**Анализ системы и выбор разделов для проверочного листа безопасности**

**Идентификация систем и их работа с точки зрения безопасности**

1. **Группа сервисов для продаж**:
   * Витрина продаж, client-tour-app, client-mart-app, client-crm-app, client-mart-estate-app.
   * Каждое приложение (кроме витрины) имеет собственную базу данных.
   * Основные риски: утечка данных клиентов, несанкционированный доступ к данным о недвижимости, уязвимости в API для онлайн-сделок.
2. **Группа сервисов ЖКУ**:
   * Витрина, tenant-core-app, CRM для собственников.
   * Основные риски: утечка персональных данных собственников, несанкционированный доступ к данным о ЖКУ, уязвимости в API для оплаты услуг.
3. **Финансы**:
   * Accountant-service-1 и служба каталогов.
   * Основные риски: утечка финансовых данных, несанкционированный доступ к бухгалтерским системам.
4. **Группа сервисов для клиентов**:
   * Монолитное приложение для подбора и бронирования недвижимости.
   * Основные риски: утечка данных клиентов, несанкционированный доступ к данным о бронированиях, уязвимости в интеграции с госорганами.
5. **Инфраструктура**:
   * Приватное облако, ЦОД, гибридное развертывание.
   * Основные риски: недостаточная защита данных в гибридной среде, уязвимости в межсетевом экране, недостаточное резервное копирование.
6. **API партнёров**:
   * Интеграция с системами управляющих компаний.
   * Основные риски: утечка персональных данных через API, несанкционированный доступ к данным через API, отсутствие единых политик безопасности.

### Выбор разделов для проверочного листа безопасности

Основные проблемы компании PropDevelopment:

1. **Нарушен контроль данных**:
   * Несколько точек регистрации клиентов без координации.
   * Отсутствие системного контроля за передачей данных между IT-продуктами.
   * Нет ограничений на доступ к данным со стороны систем обработки.
2. **Проблемы с API партнёров**:
   * Отсутствие единых политик безопасности при интеграции с API управляющих компаний.
   * Уязвимости в контрактах API, позволяющие доступ к персональным данным и несанкционированным действиям.

Исходя из этих проблем, приоритеты компании должны быть сосредоточены на:

* Усилении контроля за данными.
* Обеспечении безопасности API.
* Улучшении управления доступом.
* Защите данных и предотвращении утечек.

#### Выбранные разделы для проверочного листа и их обоснование:

1. **Управление доступом**:
   * **Почему важно**: Нарушен контроль данных и доступ к ним. Необходимо убедиться, что доступ к данным и системам предоставляется только авторизованным пользователям и системам.
   * **Что проверить**: Права доступа к данным, контроль за доступом к API партнёров, ролевая модель доступа.
2. **Защита данных**:
   * **Почему важно**: Утечка данных может привести к потере доверия клиентов и собственников, а также к юридическим последствиям.
   * **Что проверить**: Шифрование данных в хранилищах и при передаче, наличие механизмов предотвращения утечек.
3. **Безопасность API**:
   * **Почему важно**: Проблемы с API партнёров являются критическими, так как они могут привести к утечке персональных данных и несанкционированному доступу.
   * **Что проверить**: Контракты API на наличие уязвимостей, контроль за передаваемыми данными, политики безопасности при интеграции.
4. **Резервное копирование и восстановление**:
   * **Почему важно**: Для обеспечения непрерывности бизнеса и защиты данных от потерь.
   * **Что проверить**: Глубина и частота резервного копирования, тестирование процедур восстановления.
5. **Сетевая безопасность**:
   * **Почему важно**: Для защиты внутренних систем от внешних угроз.
   * **Что проверить**: Конфигурация межсетевого экрана, контроль доступа к внутренним сетям.
6. **Интеграция с партнёрами**:
   * **Почему важно**: Проблемы с API партнёров требуют особого внимания для предотвращения утечек данных и несанкционированного доступа.
   * **Что проверить**: Политики безопасности при интеграции с API партнёров, контроль за передаваемыми данными.
7. **Мониторинг и аудит**:
   * **Почему важно**: Для оперативного выявления и реагирования на инциденты безопасности.
   * **Что проверить**: Наличие систем мониторинга и аудита, контроль за логами и событиями безопасности.