

HR CRM

Ответы на технические вопросы. Для специалиста покупателя.

Документ отвечает на то, что обычно проверяют перед покупкой работающей системы. Пределы и нерешённые вопросы названы прямо: их всё равно видно в коде, и лучше обсудить их до сделки.

1. Стек и архитектура

Слой	Решение
Серверная часть	Python 3.11, FastAPI, SQLAlchemy Core
База данных	PostgreSQL 17, миграции Alembic
Интерфейс	HTML, CSS, JavaScript без сборки и внешних зависимостей
Развёртывание	Ubuntu 24.04, systemd, nginx, uvicorn
Обновления в реальном времени	Server-Sent Events

Один процесс приложения и одна база на той же машине. Внешних сервисов в работе нет: система не зависит от сторонних платных API и работает в закрытом контуре, если это потребуется.

Доступ к таблицам вынесен в отдельные модули по сущностям: пользователи, сессии, кандидаты, комментарии, журнал, настройки выгрузки. Маршруты, проверка прав и рассылка событий собраны в одном модуле.

2. Аутентификация

- Вход по логину и паролю, сессия в cookie с флагами httpOnly и Secure, режим SameSite=lax. Идентификатор сессии хранится в базе, срок жизни настраивается.
- Пароли хранятся как PBKDF2-SHA256 с индивидуальной солью и 200 000 итераций. Обратимого хранения паролей нет нигде, включая резервные копии.
- Пять неудачных попыток по паре «логин плюс адрес» дают паузу на 15 минут с кодом 429. Счётчик проверяется до вычисления хеша, поэтому перебор не нагружает процессор.
- Для несуществующего логина считается хеш-пустышка: по времени ответа нельзя определить, какие логины существуют.
- Пароль владельца через программный интерфейс не сбрасывается вообще, включая администратора системы. Меняется самим владельцем или напрямую в базе.

3. Разграничение доступа

Права проверяются на сервере. Интерфейс скрывает недоступные действия, но это оформление, а не защита: запрос в обход интерфейса получает отказ.

Видимость кандидата вычисляется чистой функцией от роли, идентификатора, команды и самого кандидата, без обращения к базе. Та же функция фильтрует получателей

событий в реальном времени, поэтому правило видимости существует в системе в одном экземпляре и не может разойтись между списком и рассылкой.

Поля контактов и реальной суммы вырезаются из ответа сервера для тех ролей, которым не положены. Клиент их не получает физически.

Матрица прав зафиксирована автоматическим тестом: 28 проверок по пяти ролям, включая проверки того, что владелец *не* имеет доступа к административным разделам. Это намеренное разделение бизнес-контура и системного, а не упущение.

4. Защита от типовых атак

Вектор	Состояние
Внедрение SQL	Запросы параметризованы через SQLAlchemy Core, строки не собираются конкатенацией. Проверено сплошным просмотром слоя доступа к данным.
Внедрение кода на странице	Проведён сплошной аудит всех 63 мест вставки разметки: данные пользователя проходят через экранирование, выпадающие списки собираются через текстовые узлы. Пригодных для внедрения мест не найдено.
Запрос с чужого сайта	Каждый изменяющий запрос сверяется по заголовку источника со списком разрешённых адресов; несовпадение даёт отказ и запись в журнале. Заголовок источника браузер проставляет сам и подделать его из скрипта нельзя.
Подбор пароля	Ограничение частоты попыток, блокировка на 15 минут, защита от определения существующих логинов.
Подмена адреса клиента	Заголовкам обратного прокси система доверяет только с локального адреса; извне подделать их нельзя.
Исчерпание памяти	Тело запроса ограничено 2 МБ, число одновременных потоков событий на пользователя — 12, размер служебных словарей ограничен сверху.

5. База данных

Семь таблиц: сотрудники, сессии, кандидаты, комментарии, журнал действий, настройки выгрузки и служебная таблица версий схемы. Схема ведётся миграциями, версия хранится в базе, состояние схемы всегда определено.

Номера кандидатов не переиспользуются: номер удалённого кандидата не достаётся новому, иначе к нему подтянулись бы чужие комментарии и записи журнала. Номер выдаётся под блокировкой базы, поэтому одновременные создания получают разные номера.

Удаление сотрудника — это архивация: история кандидатов, переписки и журнала сохраняется, учётная запись перестаёт работать.

6. Резервное копирование

- Ежедневная выгрузка базы по расписанию, хранение локальных копий 30 дней, зеркало в отдельном внешнем хранилище.
- Скрипт сверяет версию схемы источника и приёмника и отказывается работать при расхождении. Практическое следствие: новая миграция обязана применяться и к базе резервных копий, иначе копирование останавливается.
- Восстановление выполняется штатными средствами PostgreSQL, порядок описан в документации по эксплуатации.

Учебное восстановление из копии на тестовой базе рекомендуется провести при приёмке, в присутствии обеих сторон.

7. Обновление и остановка

Обновление — замена файлов и перезапуск сервиса; порядок шагов описан в документации. Миграции применяются отдельной командой, к каждой из баз.

Остановка корректная: при получении сигнала приложение закрывает открытые потоки событий и завершается примерно за 0,2 секунды, не обрывая соединения по таймауту. Проверено замером на работающем сервере с открытыми клиентскими вкладками.

Простая при обновлении около двух секунд. Открытые вкладки переподключаются сами.

8. Обновления в реальном времени

Поток событий на отдельном маршруте. События несут только идентификатор кандидата и вид действия; содержимое клиент запрашивает обычными запросами, которые проверяют права. Это значит, что через поток событий невозможно получить данные, которые роли не положены.

Очередь событий живёт в памяти процесса. Отсюда два следствия, которые надо знать:

- приложение работает в один процесс; для нескольких процессов потребуется внешний брокер — Redis или механизм уведомлений PostgreSQL;
- после перезапуска пропущенные события не восстанавливаются, клиент догоняет состояние ближайшим запросом списка.

Для одной компании ограничение непринципиально: один процесс держит проверенные 78 одновременных подключений без потерь и деградации.

9. Тестирование

Автоматический тест ходит по программному интерфейсу как обычный клиент и проверяет то, что дороже всего сломать: права по всем пяти ролям, адресность рассылки событий и поведение под нагрузкой. Последний прогон: **51 проверка, 0 провалов**.

Непрерывная интеграция настроена: на каждое изменение поднимается чистая PostgreSQL, ставятся зависимости, проверяется синтаксис, отрабатывает линтер, применяются миграции и сверяется синхронность файлов интерфейса.

Что тестами не покрыто: поведение в браузере — звук уведомлений, индикаторы непрочитанного, перерисовка списка. Проверяется вручную. Это честное ограничение автоматизации по программному интерфейсу.

10. Производительность

Замеры на одном процессе, 78 одновременных подключений, 140 записей в базу за минуту, десять параллельных читателей.

Операция	В покое	Под нагрузкой
Список кандидатов	13 мс	63 мс, 99-й перцентиль 153 мс
Комментарии по кандидату	—	26 мс
Добавление комментария	—	30 мс
Смена статуса	—	19 мс
Доставка события коллегам	25 мс	37 мс, 99-й перцентиль 233 мс

Потерь событий нет, оборванных подключений нет, ошибок сервера нет. Разница между спокойным режимом и нагрузкой по доставке событий — в полтора раза.

11. Пределы и нерешённые вопросы

Перечислено прямо. Ни одно из этого не мешает системе работать сегодня, но об этом лучше знать заранее.

Вопрос	Суть и что с этим делать
Горизонтальное масштабирование	Один процесс из-за очереди событий в памяти. Решается переходом на внешний брокер. Требуется при переходе к сотням одновременных пользователей.
Загрузка списка кандидатов целиком	Список читается полностью и фильтруется по правам в приложении. При десятках записей это 13 мс. Заметное замедление ожидается в районе десятков тысяч записей, тогда потребуется страничная загрузка и доработка интерфейса.
Одновременное редактирование	Правки соседних полей не затирают друг друга. Конфликт двух правок одного и того же поля решается в пользу последнего запроса; блокировок и предупреждений нет.
Выгрузка в Google Таблицы	Доведена до настройки и предпросмотра. Реальная запись требует учётной записи сервиса покупателя и доработки.
Наблюдаемость	Есть журнал запросов с кодами ответа и длительностью. Сбора метрик и оповещений нет: при необходимости подключается стандартными средствами.
Ограничение частоты на уровне nginx	Ограничение попыток входа работает в приложении. Дополнительный заслон на уровне nginx описан в документации и настраивается за несколько минут.
Сопровождение	Система написана одним разработчиком. Документация полная, но передача знаний второму человеку — организационная задача покупателя.

12. Что нужно для самостоятельной проверки

Всё перечисленное проверяется покупателем без участия продавца.

- Исходный код целиком, включая тесты и настройки непрерывной интеграции.
- Документация по установке с нуля: система разворачивается на чистом сервере по инструкции, без скрытых шагов.
- Запуск автоматического теста на собственной копии базы: результат должен быть 51 проверка и 0 провалов.
- Доступ к работающему серверу для просмотра журналов, схемы базы и настроек.