1. Личные границы и данные

Наш подход

Мы добросовестно относимся к личной информации и уважаем ваши границы. Не публикуем персональные данные и не продаём их. Используем информацию для работы кабинета, общения, исполнения заказа и оформления документов.

Какие данные нужны

Кабинет использует контактные данные, сведения о проекте, сообщения и вложения. Данные для договора запрашиваются на этапе его подписания. Доступы к инфраструктуре передаются через защищённую форму, а не публичные сообщения. Не присылайте данные банковской карты, CVV и коды подтверждения в чат.

Кто участвует в обработке

Данные кабинета размещены на инфраструктуре Selectel в России. Для онлайн-платежа необходимая информация передаётся ЮКассе. Сервис доставки уведомлений обрабатывает данные, необходимые для уведомления; подробные паспортные сведения и секреты не предназначены для таких сообщений. Условия обработки и права пользователя описаны в политике конфиденциальности.

Ваши возможности

Можно обращаться к администратору по вопросам данных и безопасности через «Написать нам». Для чувствительных сведений используйте специально предусмотренные поля. После настройки внешних сервисов рекомендуем менять переданные пароли самостоятельно.

2. Защита доступа и документов

Разделение прав

Доступ клиента и администратора разделён. Правила базы проверяют права на каждой операции; скрытие кнопки не заменяет серверную проверку. Клиент не может сам назначить себе роль администратора. Проверены сценарии чужого проекта и попытки изменения системных данных.

Изоляция данных

В таблицах с прикладными данными действуют политики доступа по строкам (RLS). Документы и вложения хранятся в закрытых разделах хранилища. Ссылки для доступа выдаются с ограниченным сроком. Чувствительные значения защищённых реквизитов шифруются в базе; ключи не включаются в публичные страницы.

Защищённое соединение

Кабинет и API работают по HTTPS. Настроены HSTS, ограничение источников ресурсов (CSP), запрет подмены типа содержимого и ограничения встраивания страниц.

Секреты и сервер

Ключ платёжного сервиса и служебные ключи остаются на сервере. Закрытые служебные файлы не выдаются через сайт. База не опубликована как открытый внешний сервис. Защитные ограничения и блокировка повторных попыток входа на сервере уменьшают риск перебора.

3. Защита денежных операций

Данные карты

Онлайн-оплата выполняется на стороне ЮКассы: платёжные карты и банковские коды не вводятся в кабинете. Для реферальной выплаты получатель отдельно сохраняет номер карты и банк: они зашифрованы на сервере и привязаны к его аккаунту. Клиент видит только последние четыре цифры; администратор открывает реквизиты для начисленной выплаты. CVV и банковские коды не запрашиваются.

Стоимость и права

Платёж создаёт сервер для счёта конкретного клиента. Стоимость берётся из согласованных условий, а не из значения, переданного браузером. Предоплата и доплата составляют по 50% согласованной суммы. Изменения после согласования оформляются отдельным связанным проектом.

Проверка результата

Возврат пользователя со страницы оплаты сам по себе не подтверждает поступление денег. Сервер сверяет статус через API провайдера, сумму, валюту, магазин и связь с нужным счётом. Уведомления провайдера проходят проверку; предусмотрена резервная сверка статусов.

Повторы и ограничения

Идемпотентность и контроль состояния защищают от повторного создания одной операции. Проверяются авторизация, схема запроса, допустимый размер, источники обращений и частота запросов. Проверены поддельные уведомления, несоответствие суммы и попытки доступа к чужому счёту.

Чеки

Для НПД владелец оформляет чеки через «Мой налог».

4. Проверки и обслуживание

Что проверено к 06.10.2026

Проведены проверки прав в настоящей базе с откатом тестовых изменений: роли, согласования, договор, документы и платёжные состояния. Проверены платёжные HTTP-функции с подменённым внешним API, включая ошибки и поддельные события. Публичные файлы сверены по SHA-256; закрытые технические пути не доступны через HTTP.

Критерии защиты

Чужие данные недоступны; роль клиента не повышается самостоятельно; платёж подтверждается только после серверной сверки; секреты не попадают в выдачу сайта; повтор не создаёт повторный платёж; защищённые действия требуют авторизации. Изменения публикуются с резервной копией и повторной проверкой.

Восстановление и обслуживание

Настроены ежедневные локальные резервные копии и ограничение их хранения. Требуются регулярные обновления, контроль журналов, проверка восстановления и пересмотр прав.

Связь с нами

Документ не раскрывает ключи, личные сведения и служебные секреты. Если у вас есть вопрос о своих данных, используйте «Написать нам» в кабинете.

Безопасный сервис для вашего бизнеса

Хотите иметь такой же безопасный сервис под свой бизнес? Мы это реализуем! Обсудите с нами задачу и необходимые меры защиты: https://institut21.ru/cabinet.html#support