

Технический аудит доступа к данным CRM

Пример результата ограниченного разбора

Вымышленная CRM для нескольких клиник. Laravel, Python и PostgreSQL. Владельцы хотят подключить вторую клинику и понять, изолированы ли её записи от первой.

Что входит в этот пример

Один сценарий: сотрудник клиники читает карточку звонка и её AI-транскрипт, а затем выгружает список звонков. Рассматриваем серверные права, принадлежность записей клинике и отзыв доступа.

Формат пакета

На лендинге: технический аудит от 39 000 руб., до 7 часов. В этом условном примере согласован пакет 39 000 руб. с лимитом 7 часов, включая разбор, подготовку отчёта и обсуждение выводов.

Если согласованная проверка выполнена быстрее, цена пакета сохраняется. Если лимита недостаточно, передаём выполненную часть, фиксируем непроверенное и согласуем продолжение до дополнительных расходов.

Результат

Три наблюдения с основаниями и последствиями, порядок исправлений и предварительная оценка следующего этапа. Изменения кода и повторная проверка после внедрения оплачиваются отдельно.

Версия 2.0 / 6 октября 2026. Все данные, пути API и наблюдения вымышлены. Клиентские системы не проверялись.

Что выяснили в выбранном сценарии

Решение для владельца

В демонстрационном сценарии не подключать вторую клинику к проверенным функциям до исправления серверного доступа и проверки экспорта. Работу остальных функций этот разбор не оценивает.

01 / Исправить до подключения второй клиники

В модели карточка звонка доступна по идентификатору без проверки клиники на сервере. Скрытая ссылка в интерфейсе не защищает запись от прямого запроса. Подробности на странице 3.

02 / Исправить перед выдачей доступов сотрудникам

В модели удалённый из клиники сотрудник сохраняет доступ через действующую сессию. Нужна проверка актуального членства при обращении к данным. Подробности на странице 4.

03 / Проверить до включения экспорта

Изоляция выгрузки не подтверждена: в модели недоступен обработчик фоновой задачи. Это пробел проверки, а не доказанное раскрытие данных. Подробности на странице 4.

На чём основан разбор

Модель включает просмотр выбранного кода API и политики доступа, схемы данных и синтетический тест в отдельной среде. Выводы ограничены этими материалами и указанным сценарием.

Вне объёма: AI-сервис транскрибации, резервные копии, облачная сеть, нагрузка, остальные роли и функции. Пентест и юридическая экспертиза не проводятся. Общей оценки безопасности или готовности всей CRM этот документ не даёт.

Карточка чужой клиники доступна по идентификатору

Статус в модели: подтверждено / Приоритет: до подключения второй клиники

Основание

Вымышленный GET /api/calls/{id} находит запись по ID без ограничения clinic_id. В синтетическом тесте сотрудник клиники А получает HTTP 200 и тестовую расшифровку звонка клиники В. Это иллюстрация доказательства для реального отчёта.

Последствие для бизнеса

Сотрудник одной клиники может прочитать звонки и транскрипты другой. Ошибка затрагивает границу между организациями, а не только отображение интерфейса.

Что изменить

Проверять право пользователя на клинику и конкретную запись на сервере. Ограничить выборку доступной организацией и проверить связанные операции с транскриптом. Не полагаться на скрытие ссылок.

Как принять исправление

В отдельной среде с тестовыми данными: свой звонок доступен; чужой звонок и транскрипт недоступны; анонимный запрос отклонён. Ответ не содержит чужих данных. Сохранить автоматические проверки этих случаев.

Предварительная оценка доработки

3-5 часов на этот путь API и связанные проверки, если модель ролей уже существует. Если аналогичная проблема есть в других функциях, их обследование и исправление оцениваются отдельно.

В этом демо исправления не выполнялись. Подтверждение ошибки в модели не означает, что найдена ошибка в реальном клиентском продукте.

Отзыв доступа и экспорт звонков

02 / Удаление сотрудника не прекращает доступ

Статус в модели: подтверждено. Приоритет: до выдачи доступов.

Основание: после удаления тестового сотрудника из клиники действующая сессия всё ещё позволяет прочитать её звонок. В модели роль сохранена в сессии и актуальное членство не проверяется.

Изменение: проверять действующее членство и корректно отзывать связанные права.

Приёмка: удалённый сотрудник не читает данные ни через прежнюю сессию, ни после нового входа; действующий сотрудник сохраняет разрешённый доступ.

Оценка: 2-3 часа при существующем механизме сессий и членства.

03 / Изоляция экспорта не подтверждена

Статус в модели: не проверено. Приоритет: до включения экспорта.

Основание: просмотрен код запуска выгрузки, но код фонового обработчика и выдачи файла отсутствует в материалах. Нельзя подтвердить, что в файл попадают только звонки своей клиники.

Следующий шаг: получить обработчик и конфигурацию хранения файлов, проверить границы выборки и доступ к скачиванию на синтетических данных. До подтверждения ограничить экспорт для нового контура.

Дополнительная проверка: 1-2 часа после получения материалов, вне исходного пакета. Объём исправлений определяется по её результату.

Непроверенная область остаётся открытым вопросом. Отсутствие материалов не доказывает наличие ошибки.

План, оценка и передача результата

Порядок действий

1. Исправить доступ к карточке и транскрипту: 3-5 часов.
2. Исправить отзыв прав сотрудника: 2-3 часа.
3. Проверить экспорт после получения материалов: 1-2 часа.
4. Перед подключением второй клиники зафиксировать результаты проверок и оставшиеся ограничения.

Как соотносить с услугами

Две известные доработки: предварительно 5-8 часов, включая проверки из описаний. На лендинге пакет «Исправления и доработки» начинается от 59 000 руб. с лимитом 10 часов. Возможность включить обе задачи, передачу и коммуникацию в такой пакет подтверждаем до старта. Проверка экспорта и обнаруженные в ней изменения требуют отдельного согласования.

Как принимаем выполненные изменения

Передаём изменения кода, список проверенных сценариев, среду и результаты проверки. Для каждой находки фиксируем статус: открыта, исправлена и проверена либо требует дополнительных данных. Оставшиеся ограничения перечисляем явно.

Что остаётся у владельца после аудита

Этот отчёт, приоритеты и предварительная оценка. Их можно передать своей команде. Продолжение с VRIBE необязательно. Итоговая цена и срок следующего этапа согласуются до работы; облако и внешние сервисы оплачиваются отдельно.

Аудит помогает выбрать следующий шаг. Он не включает исправления автоматически и не подтверждает готовность всей системы к запуску. В реальном проекте объём, материалы и критерии определяются вашей задачей.