Список требований для внешних интеграций

Требования к безопасности

Шифрование данных: Все данные, передаваемые между системами, должны быть защищены с использованием TLS/SSL.

Защита персональных данных: Должны быть внедрены механизмы защиты персональных данных, соответствующие требованиям законодательства РФ.

Протоколы аутентификации и авторизации

OAuth 2.0: Должен использоваться для обеспечения безопасной авторизации и аутентификации пользователей и сервисов.

JWT (JSON Web Tokens): Рекомендуется для обеспечения безопасности передачи данных между клиентом и сервером, а также для подтверждения подлинности.

Организация взаимодействия между системами

Сервис Интегратор: Введение точки интеграции, которая будет управлять и контролировать доступ к новым сервисам.

Мониторинг и аудит: Разработать системы мониторинга и журналирования для отслеживания взаимодействий между системами и фиксации потенциальных инцидентов.