

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Выполнение работ по развитию программно-инструментальной среды для эффективной работы с базой данных инженерно-геодезических изысканий на платформе Postgres PRO с целью повышения скорости доступа, обработки и визуализации пространственных данных масштаба 1:500 и 1:200

1. Общая информация об объекте закупки

1.1. Объект закупки: Выполнение работ по развитию программно-инструментальной среды для эффективной работы с базой данных инженерно-геодезических изысканий на платформе Postgres PRO с целью повышения скорости доступа, обработки и визуализации пространственных данных масштаба 1:500 и 1:200.

1.2. Код и наименование позиции Классификатора предметов государственного заказа: 02.27.05 - РАБОТЫ/РАБОТЫ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ДЛЯ ПРИКЛАДНЫХ ЗАДАЧ/РАЗРАБОТКА И ВНЕДРЕНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ И РЕСУРСОВ.

1.3. Наименования позиций Справочника предметов государственного заказа: согласно Приложению 1.

1.4. Место выполнения работ: согласно Приложению 1.

1.5. Объем работ: согласно Приложению 1.

1.6. Срок выполнения работ: согласно Приложению 1

1.7. Приложения к Техническому заданию:

– Приложение 1. – «Перечень объектов закупки».

- Приложение 2 – «Акт определения уровня защищенности персональных данных в информационной системе персональных данных».

- Приложение 3 – «Акт классификации информационной (автоматизированной) системы»)

Термины и определения

Сокращение	Расшифровка
БД	База данных
Бригада	Группа полевых исполнителей для выполнения геодезической съемки
ГИС	Геоинформационная система
Заказ/Наряд	Единица планирования работ, содержащая границы территории и атрибуты задания
ИГДИ М1:200	Инженерно-геодезические изыскания масштаба 1:200
ИГДИ М1:500	Инженерно-геодезические изыскания масштаба 1:500
ИС	Информационная система
ИС организации	Информационные системы организации (источник/приемник данных о заказах, сотрудниках, результатах работ)

Операция	Технологический этап выполнения работ в производственном процессе
ОПС	Объекты подземных сооружений
ОШС	Организационно-штатная структура
Пикеты	Точки съемки с геодезических приборов
ПМИ	Программа и методика испытаний
Полевые материалы	Комплект данных для выполнения полевых работ (включает векторные и растровые данные, карты, документацию)
Сборка «Ромашка»	Алгоритм создания актуального покрытия территории заказа, без перекрытий из контуров ранее выполненных работ
СиЗИ	Системы защиты информации
СУБД	Система управления базами данных
УГП №1, УГП №2	Управление инженерно-геодезических изысканий №1 и №2
ЦКФ	Цифровой картографический фон
ЦТП	Цифровой топографический план
ЧТЗ	Частное техническое задание
DGN, DXF, DWG, GeoJSON, PDF	Форматы данных для обмена и представления геопространственной информации и документации
Postgres PRO	СУБД
Web-портал, Система	Автоматизированная система управления подготовкой

2. Стандарт работ

2.1. Назначение разработки

Разрабатываемый web-портал «Автоматизированная система управления подготовкой» (далее – Система) предназначен для комплексной автоматизации процессов подготовки полевых материалов

и управления производственными процессами при выполнении инженерно-геодезических изысканий масштаба 1:500 (ИГДИ М1:500) в производственных подразделениях УГП №1 и УГП №2.

Система должна обеспечивать:

- автоматизацию подготовки полевых материалов, включающую анализ архивных данных в границах заказа, формирование актуальных комплектов данных для полевых бригад в форматах PDF и DXF, управление выдачей материалов в работу с учетом загрузки исполнителей;
- автоматизацию управления производственными процессами (диспетчеризация), включающую планирование и распределение заданий по бригадам с использованием алгоритмов пространственного и атрибутивного анализа, контроль сроков выполнения работ, обработку нештатных ситуаций;
- обеспечение полного мониторинга производственных процессов по всем операциям в рамках выполнения ИГДИ по всем заказам от получения наряда до выдачи заказчику;
- визуализацию геопространственных данных на картах с возможностью создания и редактирования геометрий, настройки стилей визуализации объектов;
- формирование дашбордов для вывода метрик производства и аналитических отчетов;
- удаленное взаимодействие с полевыми бригадами, включая передачу материалов на мобильные устройства и получение обратной связи;
- возможность обращения к Системе как к сервису «Подготовки полевых материалов» из систем и ПО Заказчика для формирования данных в форматах DGN, GeoJSON, DXF, DWG, PDF.

Система должна взаимодействовать с БД Postgres Pro Заказчика, обеспечивая чтение и обновление информации.

2.2. Цели разработки

Целями разработки Системы являются:

- Повышение прозрачности и управляемости производства за счет мониторинга всех операций и контроля сроков выполнения работ.
- Обеспечение быстрого доступа к оперативным данным для принятия управленческих решений.
- Автоматизация планирования и распределения инженерно-геодезических работ.
- Ускорение подготовки материалов и выдачи их в работу с учетом реальной загрузки исполнителей.
- Организация работы с данными чертежей непосредственно в существующей базе данных вместо обработки файлов на дисковых хранилищах (датацентричная модель).

2.3. Характеристика объекта автоматизации

Объектом автоматизации являются производственные процессы при выполнении инженерно-геодезических изысканий масштаба 1:500 и 1:200 (ИГДИ М1:500, ИГДИ М1:200) в производственных подразделениях Управление инженерно-геодезических изысканий №1 (УГП №1) и Управление инженерно-геодезических изысканий №2 (УГП №2).

Текущие характеристики производственных процессов:

- Количество полевых бригад: до 50 бригад по разным направлениям, закрепленных по территориям.
- Количество камеральных сотрудников: 100.
- Объем заявок: среднегодовое количество заявок в день 50.
- Количество линейных руководителей, распределяющих заказы: 20 диспетчеров.
- Количество заказов на полевую бригаду: в среднем до 5 заказов у каждой бригады.

Производственные процессы включают:

- поступление заказа и передача в работу (после поступления оплаты по договору или поручения по государственным заказам);
- подготовка полевых материалов (поиск и анализ архивных данных, формирование комплектов материалов);
- планирование выполнения работ;
- распределение заказов диспетчерами между бригадами;
- выдача полевых материалов в работу;
- выполнение полевых работ;
- планирование и распределение камеральных работ;
- выполнение камеральных работ;
- контроль сроков выполнения работ;
- решение проблемных ситуаций;
- контроль качества;
- оформление и выдача результатов заказчику.

Триггером для начала работ служит наряд на работы, сформированный отделом договоров и производственной диспетчеризации (ОДиПД) на основании нового заказа из ИС организации.

2.4. Требования к системе

2.4.1. Общие требования

Система должна быть реализована как web-портал и обеспечивать следующие общие характеристики:

- Взаимодействие с БД Postgres Pro Заказчика с возможностью чтения и обновления информации БД.
- Поддержку единовременного отображения большого количества геометрий (векторных объектов) при этом обеспечивать высокое быстродействие.
- Разграничение доступа по ролям для обеспечения безопасности и контроля действий пользователей.
- Возможность использования Системы как сервиса «Подготовки полевых материалов» из других систем и ПО Заказчика, в которых работают производственные подразделения.
- Формирование выходных файлов в форматах DGN, GeoJSON, DXF, DWG, PDF.
- Функционирование в ИТ-инфраструктуре Заказчика с обеспечением надежности, масштабируемости и безопасности.
- Поддержка вариативности системы браузерного отображения (поддержка современных web-браузеров).
- Адаптивность отдельных компонентов Системы для работы на различных устройствах (десктоп, планшет, мобильные устройства).

2.4.2. Функциональные требования

Подсистема подготовки полевых материалов должна обеспечивать следующие функции:

а) Получение заказов и нарядов:

- получение заказов/нарядов из ИС организации (триггер – создание нового наряда);
- формирование карточки заказа, содержащей следующую информацию; отображение границы

заказа на карте; ведение журнала событий по заказу.

б) Территориальный анализ данных:

- выполнение территориального запроса по границе заказа;
- анализ имеющихся в БД Postgres Pro архивных данных из различных источников по их актуальности в границах заказа;
- выборка данных на территории заказа из источников (перечень источников приведен в п. 2.4.4);
- подключение пикетов из БД Postgres Pro по территориальному запросу;
- формирование актуальных данных без пересечений (мозаика) в пределах заданной территории на текущую дату;
- выполнение анализа актуальности данных с учетом дат, типов данных и приоритетов источников.

в) Формирование пакета материалов:

- создание рабочих директорий для новых заказов в заданных каталогах с наименованием по заданному шаблону;
- сборка общего файла из актуальных материалов (формирование мозаики);
- формирование комплекта данных в форматах PDF и DXF для передачи в формат DGN и полевые камеральные подразделения;
- PDF: печатная картографическая форма (карта) по заказу/участку с обязательными реквизитами (состав реквизитов уточняется на этапе проектирования);
- DXF: векторные данные в пределах территории заказа, включая геометрию объектов из ранее выполненных заказов, границы заказа и пикеты, с CAD-атрибутами визуализации (level/layer, color, line style, line weight);
- DGN: файл используемый профильным программным обеспечением Заказчика, имеющий параметры DXF файла;
- версионирование подготовленных пакетов с фиксацией информации «кто/когда/какая версия»;
- возможность повторной пересборки пакета материалов;
- сохранение состояния подготовленного заказа для последующей обработки.

г) Выдача материалов в работу:

- выдача пакета материалов исполнителю/бригаде с подтверждением линейного руководителя;
- возможность дробления заказа на части для выдачи нескольким исполнителям;
- фиксация площадей, выданных в работу;
- фиксация факта начала работ и времени начала;
- фиксация факта завершения работ и времени завершения;
- учёт реальной загрузки исполнителей при выдаче новых заданий;
- интеграция просмотра и работы с данными подготовки полевых материалов в web интерфейсе.

д) Сборка нового заказа через базу данных (подготовка полевых работ):

Сборка нового заказа, представляющая собой подготовку полевых работ, должна быть реализована полностью на основе данных базы данных Postgres Pro с расширением PostGIS. Все исходные

материалы для сборки заказа должны браться из базы данных Postgres PRO, а промежуточные и итоговые результаты подготовки сохраняться обратно в базу данных.

Сборка заказа должна обеспечивать:

- инициирование сборки нового заказа по триггеру создания наряда либо по запросу пользователя или внешней информационной системы;
- автоматическое выполнение территориального запроса к базе данных Postgres Pro по границе заказа и выборку всех актуальных данных из оцифрованных источников;
- формирование актуальных данных без пересечений (мозаики) непосредственно на основе данных базы данных с учётом дат, типов данных и приоритетов источников;
- обеспечение возможности валидации корректности данных;
- подключение пикетов и справочной информации из базы данных по территориальному запросу;
- сохранение собранного пакета материалов, его состава, версий и статусов в базе данных Postgres Pro;
- формирование выходных файлов (PDF, DXF, DGN и др.) на основе собранных в базе данных материалов;
- обеспечение целостности сборки за счёт выполнения операций в транзакциях базы данных;
- возможность повторной пересборки заказа из базы данных с сохранением истории версий.

Алгоритмы сборки заказа, правила формирования мозаики, валидация, и приоритезации источников, а также структура хранения собранных заказов в базе данных уточняются и согласовываются с заказчиком на этапе технического проектирования.

Подсистема производственной диспетчеризации должна обеспечивать следующие функции:

а) Планирование и распределение заданий по бригадам:

- получение и обработка потока новых заказов из ИС организации;
- формирование сроков обследования (полевых работ) с учетом сроков исполнения договоров и сроков поручений (по городским заказам);
- использование алгоритмов пространственного и атрибутивного анализа данных для принятия решений о распределении заказов между исполнителями;
- распределение заказов по бригадам УГП №1 и УГП №2 с учетом:
 - сложности заказов (площадь, количество объектов, другие метрики);
 - исполнительского уровня бригад;
 - текущей загруженности бригад;
 - оптимальной маршрутизации (территориальная близость, минимизация перемещений).
- контроль равномерности загрузки бригад;
- обработка нештатных изменений плана работ (проблемы с выполнением заказов, сдвиг сроков): перераспределение заказов, переброска бригад, перенос сроков.

б) Формирование и ведение бригад:

- статус доступности и период отсутствия (отпуск, отгул, период временной нетрудоспособности — без медицинских сведений);
- тип и дата кадрового события.

Обработка персональных данных при планировании и распределении работ осуществляется Заказчиком (Учреждением) как оператором персональных данных. Система должна предоставлять соответствующий функционал. Определение перечня персональных данных, целей и сроков

обработки, уровня защищённости ПДн и мер защиты относится к ответственности Заказчика. Полный перечень персональных данных, цели и сроки их обработки и хранения фиксируются на этапе определения уровня защищённости ПДн и классификации ИС (152-ФЗ, приказы ФСТЭК России №21 и № 117).

Формирование и ведение бригад должно вестись без учета персональных данных, система должна передавать данные исключительно на основании идентификатора ID, внутри корпоративной сети.

- закрепление бригад за территорией с учетом мест проживания сотрудников;
- получение кадровых событий ОШС (организационно-штатная структура) из ИС организации (прием на работу, увольнение, перевод, отпуск, отгул, больничный);
- Из ИС организации (ОШС) данные поступают в виде событий (идентификатор сотрудника, тип события, период, статус доступности, подразделение/бригада при переводе), а не только в виде статуса сотрудника; исходные кадровые документы не передаются. Форматы и протоколы обмена согласуются на этапе проектирования.
- Указанные кадровые события не относятся к персональным данным и обрабатываются в минимально необходимом объёме; защита обеспечивается разграничением доступа по ролям, изоляцией данных по подразделениям и передачей по защищённому каналу.
- обработка потока кадровых событий, временное (отпуск, больничный) и постоянное перераспределение сотрудников по бригадам;
- накопление статистики по исполнительскому уровню бригады с учетом сложности выполненных заказов и соблюдения сроков;
- ранжирование исполнительского уровня бригад с учетом статистики.

в) Формирование заданий на обследования:

- формирование границы заказа на карте (ГИС);
- формирование ссылок на связанные файлы и документы;
- формирование печатной формы задания с необходимыми реквизитами.

г) Контроль выполнения полевых работ

Доступ к функциям и видимость полей интерфейса должна быть разграничена на основании ролевой модели (п. 2.4.6). Матрица прав доступа должна быть сформирована Исполнителем и согласована с Заказчиком. Ролям должны быть доступны следующие функции:

- текущий контроль сроков выполнения заданий на обследования (полевые работы);
- отображение карточек заказов на обследования (полевые работы) с актуальной информацией о статусе, исполнителях, сроках;
- аналитика и отчетность по заданиям на обследования (состав и содержание отчетов уточняется с функциональными подразделениями Заказчика в ходе выполнения работ);
- визуализация полной ситуации по всем операциям в рамках выполнения ИГДИ по всем заказам.

Модуль визуализации и работы с геоданными должен обеспечивать следующие функции:

- отображение геометрий (векторных объектов) на карте с поддержкой различных типов геометрий (точки, линии, полигоны, мультигеометрии);
- создание и редактирование геометрий средствами web-интерфейса;
- сохранение созданных и отредактированных геометрий в БД Postgres Pro;
- настройка стиля визуализации объектов (цвет, толщина линий, заливка, прозрачность, символы);
- выполнение пространственного анализа данных (пересечение, объединение, буферизация, расчет расстояний и площадей);

- выполнение атрибутивного анализа данных (фильтрация, поиск, группировка, агрегация);
- поддержка работы с большим количеством геометрий с обеспечением быстродействия (оптимизация отрисовки, кластеризация, генерализация).

Модуль дашбордов и аналитики должен обеспечивать следующие функции:

- формирование дашбордов для вывода метрик производства (конкретные метрики согласовываются с заказчиком на этапе изучения жизненного цикла заказа);
- визуализация полной ситуации по всем операциям по всем заказам;
- отображение карточек заказов с детальной информацией;
- формирование аналитических отчетов по заданиям (состав отчетов уточняется с функциональными подразделениями Заказчика на этапе выполнения работ);
- возможность фильтрации и группировки данных по различным параметрам (период, подразделение, исполнитель, тип операции, статус);
- экспорт отчетов в различные форматы (PDF, XLSX, CSV).

Мобильный контур должен обеспечивать следующие функции:

- предусмотреть передачу полевых материалов (файлы PDF и DXF) полевым бригадам на корпоративные мобильные устройства (через интерфейс web-приложения);
- получение обратной связи от полевых бригад (статусы выполнения, проблемы, запросы);
- фиксацию статусов выполнения работ и времени начала/завершения мобильными пользователями;
- офлайн-режим работы с возможностью:
 - предварительного скачивания заданий, материалов и геометрий;
 - фиксации статусов и внесения данных без подключения к сети;
 - автоматической синхронизации данных при восстановлении связи;
- правила синхронизации и разрешения конфликтов уточняются на этапе обследования и фиксируются в проектной документации.
- наряд/задание (номер заказа, территория и сроки работ), графические материалы по заказу (план/чертёж в формате PDF), служебные пометки исполнителя. Персональные данные ограничены служебными данными (идентификатор/ФИО исполнителя, привязка к бригаде), которые не передаются.

2.4.3 Требования к интеграции

Система должна обеспечивать интеграцию и информационное взаимодействие со следующими компонентами инфраструктуры Заказчика:

а) Взаимодействие с БД Postgres Pro Заказчика:

- чтение данных из БД Postgres Pro (пространственные данные, атрибутивные данные, пикеты, справочники);
- обновление данных в БД Postgres Pro (результаты подготовки, статусы заказов, геометрии, метаданные);

- поддержка расширения PostGIS для работы с пространственными данными;
- использование транзакций для обеспечения целостности данных;
- оптимизация запросов для обеспечения быстродействия при работе с большими объемами данных.

б) Обмен данными с ИС организации:

- получение заказов/нарядов из ИС «Договор» организации при создании;
- передача в ИС организации результатов выполнения работ:
- назначенный исполнитель;
- время начала работ;
- время завершения работ;
- площади, выданные в работу;
- тип операции;
- геометрия (GeoJSON);
- дополнительная информация о заказе;
- ведение журнала успешных/ошибочных отправок;
- обеспечение повторной отправки по согласованным правилам;
- конкретные интеграционные контракты (форматы, протоколы, перечень полей) согласовываются на этапе обследования и проектирования.

в) Возможность обращения к Системе как к сервису

Система должна предоставлять сервис «Подготовки полевых материалов» для использования из других информационных систем Заказчика, в которых работают производственные подразделения. Сервис должен обеспечивать:

- формирование файлов в форматах DGN, GeoJSON, DXF, DWG, PDF по запросу;
- прием запросов через API (REST или другой согласованный протокол);
- передачу результатов формирования файлов;
- аутентификацию и авторизацию вызовов сервиса;
- логирование обращений к сервису.

Конкретная спецификация API сервиса разрабатывается на этапе проектирования и согласовывается с Заказчиком с учетом класса защищенности информационной системы.

2.4.4 Требования к данным

Система должна обеспечивать доступ и обработку следующих источников данных для анализа и подготовки полевых материалов:

№	Наименование ресурса	Описание	Тип данных
1.	Граница заказа	Формируется по номеру заказа или территориальному запросу	База данных Postgres Pro
2.	Пикетаж	Формируется по номеру	База данных Postgres Pro

		заказа или территориальному запросу	
3.	Инженерно-геодезические изыскания (М1:500) выполненные в электронном виде	Данные заказов без фильтра по дате	База данных Postgres Pro
4.	ЦТП М1:2000	Цифровой топографический план по территориям	База данных Postgres Pro
5.	ЦКФ М1:10000	Цифровой картографический фон по листам М1:10000	База данных Postgres Pro
6.	Паспортизация	Заказы выполненные в рамках паспортизации территории	База данных Postgres Pro
7.	Геонадзор	Данные сторонних организаций	База данных Postgres Pro
8.	Московская область М1:10000	Векторные данные по Московской области	Файлы DGN (Вектор)
9.	Московская область М1:10000	Растровые данные по Московской области	Растр (Принимаемые форматы MicroStation)
10.	Контрольная съёмка по годам	Объекты подземных сооружений	База данных Postgres Pro
11.	Топография (цв., М1:500)	Архивные материалы М1:500	Растр (Принимаемые форматы MicroStation)
12.	Аэрофотосъёмка	Аэрофотосъёмка по годам	Растр (Принимаемые форматы MicroStation)
13.	Космическая съёмка	Космическая съёмка по годам	Растр (Принимаемые форматы MicroStation)

14.	Сводный план сетей	Здания и сооружения инженерных сетей	База данных Postgres Pro

Согласование конкретных данных, используемых для подготовки, и алгоритмов их обработки осуществляется на этапе анализа и проектирования системы с участием функциональных подразделений Заказчика.

Результатом согласования должны стать:

- детальное описание структуры данных каждого источника;
- правила приоритизации источников данных при формировании мозаики;
- алгоритмы определения актуальности данных;
- правила разрешения пересечений и конфликтов данных;
- требования к качеству и полноте данных;
- форматы экспорта данных (спецификации DXF и PDF).

Перечень ресурсов, очередность и объёмы обработки информации, требования к точности, системе координат уточняются и согласовываются с заказчиком на этапе анализа и проектирования системы.

2.4.5 Требования к архитектуре

Конкретная архитектура Системы проектируется и согласовывается после этапа анализа существующей инфраструктуры Заказчика.

Система должна:

- функционировать в ИТ-инфраструктуре Заказчика;
- обеспечивать надежность и отказоустойчивость за счёт кластера высокой доступности Postgres Pro с автоматическим failover, резервного копирования и резервирования компонентов Системы;
- обеспечивать масштабируемость для поддержки роста объемов данных и количества пользователей;
- обеспечивать высокую производительность при работе с большим количеством геометрий;
- обеспечивать развертывание в контейнерах, и поддерживать контейнеризацию для переносимости и единообразия сред (dev/test/prod);
- соответствовать требованиям информационной безопасности Заказчика;
- обеспечивать возможность резервного копирования и восстановления данных;
- иметь модульную структуру для упрощения поддержки и развития.

Решения по архитектуре, выбору технологий, компонентов и протоколов обмена принимаются на этапе технического проектирования на основе результатов обследования инфраструктуры с учетом требований нормативных документов по защите информации «Раздела 8» настоящего технического задания, а также требований Заказчика.

2.4.6 Требования к ролевой модели и разграничению доступа

Система должна обеспечивать разграничение прав пользователей в соответствии с их функциональными обязанностями.

Система должна обеспечивать:

- выделение ролей пользователей, как минимум: оператор подготовки материалов (камеральный сотрудник); диспетчер; линейный руководитель; администратор Системы;
- разграничение доступа к функциям и данным на основе ролей (ролевая модель доступа);
- предоставление прав по принципу наименьших привилегий;
- ведение и согласование с заказчиком матрицы доступа «роль — функция — право» на этапе проектирования;
- доменную аутентификацию пользователей и протоколирование их действий и событий доступа.

Финальный вариант ролевой модели обсуждается на этапе анализа проектирования.

2.4.7 Требования к пользовательскому интерфейсу

Пользовательский интерфейс Системы должен обеспечивать удобную и эффективную работу пользователей.

Интерфейс должен:

- быть выполнен на русском языке в едином графическом стиле;
- быть адаптивным и обеспечивать работу в современных web-браузерах;
- предоставлять интерактивную работу с картой (навигация, масштабирование, выбор объектов, отображение границ заказов и слоёв данных);
- обеспечивать основные экранные формы: реестр и карточку заказа; рабочее место подготовки материалов; рабочее место диспетчера; дашборды и средства администрирования;
- минимизировать количество действий, необходимых для выполнения типовых операций;
- отображать понятные сообщения о статусах операций и об ошибках;
- состав и макеты экранных форм согласовываются с заказчиком на этапе проектирования.

2.4.8 Требования к приёмке Системы

Приёмка Системы осуществляется на основании измеримых критериев. Критерии приёмки должны включать:

- соответствие реализованной функциональности требованиям настоящего технического задания;
- успешное выполнение программы и методики испытаний (ПМИ), согласованной с заказчиком;
- достижение согласованных показателей надёжности, производительности и доступности;
- успешное завершение опытной эксплуатации без критических замечаний;
- наличие полного комплекта эксплуатационной документации;
- отсутствие открытых дефектов критического и высокого уровня на момент приёмки.

2.4.9 Требования к сборке актуальных данных стадии «Подготовка» («ромашка»)

На стадии «Подготовка» Система должна обеспечивать автоматический сбор актуальных данных по территории нового заказа из ранее выполненных работ (сборка «Ромашка»).

Сборка должна обеспечивать:

- определение территории интереса по номеру заказа (получение границ заказа из пространственной базы данных);
- отбор контуров ранее выполненных заказов, входящих в границы нового заказа;
- сортировку отобранных контуров по дате и формирование актуального покрытия без пересечений: наиболее свежий заказ размещается сверху; перекрываемые им участки

исключаются.

- двухэтапность сборки: на первом этапе формируются и проверяются только контуры (валидация до загрузки объектов); на втором этапе подгружаются сами объекты.
- двухэтапный пространственный поиск: предварительный отбор кандидатов по габаритной рамке (bounding box) с последующим уточнением по точной геометрии контуров и отбрасыванием ложных пересечений; возможность оператора оценить контуры и при необходимости изменить выборку или перезагрузить данные до загрузки объектов (например, при неподходящем типе заказа или отсутствии данных); корректную обработку мультиконтуров и устойчивость к некорректным исходным данным.

2.4.10 Среда развертывания и жизненный цикл

В соответствии с требованиями, архитектура системы состоит из трех изолированных сред:

- **DEV** (использование);
- **TEST** (тестирование);
- **PROD** (промышленная эксплуатация).

Все три среды должны быть развернуты в рамках настоящего проекта и функционировать на изолированных наборах виртуальных машин с независимыми экземплярами СУБД, балансировщика и ETL-сервисов. Разграничение трафика между средами должно обеспечиваться логическим разделением виртуальных машин в среде виртуализации z/Virt и сегментацией сети на уровне VLAN для сред использования (dev), тестирования (test) и промышленной эксплуатации (prod):

- Среда **DEV** предназначена для использования и первичной отладки ETL-скриптов, миграций схем БД и конфигурационных файлов.
- Среда **TEST** — для автоматизированной и интеграционной проверки изменений на тестовых данных перед продвижением в промышленную эксплуатацию.
- Среда **PROD** — для промышленной эксплуатации с подключением реальных источников данных и потребителей.

Управление миграциями схем БД должно осуществляться через систему контроля версий в GitFlic. CI/CD-пайплайн должен обеспечивать автоматическую проверку ETL-скриптов на тестовых данных в среде TEST перед продвижением (promotion) в PROD по заявке Заказчика. Конфигурационные файлы Postgres Pro, Patroni, HAProxy, etcd и pgBackRest подлежат ежедневному резервному копированию с хэш-контролем целостности (SHA-256). Актуализация ER-диаграмм и карт маппинга должна выполняться при каждом релизе и передаваться Заказчику в составе эксплуатационной документации. Центральное хранилище данных должно быть разделено на три независимые базы данных, обеспечивающие изоляцию производственных процессов от служебных задач и работы с неструктурированными форматами.

2.5 Требования к пользовательскому web -приложению

2.5.1 Назначение и состав web-приложения

Web-приложение представляет собой пользовательский интерфейс, обеспечивающий доступ пользователей к следующим функциям:

- подготовка полевых материалов;
- производственная диспетчеризация;
- управление заказами;
- формирование отчетности;
- интеграционное взаимодействие;

- отображение статусов заказов.

Web-приложение должно функционировать в инфраструктуре Заказчика и использовать БД Postgres Pro в качестве основного хранилища данных.

2.5.2 Функции Web-приложения

Web-приложение должно обеспечивать:

- ведение реестра заказов;
- создание и ведение карточек заказов;
- формирование и выдачу полевых материалов;
- отображение статусов заказов и производственных операций;
- управление пакетами материалов и их версиями;
- работу с картографическими данными;
- формирование отчетов и дашбордов;
- ведение журналов действий пользователей.

2.5.3 Статусы заказов

Базовый перечень статусов заказов:

- новый;
- подготовка материалов;
- готов к полевым работам;
- в работе;
- завершены полевые работы;
- камеральная обработка;
- контроль качества;
- завершен;
- архив.

Окончательный перечень статусов согласовывается с Заказчиком на этапе проектирования.

2.5.4 Роли пользователей

Web-приложение должно поддерживать ролевую модель, определенную разделом 2.4.6:

- оператор подготовки материалов;
- диспетчер;
- линейный руководитель;
- администратор системы;
- полевой исполнитель.

При необходимости допускается введение дополнительных ролей по согласованию с Заказчиком.

2.5.5 Пользовательский интерфейс

Web-интерфейс должен удовлетворять следующим требованиям:

- работать в современных браузерах;
- обеспечивать адаптивность;
- поддерживать единый графический стиль.

2.5.6 Обмен данными и синхронизация

Web-приложение должно обеспечивать:

- работу через защищенные каналы связи;

- повторную передачу данных при ошибках;
- ведение журналирования.

2.5.7 Показатели назначения

Web-приложение должно обеспечивать штатное функционирование при следующих параметрах:

- количество обрабатываемых заказов в год — не менее 10 000;
- количество одновременно работающих пользователей — не менее 100;
- общее количество пользователей — не менее 50.

2.5.8 Требования к надёжности

Надёжность Web-приложения характеризуется следующими требованиями:

- среднее время восстановления при отказе или сбое из-за ошибок — не более 4 часов;
- среднее время наработки на отказ — не менее 60 часов.

3. Состав работ

Работы по разработке и внедрению Системы выполняются поэтапно в соответствии с календарным планом, разрабатываемым Исполнителем и согласовываемым с Заказчиком на этапе обследования и анализа.

Этап 1. Обследование и анализ

Содержание работ:

- анализ целей обработки персональных данных;
- определение перечня персональных данных и их субъектов (работники / не работники Учреждения);
- сбор и анализ исходных данных для определения класса защищённости Системы и уровня защищённости персональных данных;
- разработка модели угроз и нарушителя безопасности информации;
- изучение жизненного цикла заказа от получения наряда до выдачи результатов заказчику;
- обследование текущих процессов подготовки полевых материалов и диспетчеризации;
- анализ существующей структуры и содержания БД Postgres Pro, используемой для хранения пространственных данных;
- согласование с заказчиком метрик для мониторинга производства и необходимых данных для визуализации в Системе;
- согласование данных, используемых для подготовки полевых материалов, и алгоритмов их обработки;
- согласование источников данных, правил приоритезации и определения актуальности;
- оценка объемов и сложности данных;
- выявление требований к интеграции с информационными системами организации;
- определение ролей пользователей и требований к разграничению прав доступа;
- подготовка отчета об обследовании с рекомендациями по архитектуре и технологиям.

Результаты этапа:

- отчет об обследовании, согласованный с Заказчиком;
- уточненные требования к системе;
- согласованные метрики мониторинга и данные для визуализации;

- согласованные источники данных и алгоритмы обработки;
- рекомендации по архитектуре;
- проект акта определения уровня защищённости персональных данных;
- проект акта классификации Системы;
- модель угроз и нарушителя безопасности информации.

Этап 2. Техническое проектирование

Содержание работ:

- проектирование архитектуры web-портала (клиентская часть, серверная часть, уровень данных, интеграционный уровень);
- проектирование модели данных Системы и схемы интеграции с БД Postgres Pro Заказчика;
- разработка интеграционных контрактов с ИС организации (форматы, протоколы, перечень полей для обмена данными о заказах, кадровых событиях, результатах работ);
- проектирование подсистемы подготовки полевых материалов (алгоритмы анализа данных, формирования мозаики, генерации PDF и DXF);
- проектирование подсистемы диспетчеризации (алгоритмы планирования, распределения, контроля сроков);
- проектирование модуля визуализации и работы с геоданными (технологии отображения карт, редактирования геометрий);
- проектирование дашбордов и аналитики (состав метрик, структура отчетов);
- проектирование мобильного контура (архитектура, механизмы офлайн-работы и синхронизации);
- разработка технического проекта с описанием архитектуры, компонентов, интерфейсов, алгоритмов;
- разработка спецификаций форматов экспорта (DXF, PDF) с детальным описанием состава, структуры и правил формирования;
- проектирование системы безопасности (аутентификация, авторизация, разграничение прав, аудит);
- согласование технического проекта с заказчиком;
- разработка частного технического задания на систему защиты информации (ЧТЗ на СИЗИ);
- разработка проекта системы защиты информации (СИЗИ).

Результаты этапа:

- технический проект, согласованный с заказчиком;
- интеграционные контракты, согласованные с заказчиком;
- спецификации форматов экспорта (DXF, PDF);
- описание архитектуры системы;
- ER-диаграммы модели данных;
- описание алгоритмов обработки данных;
- описание API сервиса подготовки материалов.
- частное техническое задание на систему защиты информации (ЧТЗ на СИЗИ Системы);
- проект на создание системы защиты информации (СИЗИ Системы).

Этап 3. Разработка системы

Содержание работ:

- Разработка серверной части web-портала (backend);
- Разработка клиентской части web-портала (frontend);
- Разработка подсистемы подготовки полевых материалов:
 - модуль получения и обработки заказов;
 - модуль территориального анализа данных;
 - модуль формирования пакета материалов (PDF, DXF);
 - модуль выдачи материалов в работу.
- Разработка подсистемы диспетчеризации:
 - модуль планирования и распределения заданий;
 - модуль формирования и ведения бригад;
 - модуль контроля выполнения работ.
- Разработка модуля визуализации и работы с геоданными:
 - модуль отображения карты;
 - модуль создания и редактирования геометрий;
 - модуль пространственного и атрибутивного анализа.
- Разработка дашбордов и аналитики:
 - модуль формирования метрик;
 - модуль визуализации дашбордов;
 - модуль формирования отчетов.
- Разработка мобильного контура:
 - мобильное адаптированное web-приложение с поддержкой оффлайн доступа;
 - механизмы офлайн-работы и синхронизации.
- Разработка интеграционных модулей:
 - модуль интеграции с БД Postgres Pro;
 - модуль интеграции с ИС организации;
 - интеграция посредством шины данных;
 - модуль API сервиса для внешних систем.
- Разработка системы безопасности (аутентификация, авторизация, аудит);
- Внедрение СиЗИ в соответствии с проектом;
- Актуализация руководства пользователя;
- Актуализация руководства администратора.

Результаты этапа:

- Разработанная и развернутая в тестовой среде Система;
- Актуализированное руководство пользователя;
- Актуализированное руководство администратора;
- Актуализированное руководство администратора безопасности;
- Исходные коды Системы.

Этап 4. Тестирование

Содержание работ:

- Разработка Программы и методики испытаний (далее - ПМИ);
- Согласование ПМИ с заказчиком;
- Функциональное тестирование всех подсистем и модулей:
 - подсистема подготовки полевых материалов;
 - подсистема диспетчеризации;
 - модуль визуализации и работы с геоданными;
 - дашборды и аналитика;
 - мобильный контур.
- Интеграционное тестирование:
 - интеграция с БД Postgres Pro;
 - интеграция с ИС организации;
 - тестирование API сервиса.
- Нагрузочное тестирование:
 - проверка работы с большим количеством геометрий;
 - проверка работы при одновременном обращении множества пользователей;
 - оценка времени отклика системы.
- Тестирование безопасности:
 - разработка Программы и методики оценки соответствия системы защиты требованиям о безопасности информации (ПМИ СиЗИ).
 - проверка механизмов аутентификации и авторизации;
 - проверка разграничения прав доступа;
 - проверка аудита действий пользователей.

Конкретный перечень мер и мероприятий по защите информации формируется на этапе разработки ЧТЗ на СиЗИ в соответствии с классом ИС и уровнем защищённости персональных данных.

Приведенные проверки носят ориентировочный характер.

- Тестирование мобильного контура в офлайн-режиме;
- Оформление протоколов испытаний;
- Устранение выявленных ошибок и недостатков.

Результаты этапа:

- Программа и методика испытаний (ПМИ), согласованная с заказчиком;
- Программа и методика оценки соответствия системы защиты требованиям о безопасности информации (ПМИ СиЗИ);
- Заключение о соответствии СиЗИ требованиям о безопасности информации.

По результату этап должно быть заключение о соответствии к требованиям:

- Система, успешно прошедшая испытания и готовая к опытной эксплуатации;
- Отчет о результатах тестирования.

Этап 5. Опытная эксплуатация

Содержание работ:

- Развертывание Системы в опытной среде Заказчика;
- Настройка интеграций с БД Postgres Pro и ИС организации;
- Проведение опытной эксплуатации с участием пользователей Заказчика;
- Сбор замечаний и предложений от пользователей;
- Анализ замечаний и определение необходимых доработок;
- Доработка Системы по замечаниям опытной эксплуатации;
- Актуализация документации по результатам доработок:
- актуализация руководства пользователя;
- актуализация руководства администратора;
- актуализация руководства администратора безопасности.
- Повторное тестирование доработанного функционала;
- Подготовка отчета о проведении опытной эксплуатации.

Результаты этапа:

- Отчет о проведении опытной эксплуатации;
- Система, доработанная по замечаниям опытной эксплуатации;
- Актуализированное руководство пользователя;
- Актуализированное руководство администратора;
- Актуализированное руководство администратора безопасности;
- Документ о приемке этапа.

Этап 6. Ввод в промышленную эксплуатацию

Содержание работ:

- Развертывание Системы в промышленной среде Заказчика;
- Настройка интеграций с БД Postgres Pro и ИС организации в промышленной среде;
- Настройка резервного копирования и мониторинга;
- Проверка работоспособности Системы в промышленной среде;
- Ввод системы в промышленную эксплуатацию;
- Оформление акта приемки работ;
- Оформление документа о вводе в промышленную эксплуатацию.

Результаты этапа:

- Система, развернутая в промышленной среде и введенная в эксплуатацию;
- Акт приемки работ, подписанный заказчиком;
- Документ о вводе в промышленную эксплуатацию.

Этап 7. Обучение и передача документации

Содержание работ:

- Обучение пользователей работе с Системой:
- операторы подготовки полевых материалов;
- диспетчеры;
- линейные руководители;
- полевые исполнители (мобильный контур).
- Обучение администраторов Системы;
- Обучение администраторов Системы безопасности web-приложения;
- Подготовка программы обучения и учебных материалов;
- Проведение обучающих сессий (очно или дистанционно);
- Возможность создания видеозаписей обучающих сессий для последующего использования при обучении новых пользователей (по согласованию с заказчиком);
- Передача полного комплекта проектной и эксплуатационной документации;
- Передача регламентов эксплуатации и инструкций;
- Передача исходных кодов Системы (по требованию Заказчика).

Результаты этапа:

- Обученные пользователи и администраторы (подтверждается листами обучения/протоколами);
- Программа обучения и учебные материалы;
- Видеозаписи обучающих сессий (при наличии);
- Полный комплект документации, переданный заказчику:
- отчет об обследовании;
- технический проект;
- руководство пользователя;
- руководство администратора;
- руководство администратора безопасности;
- программа и методика испытаний (ПМИ);
- протоколы испытаний;
- отчет о проведении опытной эксплуатации;
- регламенты эксплуатации;
- исходные коды (по требованию).
- Документ о приемке этапа.

4. Объем и сроки гарантий качества

4.1. Гарантийный срок

Гарантийный срок на выполняемые работы составляет 365 (триста шестьдесят пять) дней с даты подписания сторонами документа о приемке работ.

4.2. Устранение недостатков

Если в период гарантийного срока Заказчиком будут обнаружены недостатки, то Исполнитель обязан устранить их за свой счет в срок, не превышающий 7 (семи) рабочих дней с момента предъявления соответствующего требования Заказчиком.

Гарантийный срок в этом случае продлевается на период устранения недостатков.

4.3. Недостатки, выявленные в ходе испытаний

Недостатки и ошибки, выявленные в ходе проведения испытаний, должны быть устранены Исполнителем в рамках выполнения работ до подписания акта приемки.

4.4. Недостатки, выявленные в период гарантийного обслуживания

Недостатки и ошибки, выявленные в период гарантийного обслуживания, устраняются Исполнителем в рамках очередного обновления Системы или в рамках внеочередного экстренного обновления в случае, если обнаруженные ошибки препятствуют или ограничивают эксплуатацию Системы в штатном режиме.

4.5. Актуализация документации

Исполнителем должны быть внесены соответствующие актуализирующие исправления в техническую и рабочую документацию, связанные с устранением замечаний к работе Системы, и предъявлены Заказчику до завершения срока гарантийного обслуживания.

5. Требования к безопасности выполнения работ

Обеспечение защиты информации при реализации функций web-приложения должно отвечать требованиям законодательства и нормативно-правовым актам в области защиты информации РФ. Исполнитель должен обладать лицензией ФСТЭК России на осуществление работ по технической защите конфиденциальной информации в части оказания услуг по проектированию средств и систем информатизации в защищенном исполнении, а также контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации (Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»).

При отсутствии у Исполнителя соответствующей лицензии ФСТЭК России, по согласованию с Заказчиком, Исполнитель вправе привлекать для работ по созданию подсистемы защиты информации подрядную организацию, имеющую лицензию ФСТЭК России на осуществление работ по технической защите конфиденциальной информации в части оказания услуг по проектированию средств и систем информатизации в защищенном исполнении, а также контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации (Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»).

В рамках анализа угроз безопасности информации, обрабатываемой в web-приложении, должны быть проведены следующие работы:

- определение перечня возможных угроз безопасности;
- определение негативных последствий от реализации угроз безопасности;
- определение объектов воздействия;
- определение нарушителей безопасности;
- разработку сценариев реализации угрозы безопасности в соответствии с методическим документом ФСТЭК России "Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021);
- определение уровня защищенности персональных данных в web-приложении.

После определения уровня защищенности составляется Акт определения уровня защищенности персональных данных в информационной системе персональных данных. (форма акта – Приложение № 2).

Исполнителем должна быть проведена классификация ИС, в результате которой составляется Акт классификации информационной (автоматизированной) Системы (форма акта – Приложение № 3).
Содержание Акта:

- разграничение ответственности в части защиты информации;
- определение уровня защищённости персональных данных;
- определение класса информационной системы;
- разработка модели угроз;
- разработка частного технического задания на систему защиты информации (ЧТЗ на СиЗИ);
- разработка проекта системы защиты информации (СиЗИ);
- внедрение СиЗИ;
- разработка ПМИ СиЗИ;
- оценка соответствия и аттестационные мероприятия относятся к зоне ответственности Заказчика, либо привлекаемого им исполнителя.

Исполнитель отвечает за реализацию в Системе встроенных механизмов защиты (аутентификация, ролевое разграничение доступа, Row Level Security, журналирование, защита каналов TLS/mTLS) и за предоставление исходных данных, необходимых для выполнения указанных мероприятий.

Перечисленные в разделе «Состав работ» работы по созданию системы защиты информации выполняются в указанном разграничении ответственности.

Должно быть разработано частное техническое задание на создание системы защиты информации web-приложения, при этом защитные меры должны быть адаптированы к актуальным угрозам безопасности информации, определённым при формировании модели угроз безопасности информации и классификации ИС.

Частное техническое задание (далее – ЧТЗ) на создание системы защиты информации должно содержать, в том числе, перечень подсистем защиты информации, обеспечивающих нейтрализацию актуальных угроз безопасности информации. Структура и содержание частного технического задания на создание системы защиты должны разрабатываться в соответствии с требованиями документа ГОСТ 34.602-2020. «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы». Система защиты информации информационной системы не должна препятствовать достижению целей создания ИС и ее функционированию.

При проектировании системы защиты информации ИС:

- определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным программным обеспечением, иные объекты доступа);
- определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в web-приложении;
- выбираются меры защиты информации, подлежащие реализации в системе защиты информации web-приложения;
- определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;
- определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;
- осуществляется выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и

особенностей их реализации, а также класса защищенности информационной Системы;

- определяются требования к параметрам настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей информационной Системы, приводящих к возникновению угроз безопасности информации;
- определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации. Результаты проектирования системы защиты информации web-приложения отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей документации) на web-приложение (систему защиты информации web-приложения), разрабатываемых с учетом ГОСТ 34.201 "Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем". При разработке системы защиты информации ИС должно учитываться ее информационное взаимодействие с иными ИС Учреждения. Требования по ИБ, предъявляемые к системе защиты информации на этапе формирования ЧТЗ, должны быть согласованы с Отделом защиты информации Заказчика.

Исполнителем должны быть представлены решения по управлению доступом, регистрации и учёту событий безопасности, обеспечению целостности и резервному копированию информации в соответствии с требованиями настоящего Технического задания и политикой безопасности Учреждения.

В случае интеграции разрабатываемого web-приложения с корпоративной сетью ГБУ «Мосгоргеотрест» реализованные в web-приложении решения по использованию средств аутентификации и авторизации должны обеспечивать выполнение требований, установленных Правилами управления доступом к ресурсам корпоративной сети ГБУ «Мосгоргеотрест».

5.1. Требования по защите персональных данных

При обработке персональных данных Система должна обеспечивать необходимые организационные и технические меры по обеспечению безопасности персональных данных в соответствии с требованиями законодательства РФ.

5.2. Работа с конфиденциальными данными

При работе с конфиденциальными данными Исполнитель должен руководствоваться нормативными правовыми актами Заказчика, а также иным нормативным правовым актам в области защиты конфиденциальной информации Российской Федерации.

5.3. Аутентификация и управление учётными записями

- аутентификация сетевых подключений к СУБД Postgres Pro должен выполняться методом SCRAM-SHA-256 (метод trust должен применяться исключительно для локальных соединений на адресе 127.0.0.1/32, любые сетевые подключения с методом trust запрещены);
- централизованное управление учётными записями пользователей должно осуществляться через систему Avanpost IDM Заказчика, предоставление и отзыв доступа автоматизированы в соответствии с утверждённой ролевой моделью и выполняются по регламенту IDM, интеграция должна выполняться по протоколу RADIUS / REST API на этапе пусконаладочных работ;
- многофакторная аутентификация (MFA) для критичных компонентов (административных интерфейсов и консолей управления) в текущем контуре не реализуется (Avanpost FAM в контуре не применяется);
- контроль привилегированного доступа (администраторов ИТ-инфраструктуры и ИБ) должен реализовываться средствами Indeed PAM с записью интерактивных сессий, полной фиксацией

действий и формированием аудиторских отчётов, прямой административный доступ должен осуществляться исключительно через шлюз привилегированного доступа Indeed PAM.

5.4. Криптографическая защита и управление секретами

- все сетевые соединения между компонентами должны быть защищены протоколом TLS версии не ниже 1.2, должен применяться единый внутренний удостоверяющий центр (CA) Заказчика, сертификаты должны быть размещены в каталоге /etc/pki/cluster/ на каждом узле кластера, ротация сертификатов должна выполняться по регламенту ИБ Заказчика;
- межузловая репликация Postgres Pro должна выполняться строго по TLS (директива hostssl); взаимодействие Patroni с etcd и REST API Patroni должна осуществляться по протоколу HTTPS с взаимной аутентификацией mTLS (порты 2379, 2380, 8008);
- аутентификационные данные (пароли СУБД, HAProxy, Keepalived, ключи шифрования pgBackRest) должны храниться в зашифрованном хранилище Ansible Vault (алгоритм AES-256-CBC), размещение секретов в репозиториях кода и журналах событий должно быть заблокировано средствами pre-commit хуков и политик аудита.

Схема защиты межкомпонентных коммуникаций приведена в таблице ниже.

Канал связи	Протокол / режим	Аутентификация
Client → HAProxy	TLS 1.2+	Серверный сертификат CA
HAProxy → PgBouncer	TCP (TLS passthrough)	—
PgBouncer → Postgres Pro	TLS 1.2+ (sslmode=require)	SCRAM-SHA-256
Репликация (hostssl)	TLS 1.2+	SCRAM-SHA-256 + серверный сертификат
Patroni → etcd (порт 2379)	HTTPS mTLS	Клиентский + серверный сертификат
etcd peer (порт 2380)	HTTPS mTLS	Клиентский + серверный сертификат
Patroni REST API (порт 8008)	HTTPS	Серверный сертификат

Данные требования к реализации мер защиты информации определяются на основании 117 приказа ФСТЭК России, Методического документа ФСТЭК России от 12.03.2026 после определения УЗ ПДн, классификации ИС и создания МУ на ИС перед формированием ЧТЗ на СиЗИ ИС.

5.5. Журналирование и аудит

- аудит SQL-операций уровня СУБД должен быть реализован на базе расширения pgaudit (загружается через shared_preload_libraries); конфигурация аудита должна управляться через Patroni DCS и применяться единообразно на всех узлах кластера (параметры: pgaudit.log = write, ddl, role; pgaudit.log_catalog = off; pgaudit.log_relation = on; pgaudit.log_statement_once = off);
- для анализа производительности должно применяться расширение pg_stat_statements; сквозная корреляция событий обеспечивается идентификаторами request_id (запрос) и txid (транзакция);
- источники событий централизованного журналирования: auditd (системные и привилегированные действия), sudo (команды с повышением привилегий), journald / syslog (события сервисов ОС), Web-логи, pg_log / pgaudit (SQL-события), HAProxy (события балансировщика);
- единый источник времени (NTP) должен обеспечивать синхронизацию часов на всех узлах кластера с допустимым смещением не более 100 мс;
- журналы должны передаваться в систему MR SIEM Заказчика по протоколу TCP/syslog с маршрутизацией через VM управления конфигурацией и шифрованием TLS; номинальный

объём событий — 50–150 EPS;

- срок хранения журналов должен быть не менее 1 (одного) года; целостность архивных журналов должна быть защищена контрольными суммами SHA-256 (реестр контрольных сумм ведётся отдельно от файлов журналов); доступ к каталогу pg_log на уровне ОС должен быть ограничен правами 0600 (владелец — postgres), операции удаления и модификации файлов журналов должны фиксироваться подсистемой auditd.

5.6. Изоляция данных на уровне строк (RLS)

Для изоляции данных на уровне строк по подразделениям Заказчика в СУБД Postgres Pro должен применяться механизм Row Level Security (RLS). Политики RLS должны определяться на уровне схем и таблиц основной базы данных mggt_dgn и обеспечивать автоматическую фильтрацию строк в зависимости от контекста сеанса (идентификаторы подразделения, переданного в переменной сеанса). Прикладной сервис должен устанавливать контекст сеанса при подключении; доступ к строкам других подразделений должен быть исключён без явного предоставления суперпользовательских прав. Детальная конфигурация политик RLS согласовывается с Заказчиком и фиксируется в документации на этапе ввода в эксплуатацию.

Исполнитель обязан:

- Обеспечить конфиденциальность информации, к которой получен доступ в рамках выполнения работ;
- Не разглашать информацию третьим лицам;
- Использовать информацию исключительно в целях выполнения работ по настоящему Техническому заданию;
- Соблюдать требования Заказчика по работе с конфиденциальной информацией.

5.7. Ответственность за распространение информации

Исполнитель несёт ответственность за распространение информации, к которой может получить доступ в рамках выполнения работ по Техническому заданию, в соответствии с законодательством Российской Федерации и условиями договора.

6. Требования к используемым материалам и оборудованию

6.1. Программное обеспечение

Система должна функционировать с использованием следующего программного обеспечения:

- СУБД: Postgres Pro с расширением PostGIS (инфраструктура и данные Заказчика, инсталляция за Исполнителем);
- Web-технологии для разработки портала (серверная и клиентская части) – конкретные технологии, фреймворки и библиотеки определяются Исполнителем на этапе проектирования и согласовываются с Заказчиком;
- В системе должны использоваться импортозамещенные программные продукты и компоненты;
- Система должна обеспечивать кроссплатформенность (поддержка различных операционных систем на стороне сервера);
- Система должна обеспечивать кроссбраузерность (поддержка современных web-браузеров: Chrome, Firefox, Safari, Edge);
- Средства разработки и тестирования предоставляются Исполнителем за свой счет.

6.2. Оборудование

- Требования к оборудованию (серверное оборудование, сетевое оборудование, средства защиты информации) определяются на этапе технического проектирования и требований к производительности Системы.
- Система должна функционировать на оборудовании, предоставляемом Заказчиком.

Оборудование, необходимое Исполнителю для выполнения работ (рабочие станции разработчиков, тестовые серверы), предоставляется Исполнителем за свой счет.

7. Перечень нормативных правовых и нормативных технических актов

7.1. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

7.2. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных".

7.3. Постановление Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

7.4. Постановление Правительства РФ от 06.07.2015 N 676 "О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации".

7.5. Закон г. Москвы от 24.10.2001 N 52 "Об информационных ресурсах и информатизации города Москвы".

7.6. Распоряжение Правительства Москвы от 03.07.2012 N 342-РП "О требованиях к вводу в эксплуатацию информационных систем, создаваемых в городе Москве".

7.7 Приказ ФСБ России от 18.03.2025 N 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»

7.8 Приказ ФСТЭК России от 11 апреля 2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

7.9 Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

7.10 Распоряжение Правительства Москвы от 03 июля 2012 № 342-РП «О требованиях к вводу в эксплуатацию информационных систем, создаваемых в городе Москве».

7.11. Постановление Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

Перечень объектов закупки

1. Работы по внедрению информационных систем и ресурсов			
Характеристики	Объем (единица измерения)	Адрес	Срок
Вид работ: Внедрение.	1 (Условная единица)	Город Москва, проспект Ленинградский, дом 11	с 1-го по 100-й календарный день с даты заключения контракта.

Приложение № 2 к Техническому заданию

Акт определения уровня защищенности персональных данных в информационной системе персональных данных *«Название*

ИС»

	УТВЕРЖДАЮ Первый заместитель Управляющего ГБУ «Мосгоргеотрест» И.О. Фамилия «_____» _____ 202_ г.
--	--

По результатам проведенного анализа исходных данных информационной системы персональных данных *«Название ИС»* в соответствии с постановлением Правительства РФ от 01.11.2012 №1119

«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее - Постановление) были установлены следующие характеристики обработки персональных данных:

1. Категории субъектов персональных данных: в *«Название ИС»* обрабатываются персональные данные работников ГБУ «Мосгоргеотрест».
2. Категории обрабатываемых персональных данных: В *«Название ИС»* не обрабатываются специальные и биометрические категории персональных данных. Категория персональных данных, обрабатываемых в *«Название ИС»* - указать категорию персональных данных:
 - перечислить персональные данные, обрабатываемые в «Название ИС».

3. Количество субъектов персональных данных: В *«Название ИС»* обрабатываются персональные данные указать количество субъектов персональных данных.

4. Актуальные угрозы: Для *«Название ИС»*. актуальны указать тип актуальных угроз.

На основании полученных данных, согласно подпункту «б» пункта 12 Постановления в *«Название ИС»*., необходимо обеспечить **указать уровень защищенности персональных данных**.

Настоящий Акт определения уровня защищенности персональных данных *«Название ИС»* действителен при отсутствии изменений в пунктах 1-4.

Начальник отдела защиты информации ГБУ «Мосгоргеотрест»		Фамилия И.О.
--	--	--------------

Приложение № 3 к Техническому заданию

УТВЕРЖДАЮ

Первый заместитель Управляющего
ГБУ «Мосгоргеотрест»

И.О. Фамилия

«_____» _____ 202_ г.

АКТ

классификации информационной (автоматизированной) системы

(наименование информационной (автоматизированной) системы)

Комиссия, назначенная приказом _____, провела классификацию информационной (автоматизированной) системы

Комиссия установила:

1. Масштаб информационной (автоматизированной) системы _____.
2. Уровень значимости информации, содержащейся в информационной (автоматизированной) системе
_____.
3. Класс защищенности информационной (автоматизированной) системы _____.

Члены комиссии:

(должность)

(подпись, фамилия и инициалы)

(должность)

(подпись, фамилия и инициалы)