартовые папки «Базовые слои» и «Внешние источники»;

– слой «Спутник (ESRI)» и слой «Кадастровая карта (Росреестр)» отображаются корректно;

– загрузка тестового набора геоданных завершается без критических ошибок;

– создание пользователя, роли и изменение прав доступа отражаются в журнале аудита;

– дашборды и шаблоны виджетов доступны, а история AI-аналитики записывается в БД при наличии ключей.

4 ОПИСАНИЕ ОПЕРАЦИЙ

4.1 Операции в рамках Системы

4.1.1 Администрирование Системы «GeoBIM»

4.1.1.1 Состав и содержание дистрибутива

Основные компоненты дистрибутива и их назначение приведены в таблице 5.

Таблица 5 - Основные компоненты дистрибутива и их назначение

Наименование	Расположение / назначение
backend	FastAPI-приложение, доменные роутеры, миграции Alembic, seed-скрипты
frontend	Angular 21 SPA, модули карты, аналитики, слоев и администрирования
infra/nginx/nginx.conf	Конфигурация gateway и проксирование API, Keycloak и frontend
infra/keycloak/realm-export.json	Стартовая конфигурация realm geobim
infra/keycloak/Dockerfile и infra/keycloak/.dockerignore	Сборка образа Keycloak на базе Debian и ограничение контекста сборки
deploy/<profile>/config.json	Брендинг инстанса, карта, логотип, title и экспортный префикс
docker-compose.yml	Оркестрация контейнеров gateway, keycloak, db, backend и frontend
.env.example / backend/.env.example	Шаблоны переменных окружения для штатного и локального запуска
frontend/public/assets/guide/dashboard-guide.md	Пользовательское руководство по дашбордам

4.1.1.2 Порядок установки и настройки

Ключевые параметры конфигурации, используемые администратором при штатной эксплуатации, приведены в таблице 6.

Таблица 6 - Ключевые параметры конфигурации, используемые администратором при штатной эксплуатации

Наименование	Назначение
COMPOSE_PROJECT_NAME	Имя проекта Docker Compose и префикс контейнеров/томов; по умолчанию geobim. Позволяет разворачивать несколько стендов на одном узле

GATEWAY_PORT	Публикуемый порт Nginx gateway — основная точка входа в Систему; по умолчанию 80
FRONT_PORT	Прямой доступ к серверу разработки Angular; по умолчанию 4200
DB_PORT	Порт СУБД, публикуемый на хосте; по умолчанию 5432
KEYCLOAK_PORT	Порт консоли администрирования Keycloak; по умолчанию 8080
YANDEX_FOLDER_ID	Идентификатор каталога Yandex Cloud для AI-аналитики
YANDEX_API_KEY	Секретный API-ключ сервисного аккаунта Yandex Cloud
YANDEX_MODEL	Имя модели Yandex Foundation Models
SEED_PROFILE	Профиль стартовых данных, применяемый при первом запуске backend; по умолчанию geobim. Пустое значение отключает загрузку seed
DATABASE_READONLY_URL	Строка подключения backend к read-only пользователю БД

Контейнеры и их типовые образы приведены в таблице 7.

Таблица 7 - Контейнеры и их типовые образы

Наименование	**Тип**	**Дистрибутив / образ**
gateway	Веб-шлюз	nginx:bookworm
keycloak	Провайдер идентификации	Сборка из infra/keycloak/Dockerfile, тег geobim-keycloak:24.0.5
db	СУБД пространственных данных	postgis/postgis:16-3.4
backend	Backend API и миграции	Сборка из backend/Dockerfile (python:3.12-slim)
frontend	Клиентское SPA	Сборка из frontend/Dockerfile (node:24-slim)
Yandex Foundation Models	Внешний API	Облачный сервис, подключаемый по HTTPS

В административном интерфейсе доступны операции по созданию и блокировке пользователей, назначению ролей admin/editor/observer, управлению feature-флагами и матрицей прав на слои.

Для ролей поддерживаются feature-коды access_map, access_analytics, access_layers, upload_layers и manage_datasources. Права на слой задаются по флагам can_view, can_edit, can_publish и can_view_source.

Загрузка геоданных выполняется через модуль upload и поддерживает SHP, GeoJSON, JSON, TAB, GPKG, KML, GML, DWG и DXF. При импорте выполняется попытка автоматического исправления невалидной геометрии; предупреждения по пропущенным объектам возвращаются пользователю.

Для каждого вновь созданного слоя non-admin пользователю автоматически выдаются права просмотра, редактирования и просмотра источника для всех его ролей. Для 3D-слоев поддерживается загрузка только файлов .gltf и .glb размером до 20 МБ.

Экспорт конфигурации через /api/config/export переносит описания слоев и каталога, но не включает сами объекты features, пользователей, роли, данные Keycloak и журналы аудита; для них требуется резервное копирование БД и томов.

4.1.1.3 Метрики мониторинга

Система не требует обязательного выделенного контура мониторинга, однако для штатной эксплуатации рекомендуется контролировать показатели, приведенные в таблице 8.

Таблица 8 -

Метрика	**Описание**	**Минимальное допустимое значение**	**Максимальное допустимое значение**	**Уровень критичности**
HTTP /api/health	Проверка доступности backend API через gateway	status=ok	5xx/timeout отсутствуют	Высокий
Container backend	Состояние контейнера backend	Up	Restarting/Exited не допускается	Высокий
Container db	Состояние контейнера PostgreSQL,	Up	Restarting/Exited не допускается	Высокий

	Postgres Pro /PostGIS			
Container keycloak	Состояние контейнера Keycloak	Up	Restarting/Exited не допускается	Высокий
Свободное место	Свободное место на дисках и томах	не менее 20%	менее 10% – аварийный порог	Высокий
Ошибки backend	Количество критических ошибок в логах backend	0	рост повторяющихся ошибок	Средний
Рост таблицы features	Динамика объема пространственных данных	в пределах ожидаемой нагрузки	резкий рост без бизнес-причины	Средний
AI-аналитика	Успешность запросов к Yandex Cloud	доступна при наличии ключей	503 при штатно настроенных ключах	Средний
Главная страница	Время ответа страницы входа и карты	стабильная загрузка	длительные таймауты/ошибки загрузки	Средний

Политика автоматического перезапуска для сервисов не задана: аварийно завершившийся контейнер backend не восстанавливается самостоятельно, а веб-шлюз при этом остается доступным и возвращает 502. Контроль состояния контейнера backend в соответствии с таблицей 8 является обязательным.

4.2 Общесистемные задачи и процедуры администрирования

4.2.1 Режимы функционирования

Система поддерживает режим первичного развертывания, штатный эксплуатационный режим, режим технического обслуживания и режим ограниченной функциональности без AI-аналитики. Переход между режимами осуществляется без изменения состава контейнеров, за исключением остановки/запуска сервисов и отключения внешних интеграций.

Штатный запуск использует отладочные режимы: uvicorn с параметром --reload, сервер разработки Angular и Keycloak в режиме start-dev. Для продуктивной эксплуатации требуется отдельная конфигурация без отладочных режимов.

4.2.2 Штатный запуск

– проверить актуальность .env, профиля deploy и доступность портов;

– при необходимости выполнить docker compose pull и docker compose build; образ Keycloak собирается локально согласно пункту 3.2.7, поэтому ошибка его загрузки из реестра не препятствует запуску;

– перед первым запуском новой версии выполнить требования к пустой базе данных согласно пункту 3.2.8;

– запустить стек командой docker compose up -d --build;

– проверить docker compose ps и ответ /api/health, выполнить остальные проверки по таблицам 3 и 4;

– выполнить контрольный вход в GeoBIM и Keycloak.

– docker compose up -d --build

4.2.3 Штатная остановка

Для штатной остановки необходимо предупредить пользователей о перерыве, убедиться в завершении критичных операций импорта, после чего выполнить остановку контейнеров.

– docker compose down

Команда docker compose down -v применяется только для полной очистки среды и удаления томов данных. Перед ее выполнением необходимо подтвердить отсутствие ценных данных либо снять резервную копию.

4.2.4 Архивирование данных

Для архивирования конфигурации рекомендуется периодически выгружать JSON-конфигурацию слоев и каталога, экспортировать JSON дашбордов, сохранять файлы deploy/<profile>/config.json, .env и служебные настройки инфраструктуры.

Журнал аудита может быть выгружен в CSV через /api/audit/export. Для сохранения учетных записей и состояния realm Keycloak требуется резервное копирование тома geobim_keycloak_data либо актуального realm-export.json.

4.2.5 Резервное копирование и восстановление

Минимально достаточный комплект резервного копирования включает: дамп базы данных geobim, данные Keycloak, корневой .env, профиль deploy, экспорт конфигурации слоев/каталога и экспорт дашбордов.

– docker compose exec db pg_dump -U geobim -d geobim -Fc -f /tmp/geobim.dump

Восстановление выполняется после остановки стека, возврата дампа PostgreSQL, Postgres Pro в пустую базу данных и, при необходимости, данных Keycloak. Повторный запуск ревизии 001_initial не требуется: версия схемы содержится в самом дампе. После восстановления проводится полная проверка сервиса по таблицам 3 и 4.

– docker compose exec -T db pg_restore -U geobim -d geobim --clean --if-exists < geobim.dump

При восстановлении из пустой БД допускается повторный запуск seed-профиля; при восстановлении из боевого дампа seed-профиль должен оставаться идемпотентным и не должен разрушать пользовательские данные.

При необходимости сохранения данных предыдущей версии Системы восстановление выполняется из дампа, снятого предыдущей версией, в пустую базу данных без повторного запуска ревизии 001_initial.

4.2.6 Фиксация версий зависимостей backend

Версии зависимостей backend зафиксированы в backend/requirements.txt и не подлежат изменению в рамках эксплуатации. В частности, зафиксирована версия cryptography 46.0.4: начиная с версии 47.0.0 при импорте модуля jose.jwt процесс backend аварийно завершается с сигналом SIGILL («Illegal instruction») на платформе aarch64. Ранее версия библиотеки не фиксировалась и устанавливалась транзитивно, что приводило к неработоспособности backend при пересборке образа.

Обновление зависимостей выполняется только в рамках выпуска новой версии Системы с проведением проверок по таблицам 3 и 4.

Используется версия python-jose 3.3.0, не обновлявшаяся с 2021 года и имеющая известные уязвимости. Замена библиотеки подлежит планированию в рамках регламента устранения уязвимостей.

5 АВАРИЙНЫЕ СИТУАЦИИ

5.1 Отказ в доступе

При отказе в доступе необходимо проверить доступность Keycloak по пути /auth, корректность realm geobim, активность учетной записи пользователя и назначенные ему роли. Также следует проверить, не сработала ли brute-force защита Keycloak и не истек ли сеанс пользователя.

5.2 Не загружается главная страница

Если не загружается главная страница, необходимо проверить контейнеры gateway и frontend, конфигурацию порта GATEWAY_PORT, логи nginx и наличие статических ресурсов frontend/public/assets.

5.3 Действия в случае несоблюдения условий выполнения технологического процесса, в том числе при длительных отказах технических средств

При длительных отказах инфраструктуры следует остановить пользовательские операции записи, зафиксировать состояние контейнеров и журналов, оценить актуальность последней резервной копии и перевести систему в режим технического обслуживания до устранения причины отказа.

5.4 Действия по восстановлению программ и/или данных при отказе магнитных носителей или обнаружении ошибок в данных

При потере данных или повреждении томов необходимо восстановить PostgreSQL, Postgres Pro из последнего корректного дампа в пустую базу данных согласно пункту 4.2.5, вернуть файлы конфигурации, после чего выполнить проверку каталогов, слоев, прав доступа и работоспособности AI-аналитики и дашбордов.

5.5 Действия в случаях обнаружении несанкционированного вмешательства в данные

При обнаружении несанкционированного вмешательства необходимо немедленно ограничить доступ подозрительных учетных записей, сменить административные пароли Keycloak и БД, отозвать или заменить Yandex API key, выгрузить журнал аудита и провести анализ изменений по affected-слоям.

5.6 Действия в других аварийных ситуациях

К прочим аварийным ситуациям относятся конфликт портов, недоступность внешних картографических источников, ошибки импорта поврежденных геоданных, а

также временная недоступность Yandex Cloud. В этих случаях допускается эксплуатация системы с частичным отключением соответствующего модуля.

5.7 Backend не запускается после обновления версии

Признаки: контейнер backend в состоянии Exited (255); в журнале backend — сообщение «FAILED: Can't locate revision identified by '036'»; обращение к /api/health через шлюз возвращает 502 Bad Gateway; остальные контейнеры работают штатно.

Причина: том базы данных содержит версию схемы, отсутствующую в текущей истории миграций.

Действия администратора: подтвердить отсутствие ценных данных либо снять резервную копию, остановить стек с удалением томов и выполнить повторное развертывание согласно пункту 3.2.8. При необходимости сохранения данных восстановление выполняется из дампа, снятого предыдущей версией Системы, в пустую базу данных согласно пункту 4.2.5.

5.8 Backend завершается с сигналом «Illegal instruction»

Признаки: журнал backend содержит запись «Started reloader process» и далее не пополняется; обращение к /api/health возвращает 502; при ручном запуске приложения в контейнере выводится сообщение «Illegal instruction» с кодом завершения 132.

Причина: установлена версия библиотеки cryptography 47.0.0 или выше, несовместимая с платформой узла.

Действия администратора: проверить фиксацию cryptography==46.0.4 в backend/requirements.txt, пересобрать образ backend и убедиться в появлении записи «Application startup complete».

– docker compose up -d --build backend

Таблица 9 – Аварийные ситуации

Аварийная ситуация	**Возможные потери информации**	**Действие**	**Подрядчик**
Недоступен gateway/frontend	Невозможность входа и просмотра карты	Проверить контейнеры gateway/frontend, порт GATEWAY_PORT и логи nginx; перезапустить сервисы	Администратор

Аварийная ситуация	**Возможные потери информации**	**Действие**	**Подрядчик**
Недоступен backend или БД	Недоступность API, невозможность изменения данных	Проверить db/backend, миграции, подключение к БД; при необходимости восстановить сервис из резервной копии	Администратор
Повреждение данных PostgreSQL, Postgres Pro	Частичная или полная потеря пространственных данных и журналов	Остановить запись, восстановить БД из дампа, проверить каталоги и права доступа	Администратор
Ошибочная настройка ролей и прав	Отказ в доступе либо избыточный доступ пользователей	Проверить роли, feature-флаги и матрицу permissions в /admin, выгрузить аудит изменений	Администратор
Недоступны внешние сервисы (Yandex, Росреестр)	Частичная потеря аналитики или внешних слоев	Отключить проблемную интеграцию, уведомить пользователей, восстановить доступ после проверки внешнего сервиса	Администратор
Несовместимость тома базы данных с историей миграций	Потеря данных предыдущей версии при очистке томов	Снять резервную копию, выполнить docker compose down -v и повторное развертывание; восстановление выполнять в пустую базу данных	Администратор

Аварийная ситуация	**Возможные потери информации**	**Действие**	**Подрядчик**
Аварийное завершение backend при импорте библиотек	Отсутствуют, API недоступен до устранения	Проверить фиксацию версий в backend/requirements.txt, пересобрать образ backend	Администратор
Недоступность источника дистрибутива Keycloak при сборке	Отсутствуют, развертывание не выполняется	Использовать резервный источник repo1.maven.org либо внутреннее зеркало через аргумент сборки KEYCLOAK_DIST_URL	Администратор

6 РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

Для освоения задач системного администрирования системы рекомендуется выполнить полный цикл развертывания на тестовом окружении, включая настройку .env, запуск docker compose, проверку модулей карты, аналитики и слоев.

– создать тестовых пользователей с ролями admin, editor и observer и проверить разграничение доступа;

– отработать сценарии импорта GeoJSON/SHP, создания источника данных и загрузки GLTF-модели;

– проверить экспорт/импорт конфигурации, экспорт дашборда и выгрузку журнала аудита;

– выполнить тренировочное резервное копирование и восстановление БД и конфигурации;

– использовать README.md, deploy/README.md и dashboard-guide.md как оперативные справочные материалы.

Каталог docs с планом нативной установки выведен за пределы репозитория. Ссылки на README.md, deploy/README.md и dashboard-guide.md остаются действительными.