

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Система управления доступами (IDM System)

Версия: 2.0 **Дата:** 27 января 2026 г. **Заказчик:** ОАО "Ориёнбонк"

Исполнитель: Отдел информационных технологий

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование системы

Полное наименование: **Система управления идентификацией и доступом**

Краткое наименование: **IDM System**

1.2. Назначение системы

IDM System предназначена для автоматизации процессов управления доступом сотрудников к корпоративным информационным системам, включая: - Централизованный запрос доступа к системам - Многоуровневое согласование заявок - Аудит и контроль предоставленных доступов - Автоматизация жизненного цикла доступа

1.3. Цели создания системы

- Повышение безопасности за счёт контролируемого предоставления доступа
- Сокращение времени на обработку заявок на доступ
- Обеспечение прозрачности процесса согласования
- Соответствие требованиям регуляторов (НБТ, ISO 27001)
- Снижение операционных рисков

2. ТРЕБОВАНИЯ К СИСТЕМЕ

2.1. Функциональные требования

2.1.1. Модуль аутентификации

ID	Требование	Приоритет
AUTH-01	Интеграция с Active Directory (LDAP)	Высокий
AUTH-02	JWT-токены для API авторизации	Высокий
AUTH-03	Автоматическое обновление токенов	Высокий
AUTH-04	Двухфакторная аутентификация (2FA)	Средний
AUTH-05	Управление сессиями пользователей	Средний

2.1.2. Модуль управления заявками

ID	Требование	Приоритет
REQ-01	Создание заявки на доступ	Высокий
REQ-02	Многоуровневое согласование	Высокий
REQ-03	Отслеживание статуса заявки	Высокий
REQ-04	Комментирование заявок	Высокий
REQ-05	История изменений заявки	Высокий
REQ-06	Массовые заявки	Средний
REQ-07	Шаблоны заявок	Средний
REQ-08	Делегирование согласования	Средний

2.1.3. Модуль управления системами

ID	Требование	Приоритет
SYS-01	Каталог информационных систем	Высокий
SYS-02	Роли доступа для каждой системы	Высокий

ID	Требование	Приоритет
SYS-03	Подсистемы и компоненты	Средний
SYS-04	Цепочки согласования	Высокий
SYS-05	Владельцы систем	Высокий

2.1.4. Модуль администрирования

ID	Требование	Приоритет
ADM-01	Управление пользователями	Высокий
ADM-02	Управление ролями и правами	Высокий
ADM-03	Журнал аудита	Высокий
ADM-04	Экспорт данных (PDF, Word, Excel)	Средний
ADM-05	Настройка системы	Средний

2.1.5. Модуль уведомлений

ID	Требование	Приоритет
NOT-01	Email-уведомления о статусе заявок	Высокий
NOT-02	Telegram-бот для уведомлений	Средний
NOT-03	Push-уведомления в браузере	Низкий
NOT-04	Настройка типов уведомлений	Средний

2.1.6. Модуль отчётности и аналитики

ID	Требование	Приоритет
REP-01	Дашборд со статистикой	Высокий
REP-02	Отчёт по заявкам за период	Высокий
REP-03	Матрица доступов	Средний
REP-04	Графики и диаграммы	Средний

ID	Требование	Приоритет
REP-05	Экспорт отчётов	Средний

2.1.7. Дополнительные функции

ID	Требование	Приоритет
ADD-01	Тёмная тема интерфейса	Низкий
ADD-02	Мультиязычность (RU/EN/TJ)	Низкий
ADD-03	Глобальный поиск	Средний
ADD-04	Мобильная адаптация	Средний

2.2. Нефункциональные требования

2.2.1. Производительность

- Время отклика страниц: не более 2 секунд
- Одновременных пользователей: не менее 100
- Время обработки API запроса: не более 500 мс

2.2.2. Безопасность

- Шифрование данных при передаче (HTTPS/TLS 1.3)
- Хеширование паролей (bcrypt)
- Защита от CSRF, XSS, SQL-инъекций
- Журналирование всех действий пользователей

2.2.3. Доступность

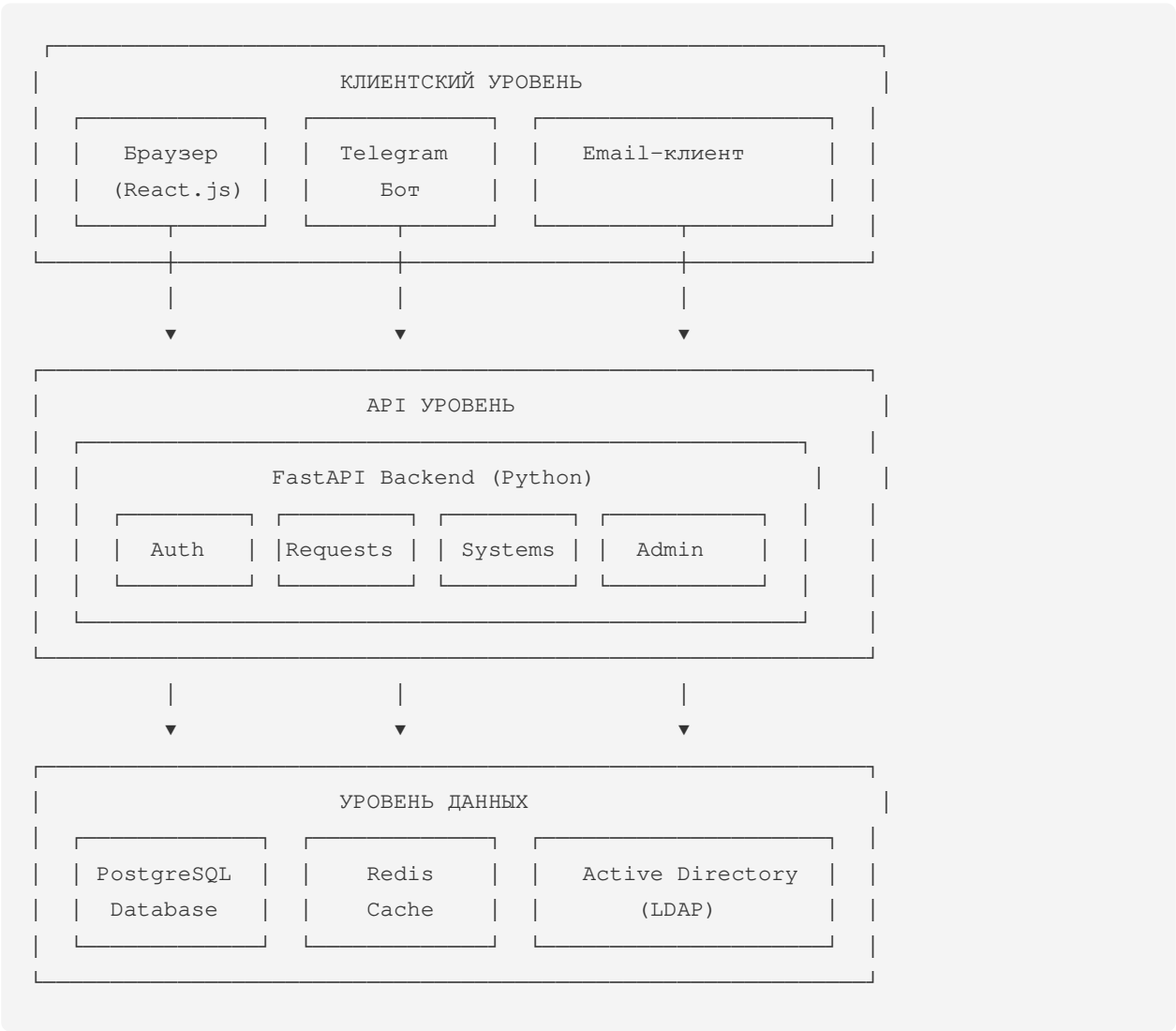
- Режим работы: 24/7
- Допустимое время простоя: не более 4 часов в месяц
- Резервное копирование: ежедневно

2.2.4. Масштабируемость

- Горизонтальное масштабирование backend
 - Кэширование (Redis)
 - Асинхронная обработка задач
-

3. АРХИТЕКТУРА СИСТЕМЫ

3.1. Общая архитектура



3.2. Технологический стек

Компонент	Технология	Версия
Frontend	React.js + Vite	18.x
UI Framework	Tailwind CSS	3.x
Backend	FastAPI (Python)	0.100+
База данных	PostgreSQL	15+
Кэш	Redis	7+

Компонент	Технология	Версия
Аутентификация	LDAP / JWT	-
Email	SMTP (aiosmtplib)	-
Telegram	python-telegram-bot	20+

3.3. Структура базы данных

Основные таблицы:

- **users** — пользователи системы
- **roles** — роли пользователей
- **permissions** — права доступа
- **systems** — информационные системы
- **access_roles** — роли доступа к системам
- **access_requests** — заявки на доступ
- **approvals** — согласования заявок
- **audit_logs** — журнал аудита

4. ОПИСАНИЕ ФУНКЦИЙ

4.1. Email-уведомления

Назначение: Автоматическая отправка уведомлений о статусе заявок на электронную почту.

Типы уведомлений: 1. Новая заявка создана (для согласующих) 2. Заявка согласована/отклонена (для заявителя) 3. Заявка ожидает вашего согласования 4. Напоминание о просроченной заявке 5. Доступ скоро истекает

Технические требования: - SMTP-сервер с поддержкой TLS - HTML-шаблоны писем - Очередь отправки (Redis Queue) - Логирование отправленных писем

4.2. Telegram-бот

Назначение: Мгновенные уведомления и быстрое согласование через Telegram.

Функции бота: 1. `/start` — привязка Telegram к учётной записи 2. `/my_requests` — список моих заявок 3. `/pending` — заявки на согласование 4. Inline-кнопки для согласования/отклонения 5. Уведомления о новых заявках

Технические требования: - Telegram Bot API - Webhook или Long Polling - Привязка telegram_id к пользователю - Защита от несанкционированного доступа

4.3. Тёмная тема

Назначение: Альтернативная цветовая схема для комфортной работы.

Реализация: - CSS-переменные для цветов - Переключатель в настройках профиля - Сохранение предпочтения в localStorage - Автоопределение системной темы

Цветовая схема: | Элемент | Светлая тема | Тёмная тема |
|-----|-----|-----| | Фон | #FFFFFF | #1a1a2e | | Текст | #1F2937 | #E5E7EB | | Акцент | #16306C | #3B82F6 | | Карточки | #FFFFFF | #16213e |

4.4. Дашборд статистики

Назначение: Визуальное отображение ключевых метрик системы.

Виджеты дашборда: 1. **Счётчики:** - Всего заявок за период - Ожидают согласования - Согласовано / Отклонено

1. Графики:

- Динамика заявок по дням/неделям
- Распределение по системам (pie chart)
- Среднее время согласования

5. Топ-списки:

- Самые запрашиваемые системы
- Активные пользователи
- Медленные согласования

Фильтры: - Период (день/неделя/месяц/год) - Система - Статус заявки - Подразделение

5. ЭТАПЫ РАЗРАБОТКИ

Этап 1: MVP (Реализовано)

- ☒ Аутентификация через AD
- ☒ Создание и согласование заявок
- ☒ Управление системами и ролями
- ☒ Журнал аудита
- ☒ Экспорт данных

Этап 2: Уведомления (Планируется)

- ☐ Email-уведомления
- ☐ Telegram-бот
- ☐ Настройки уведомлений

Этап 3: Аналитика (Планируется)

- ☐ Дашборд статистики
- ☐ Расширенные отчёты
- ☐ Графики и диаграммы

Этап 4: UI/UX (Планируется)

- ☐ Тёмная тема
- ☐ Мобильная адаптация
- ☐ Мультиязычность

6. ТРЕБОВАНИЯ К ИНФРАСТРУКТУРЕ

6.1. Серверные требования

Параметр	Минимум	Рекомендуется
CPU	2 ядра	4 ядра
RAM	4 GB	8 GB
Диск	50 GB SSD	100 GB SSD
ОС	Ubuntu 22.04	Ubuntu 22.04

6.2. Сетевые требования

- Доступ к LDAP-серверу (порт 389/636)
 - Доступ к SMTP-серверу (порт 587/465)
 - Доступ к Telegram API (api.telegram.org)
 - Открытые порты: 80, 443, 8000
-

7. ПРИЛОЖЕНИЯ

Приложение А: Глоссарий

- **IDM** — Identity Management (Управление идентификацией)
- **LDAP** — Lightweight Directory Access Protocol
- **JWT** — JSON Web Token
- **SoD** — Segregation of Duties (Разделение обязанностей)

Приложение Б: Ссылки

- Репозиторий: <https://github.com/Adminpm04/idm-system>
 - API документация: /api/docs (Swagger)
-

Согласовано:

Роль	ФИО	Подпись	Дата
Заказчик	_____	_____	—
Руководитель проекта	_____	_____	—
Технический директор	_____	_____	—