DOI: 10.25728/avtprom.2020.04.11

Мобильные решения для диспетчеризации и управления работами ТОиР

А.Ю. Кузнецов (ООО "Газпром центрремонт"), И.С. Решетников (ИПУ РАН), А.А. Чиглинцев (ООО "Газпром центрремонт)

Рассматривается подход к созданию мобильного приложения для диспетчеризации и управления работами по ТОиР на объектах разветвленной инфраструктуры. Обсуждаются вопросы, связанные с обеспечением доступа к данным, персонализацией информации и интерфейсов, информационной безопасностью. Достоинством предложенного подхода является возможность реализовать динамическую генерацию персональных версий приложения, структуры и состава данных на уровне настроек. На примере опыта эксплуатации комплекса в ООО «Газпром центрремонт» показана эффективность предлагаемого решения для автоматизации работ ТОиР в ситуации быстро меняющихся бизнес-процессов с сохранением минимальной общей стоимости владения программным комплексом.

Ключевые слова: мобильное приложение, ТОиР, информационная безопасность, персонализация, интерфейс, наборы данных, диспетчеризация, трафик данных.

Введение

При организации и выполнении работ по техническому обслуживанию и ремонту (ТОиР) на объектах сетевой инфраструктуры (таких как объекты газоснабжения, транспорта, коммунальных сетей) координация действий между всеми участниками процесса ТОиР и производственными службами имеет первостепенное значение. Даже самое незначительное отклонение может привести к снижению пропускной способности системы в целом и срыву контрактных обязательств. Ключевым фактором эффективности координации и диспетчеризации работ ТОиР является наличие единого информационного блока для всех лиц, принимающих решения. При этом только постоянный доступ ко всему массиву информации о ходе подготовки и выполнения работ, рисках отклонения от плана-графика, «узких местах», влиянии ремонтов на подготовку к зимнему периоду и т.д. обеспечивает возможность принятия правильных и своевременных решений.

При организации обслуживания сложных технологических систем, например, Единой системы газоснабжения (ЕСГ) РФ, системы нефтепроводов, железных дорог и т.д., объем информации огромен. В этом случае работа службы организации ТОиР становится практически невозможной без использования информационно-управляющей системы (ИУС), где накапливается и агрегируется весь массив информации, касающейся проведения ТОиР как от эксплуатирующих служб, так и от непосредственных исполнителей работ [1].

Такими ИУС могут быть модули корпоративной информационной системы (КИС), специализированные информационные системы производственно-хозяйственной деятельности (ИУС ПХД) предприятия, специализированные ИУС ТОиР. Важно то, что в данных системах обрабатывается "чувствительная" для предприятия информация об эксплуатируемом оборудовании, плане поставок и «узких» местах основной деятельности, поэтому, как правило, непосредственный доступ к такой системе ограничен рамками локальной сети (ЛВС) предприятия.

Но в то же время системы уровня ИУС ТОиР относятся к классу систем операционного менеджмента и оперативного управления и должны быть не просто доступными, но стать повседневным рабочим инструментом. Поэтому важно, чтобы доступ к ИУС или, как минимум, к информации из такой ИУС для ряда сотрудников был возможен из любого места и в любое время, а не только с рабочих мест с доступом к ЛВС.

Например, руководству организации требуется доступ к операционной отчетности, сводным данным или паспортам критически важных объектов во время совещания. Диспетчеру, куратору работ, мастеру или региональному представителю может понадобиться информация о свободных резервах на соседних объектах, о корректировке комплексного плана-графика работ или об изменении режима работы на участке прямо в «поле», то есть непосредственно во время выполнения работ.

Востребована и обратная функциональность по сбору данных "извне": исполнитель на объекте либо руководитель на совещании может внести оперативные корректировки, комментарии, которые должны быть сразу доступны для всех сотрудников в привязке к конкретной работе. Это позволяет не только повысить оперативность, но и минимизировать ошибки в информационном взаимодействии между участниками процесса организации ТОиР.

Одним из решений проблемы является публикация в сети Internet отдельных интерфейсов ИУС, но этот подход не всегда применим по нескольким причинам:

- публикация ресурсов в сети Internet ограничена корпоративной политикой по информационной безопасности;
- взаимодействие между блоками с публичным доступом и в корпоративной ЛВС ограничено корпоративной политикой по информационной безопасности;
- отсутствие постоянного доступа в Internet на удаленных объектах.

Для решения поставленной задачи предлагается использовать полноценное мобильное приложение, отвечающее требованиям к информационной безопасности, обеспечивающее гибкий доступа к данным и персонализацию пользовательских интерфейсов.

Поставленную задачу не следует путать с задачами, называемыми "мобильный ТОиР", где функциональность сводится, например, к ведению паспортов ремонтных работ в мобильных устройствах [2]. В данной статье рассматривается другой класс задач и систем. Поставленная в данной работе задача направлена на управление процессами ТОиР в целом, в том числе в многоуровневых интегрированных структурах.

Архитектурные требования к мобильной системе управления ТОиР

Рассмотрим основные требования к мобильной системе управления ТОиР.

Автономность приложения. В связи с обычными для крупных структур ограничениями информационной безопасности, когда доступ к информации запрещен извне ЛВС, и тем, что работа с мобильным приложением должна быть возможна и в труднодоступных местах, где отсутствуют какие-либо каналы связи (в том числе Internet), мобильное приложение должно функционировать и в полностью автономном режиме.

Иными словами, оно должно быть реализовано не в качестве клиента, работающего с центральным сервером в клиент-серверной модели, а как самостоятельное приложение на мобильном устройстве с отдельной СУБД, периодически синхронизирующейся с центральным сервером при наличии подключения.

Гибкость настроек. Поскольку приложение предназначено для сотрудников разного уровня от рядового специалиста до высшего руководства компании, всем необходим разный набор информации из КИС с разной степенью абстракции и моделью представления информации. Иными словами, для каждого сотрудника необходим свой набор данных и свой внешний вид приложения.

Кроме того, задачи сотрудников периодически меняются. Критичным требованием является обеспечение возможности быстрой настройки подключения новых срезов данных и настройки новых форм отображения данных в соответствии с новыми требованиями без переделок программного кода и привлечения разработчиков.

Сложность состоит еще и в том, что функциональность и информативность интерфейсов в мобильном приложении заведомо ограничены в силу фиксированных объема памяти, размера экрана и функциональности по вводу данных на мобильном устройстве.

Ограничение трафика данных. В классической клиент-серверной архитектуре весь массив данных хранится в центральной СУБД, а пользователь через клиентское приложение получает доступ к нужной ему информации в рамках предоставленных ему полномочий. Для автономно функционирующего мобильного приложения такой подход невозможен. Например, в ИУС ПХД содержатся десятки миллионов записей и ежедневно выполняются миллионы транзакций, выгружать такой объем данных на мобильное устройство нереально.

Важным требованием к мобильному решению является персонализация не только интерфейсов пользователя, но и трафика для конкретного устройства. При этом персонализация версии приложения должна не программироваться, а настраиваться.

Схема информационного взаимодействия

С точки зрения конечного пользователя мобильное ПО для управления ТОиР выглядит как обычное приложение, устанавливаемое на устройство. Но на практике архитектура данной системы должна быть более сложной и включать следующие элементы:

- серверная часть, в которой администратор регистрирует устройства, настраивает версии приложения, функционирующие на устройствах, управляет метаданными, генерирует версии приложения и защищенные сессии обмена данными с приложениями, установленными на мобильных устройствах;
- клиент — мобильное приложение, которое обеспечивает синхронизацию данных с центральным сервером, хранит данные, позволяет пользователю просматривать и редактировать данные в рамках предоставленных полномочий.

Для обеспечения информационной безопасности взаимодействие между центральным хранилищем данных и мобильными устройствами должно проводиться через промежуточный сервер, желательно находящийся в зоне DMZ[1]. Протоколы обмена данными должны иметь шифрование или кодирование в зависимости от требований.

Рассмотрим пример информационных потоков в схеме взаимодействия с транспортным протоколом электронной почты (рис. 1). При выполнении синхронизации на серверной части выполняются следующие операции:

- в соответствии с правилами синхронизации данные извлекаются из основной ИУС ТОиР;
- данные подготавливаются и сохраняются в обменном формате в xml;
- файлы шифруются и отправляются на обменный сервер;
- на обменном сервере зашифрованные файлы синхронизации публикуются и становятся доступны для соответствующих устройств.

В приложении, установленном на мобильном устройстве:

- файлы синхронизации забираются с обменного сервера;
- данные расшифровываются и сохраняются в локальной базе данных для дальнейшего использования в приложении.

[4] DMZ (*Demilitarized Zone* — демилитаризованная зона) — сегмент сети, содержащий общедоступные сервисы и отделяющий их от локальных ресурсов. Цель зоны DMZ — добавить дополнительный уровень безопасности локальной сети.

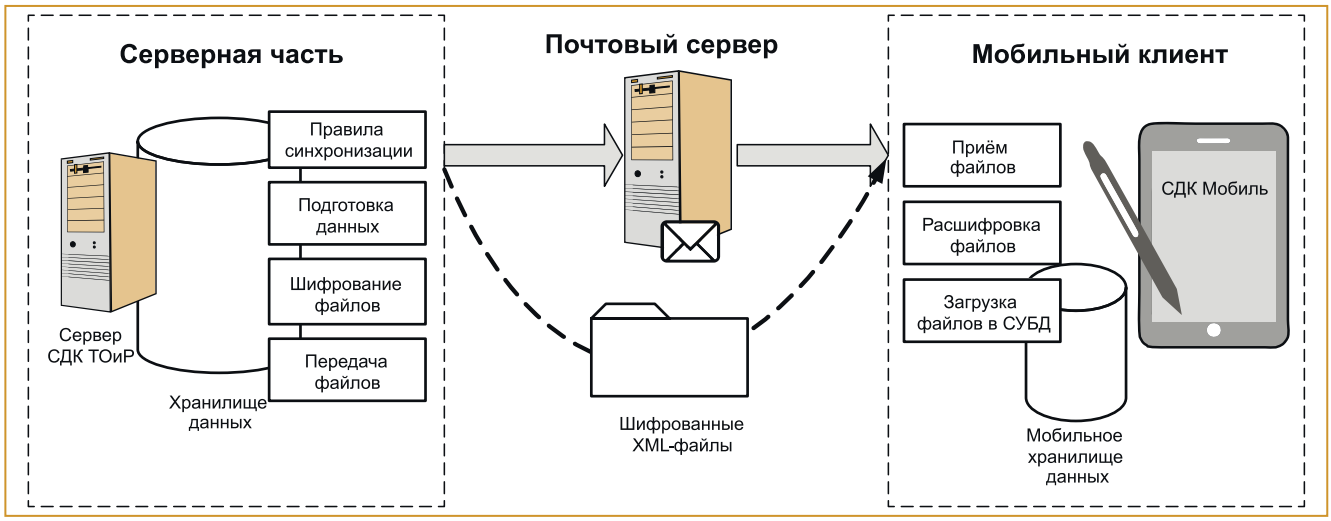

Рис. 1. Схема организации информационных потоков в примере передачи по электронной почте

Управление метаданными

В отличие от стандартного приложения, интерфейсы предлагаемого мобильного решения для планшета должны быть компактными и функционально-ориентированными на решение конкретных задач. Универсальные формы в условиях ограниченности размера экрана работают крайне неэффективно. Кроме того, в мобильном приложении объем и глубина ретроспективы данных ограничены, и их нужно очень тщательно планировать.

Для реализации данных требований предлагается поэтапная структура управления метаданными объектов.

На первом этапе регистрируются наборы данных, соответствующие экранным формам основной корпоративной системы ТОиР. Наборы данных делятся по классам, например, на сводные и на объектные. На этом этапе определяются связи между этими наборами, то есть, по каким полям и каким образом они могут быть связаны.

На следующем этапе создаются прототипы приложений для различных групп пользователей. Через конфигуратор задается, какие наборы данных доступны для каждого из типа приложений и перечень реплицируемых параметров, взаимосвязь и порядок следования различных наборов данных. На основании такой настройки генерируется версия приложения, ориентированная на конкретную группу пользователей.

Практика реальной эксплуатации показала, что оптимальным подходом к персонализации данных является настройка системы, когда пользователь ставит на контроль отдельный объект или группу объектов и получает по ним расширенный набор данных.

Аналогичным образом решается задача сбора данных: для набора редактируемых данных определяется первичный ключ и фиксируется, какие поля будут редактируемыми. Мобильное приложение отправляет тип поля, первичный ключ набора и его значение. Привязанные к набору процедуры редактирования автоматически выполняют обработку входящего пакета после прохождения соответствующих верификаций.

Данный подход позволяет решить одну из самых сложных организационных задач с точки зрения постоянного сопровождения и адаптации подобных персонализированных приложений: для разработки новой формы разреза данных или формы сбора привлечение специалиста по разработке мобильных приложений не требуется. Эти действия могут быть полностью перенесены на сторону пользователя. Таким образом, для адаптации системы к требованиям пользователей в 90% случаях достаточно локального администратора системы.

Практическая реализация

Совместно с ООО "Компания "ТЕРСИС" было разработано решение СДК Мобиль, состоящее из серверной и мобильной частей. Данное решение было успешно апробировано в режиме опытной эксплуатации в холдинге ООО «Газпром центрремонт», выполняющей организацию ремонтных работ на всех объектах ЕСГ РФ (около 40 тыс. работ в год) [3]. Среди объектов проведения работ ООО «Газпром центрремонт»: магистральные газопроводы, компрессорные станции, подземные хранилища газа и газораспределительные станции. Система СДК Мобиль была интегрирована с программным комплексом диспетчерского контроля работ ТОиР СДК ТОиР (разработчик — ООО "Компания "ТЕРСИС"), которая является центральной корпоративной ИУС ТОиР холдинга. Важным аспектом эксплуатации оказалось удобство интерфейсов, что существенно повышало эффективность владения комплексом.

Серверное приложение

Основной проблемой стала генерация соответствующих процедур обмена данными между центральной СУБД и базой данных конкретных устройств. Для реализации этого механизма было разработано специализированное приложение-генератор на языке Java, которое позволяет генерировать xml описание форм и процедуры настройки обмена данными для синхронизации с центральным сервером. В такой модели

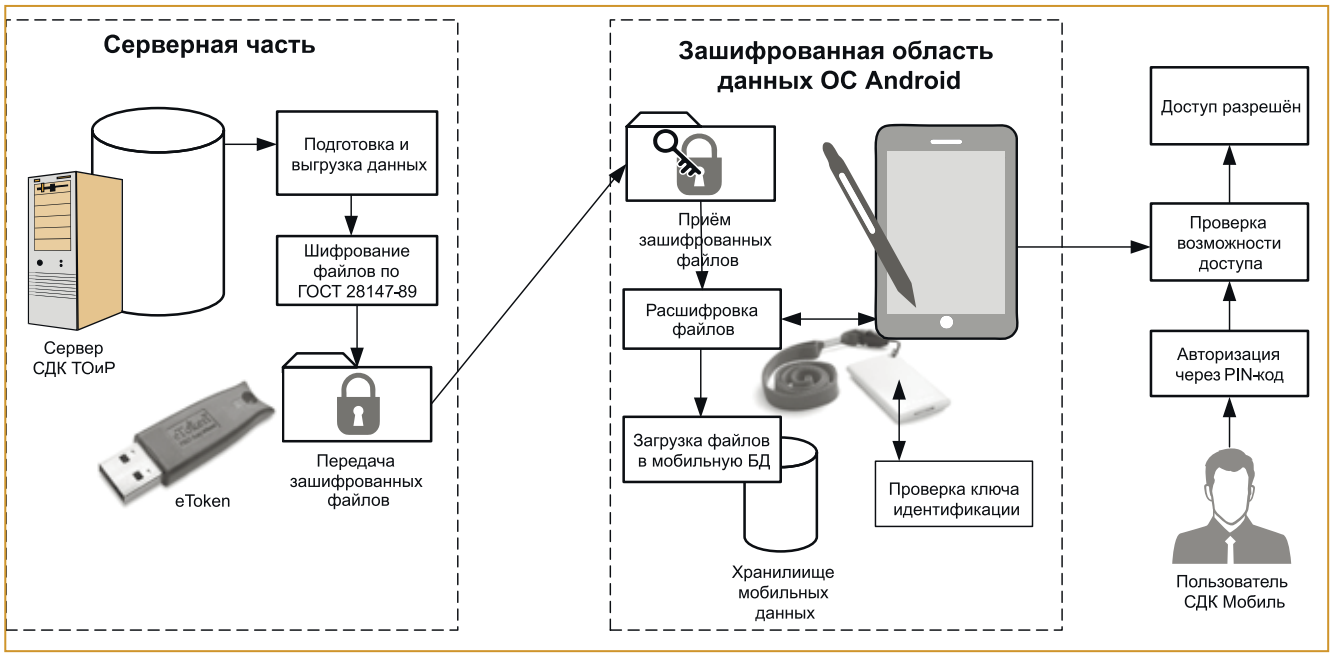

Рис. 2. Схема обеспечения информационной безопасности

отображение и редактирование данных на мобильном устройстве не программируется, а настраивается на уровне метаданных. На уровень настроек вынесена генерация интерфейсных элементов: фильтров, подсчета итогов, сортировки, формата полей и т. п.

Администратор выполняет регистрацию устройств, настройку наборов данных и другие операции по управлению мобильным приложением через специализированное Web-приложение. Это приложение может быть интегрировано в любую КИС. Для этого достаточно однократно настроить слои с наборами данных, которые должны передаваться на мобильное устройство и поддерживать их в актуальном состоянии.

Обеспечение защиты информации

Основными пользователями мобильных устройств стало руководство, что предполагало работу с критичными для организации данными категории коммерческая тайна. Перехват таких данных при доставке либо их утеря вместе с устройством недопустимы. При создании приложения первоочередное внимание было уделено обеспечению информационной безопасности и минимизации рисков перехвата данных. Поскольку информация в системе касается инфраструктурных объектов, то в соответствии с рекомендациями Министерства экономического развития для вспомогательных операций использовалось исключительно российское ПО.

Угрозы информационной безопасности возникают на следующих шагах:

- публикация данных на сервере в DMZ;
- передача данных между сервером и мобильным устройством;
- использование приложения;
- потеря данных при физической утере устройства.

Для минимизации рисков утери данных был использован комплекс технических решений (рис. 2).

1. Защита мобильного устройства. В качестве клиента может быть использовано только устройство, специально подготовленное и проверенное службой защиты: устанавливается антивирусная защита, блокировка по пин-коду, выпускается персональный ключ криптозащиты, который необходим для шифрования данных мобильного приложения.

2. Защита каналов передачи. Все данные шифруются средствами пакета КриптоПро, при этом каждый пакет данных может быть расшифрован только на определенном устройстве персональным ключом. Доступ к данным на сервер ограничен по imei и mac-адресу устройства, то есть для получения доступа к данным необходимо сочетание корректного imei, mac-адреса и персонального ключа сотрудника.

3. Защита хранения данных на устройстве. Все данные хранятся в зашифрованном виде, доступ к ним возможен только при наличии ключа шифрования и после корректного ввода пин-кода для ключа шифрования.

4. Защита при утере устройства. При утере устройства без ключа все данные на нем будут зашифрованы и недоступны злоумышленнику. Пин-код обеспечивает дополнительный уровень защиты. После регистрации устройства как утерянного, на него высылается команда на уничтожение данных и блокировку устройства, которая будет выполнена при первом подключении устройства к Internet.

5. Надежность защиты. Для шифрования используются сертифицированные ФСТЭК алгоритмы шифрования и носители.

Такие меры обеспечения защиты данных могут показаться излишними. Но холдинг ООО «Газпром центрремонт» — это десятки тысяч заявок на ремонт с общей стоимостью более 100 млрд. руб. ежегодно, а также жесткие требования к соблюдению сроков ремонта и их качеству: сбой в программе ТОиР

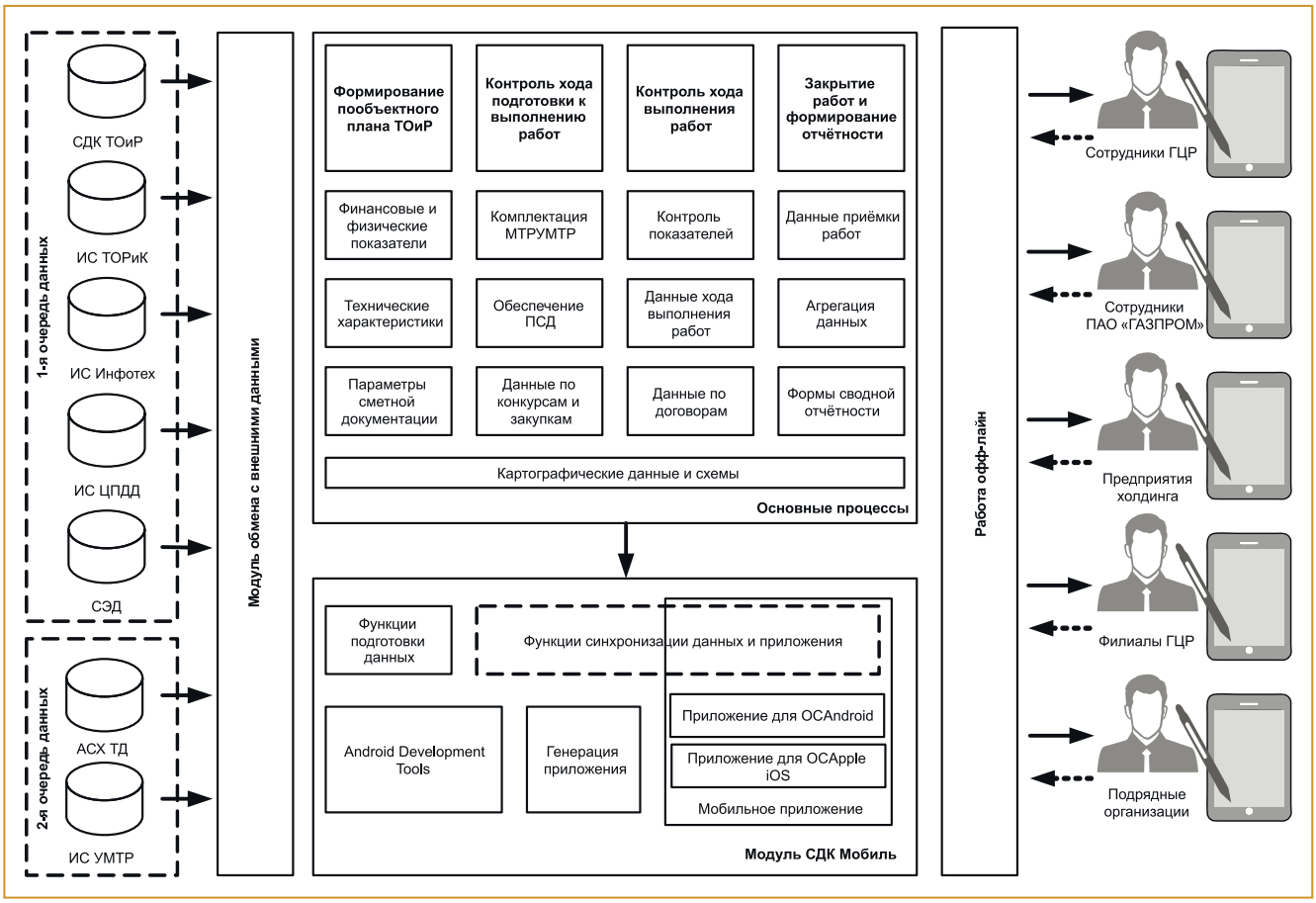

Рис. 3. Схема информационных источников и потоков данных

на критичном объекте может привести к убыткам на миллиарды рублей и необратимым социальным и экономическим последствиям.

Сложность структуры информационных источников и решаемых задач чрезвычайно высока и охватывает не только центральную КИС СДК ТОиР, но и множество других ИУС головной компании холдинга, головной структуры ПАО "ГАЗПРОМ" и предприятий холдинга (рис. 3).

Интерфейс мобильного приложения

Первоочередное внимание при проектировании и разработке уделялось тому, как разместить на ограниченном экране мобильного устройства весь необходимый массив данных в максимально сжатом и эргономичном виде. При этом в ходе внедрения все интерфейсы мобильного приложения настраивались штатными средствами администраторского приложения без привлечения специалистов по разработке мобильных приложений.

Основные блоки данных, с которым работает диспетчер ТОиР и которые определили набор основных функциональных блоков СДК Мобиль, следующие (рис. 4):

- пообъектный план работ и ход его выполнения;
- договорная кампания;
- ход работ на отдельных критических либо влияющих на пропускную способность объектах ремонта;
- согласованные изменения режима транспорта газа;
- сводные и статистические данные о ходе выполнения программы ремонта.

Рассмотрим для примера справочную форму «Ход организации ТОиР», с которой работает диспетчер.

Рис. 4. Функциональные блоки СДК Мобиль

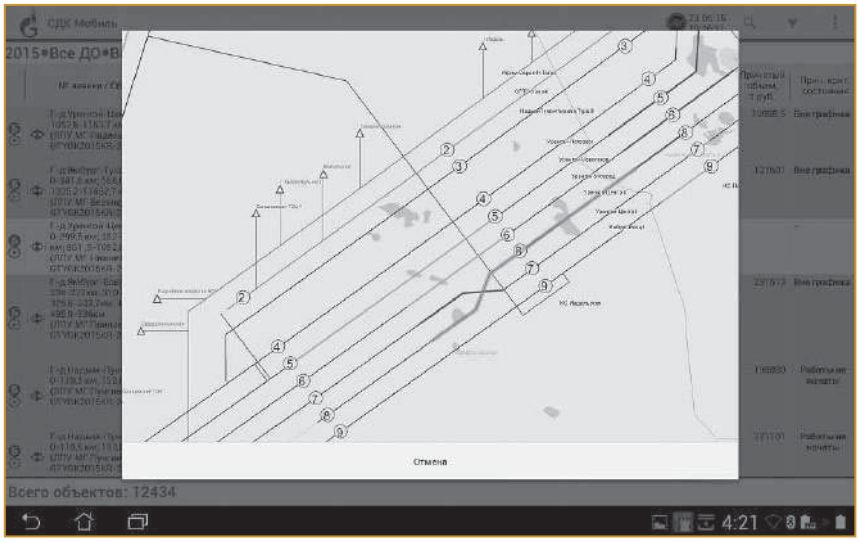

Рис. 5. Модель изменения режима транспорта газа на технологической схеме

Форма организована так, что позволяет быстро сфокусироваться на той информации, которая нужна диспетчеру ТОиР: за счет фильтров, цветовой маркировки, пиктограмм достигается максимальная наглядность. Большинство данных имеют детализацию как в табличной форме, так и в виде специальных представлений, например, технологических схем или иллюстраций (рис. 5). Все информационные блоки являются частью приложения СДК ТОиР, что обеспечивает унификацию представлений.

Аналогичным образом в других формах куратор работ ТОиР может быстро (в один-два перехода) найти информацию о проблемных объектах, отставании от графика и даже получить доступ к сопроводительной документации по ремонту: к дефектной ведомости, плану-графику работ или ремонтному формуляру. Аналогично куратор работ получает доступ к сводкам по ходу выполнения работ в разрезе исполнителей, направлений деятельности и других параметров с возможностью перехода к паспортам отдельных ремонтов для выявления отклонений от выполнения программы ремонта в целом и принятия соответствующих управленческих решений.

Результаты апробации

В ходе выполнения проекта было настроено 12 основных ролевых моделей (наборов данных и интерфейсов), адаптированных под функциональные обязанности специалистов, что оказалось вполне достаточным даже для такого большого объема данных.

В ходе эксплуатации силами ИТ-службы заказчика ежемесячно вносились незначительные изменения в интерфейсы пользователя для отдельных версий, при изменении внешних требований ПАО «Газпром» расширялись базовые наборы данных.

Таким образом, в ходе эксплуатации даже с учетом постоянно меняющихся требований функциональных заказчиков не потребовалось привлечение разработчиков, большая часть доработок выполнялась локально администраторами в штатном режиме, и только в исключительных случаях приходилось подключать специалистов по данным, но также из числа специалистов пользователя.

Выводы

В статье рассмотрены основные проблемы и задачи, возникающие при разработке мобильных приложений для службы ТОиР, обеспечивающей выполнение работ на сложных объектах инфраструктуры. Предложены подходы к решению данной задачи, позволяющие обеспечить диспетчеров и кураторов работ необходимой информацией и автоматизировать процессы обмена информацией между участниками процесса ТОиР даже при динамично меняющихся требованиях с минимальным привлечением программистов. Продемонстрировано практическое решение, созданное на базе данных подходов, и приведены результаты его апробации при организации ТОиР на максимально сложной инфраструктуре ЕСГ ПАО "ГАЗПРОМ".

Апробация показала, что предложенное решение позволяют создать удобное и функциональное мобильное приложение для службы ТОиР с минимальной общей стоимостью владения и могут быть широко использованы при разработке мобильных приложений для служб ТОиР, как организовывающих работы на объектах газоснабжения, так и на других инфраструктурных объектах.

Список литературы

1. *Решетников И.С.* Автоматизация производственной деятельности газотранспортной компании. М.: НГСС. 2011.
2. *Коробань Е.И.* Мобильное ТОРО и стратегия ТОРО по надежности: опыт внедрения // Автоматизация в промышленности. 2019. №8.
3. *Решетников И.С.* Автоматизация управления ремонтами: от телеграфа до полной визуализации // Газовая промышленность. 2012. №10. с. 70-71.

Кузнецов Андрей Юрьевич *– начальник отдела,*
Чиглинцев Алексей Антонович *– начальник отдела ООО "Газпром центрремонт",*
Решетников Игорь Станиславович *– канд. техн. наук, старший научный сотрудник ИПУ РАН.*
Контактный телефон (495) 334-87-59.