

УТВЕРЖДЕНО

Директор УРАИТ

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **<ФИО>**

« » \_\_\_\_\_\_\_\_\_\_\_\_\_ 2014г.

<Наименование подразделения-разработчика>

Детальная архитектура автоматизированной системы «iNavigator»

Москва 2014г.

Лист согласования

к документу Детальная архитектура автоматизированной системы «iNavigator»

Документ разработан:

Аналитик Управления развития ЦХД (MIS)

**Григорьев И.Л.**

**Гордиенко М.В.**

Документ согласован:

Руководитель проектов УРАИТ

**<ФИО>**

Центр сопровождения ИТ

**<ФИО>**

Руководитель проекта ДФ

**Рождественский А. В.**

Начальник отдела Управления развития ЦХД (MIS)

**Порфирьев С. И.**

Руководитель проекта

**Фролов М.В.**

Детальная архитектура автоматизированной системы «iNavigator»

**Содержание**

[1 Общие сведения 4](#_Toc399841695)

[1.1 Назначение документа 4](#_Toc399841696)

[1.2 История изменений 4](#_Toc399841697)

[1.3 Изменения по сравнению с прошлой редакцией 4](#_Toc399841698)

[1.4 Идентификация системы 5](#_Toc399841699)

[1.5 Основания для создания и история системы 5](#_Toc399841700)

[1.5.1 Основания для создания системы 6](#_Toc399841701)

[1.5.2 Проекты, оказывающие влияние на АС 6](#_Toc399841702)

[1.5.3 Документы, регламентирующие создание и разработку АС 6](#_Toc399841703)

[1.5.4 Релизы АС 7](#_Toc399841704)

[1.5.5 Глоссарий 7](#_Toc399841705)

[2 Функциональная архитектура 8](#_Toc399841706)

[2.1 Визуализация данных 9](#_Toc399841707)

[2.1.1 iNavigator 9](#_Toc399841708)

[2.1.2 iRubricator 9](#_Toc399841709)

[2.1.3 MISMobile 10](#_Toc399841710)

[2.1.4 Инструмент управления продажами 10](#_Toc399841711)

[2.1.5 Динамическая модель CIB 11](#_Toc399841712)

[2.1.6 Выполнение ППР/КПЭ руководителей 11](#_Toc399841713)

[2.1.7 Отчёт по балансу Сбербанка 11](#_Toc399841714)

[2.1.8 Сравнение с конкурентами 11](#_Toc399841715)

[2.2 Управление жизненным циклом мобильных приложений 11](#_Toc399841716)

[2.2.1 Сервер конфигураций (Configuration Server) 11](#_Toc399841717)

[2.2.2 Каталог приложений 12](#_Toc399841718)

[2.3 Модуль управления доступом и синхронизацией (Sync Cache Server) 12](#_Toc399841719)

[2.3.1 Сервисы кэширования. 12](#_Toc399841720)

[2.3.2 Сервисы транспортировки данных. 12](#_Toc399841721)

[2.3.3 Сервис SQL-запросов 12](#_Toc399841722)

[2.3.4 Управляющая консоль 12](#_Toc399841723)

[2.3.5 Функции безопасности 13](#_Toc399841724)

[2.3.6 Функции журналирования событий 13](#_Toc399841725)

[2.3.7 Перечень используемых сервисов 13](#_Toc399841726)

[2.4 Модуль отслеживания и отправки актуальных данных с MIS Портала (Sync Generator) 15](#_Toc399841727)

[2.4.1 SQLite Generator 15](#_Toc399841728)

[2.4.2 ChangeSet Generator 15](#_Toc399841729)

[2.4.3 Управляющая консоль 15](#_Toc399841730)

[2.4.4 Функции журналирования событий 15](#_Toc399841731)

[2.4.5 Перечень используемых сервисов 15](#_Toc399841732)

[2.5 Модуль выполнения онлайн запросов (SQL Proxy Server) 16](#_Toc399841733)

[2.6 Модуль мониторинга (Alpha Monitor, Sigma Monitor) 16](#_Toc399841734)

[2.6.1 Alpha Monitor 16](#_Toc399841735)

[2.6.2 Sigma Monitor 17](#_Toc399841736)

[3 Архитектура данных 18](#_Toc399841737)

[3.1 Источники данных 18](#_Toc399841738)

[3.2 Потоки данных 18](#_Toc399841739)

[3.2.0 Консолидация данных 21](#_Toc399841740)

[3.2.1 Потоки передачи данных в кэш мобильного устройства (МУ) – офлайн визуализация 21](#_Toc399841741)

[3.2.2 Потоки передачи данных при онлайн визуализации 24](#_Toc399841742)

[3.2.3 Потоки модификации отчётов 29](#_Toc399841743)

[4 Архитектура приложений 30](#_Toc399841744)

[4.1 Приложения на мобильном устройстве 30](#_Toc399841745)

[4.2 Приложения Java EE 31](#_Toc399841746)

[4.3 Сервер приложений 31](#_Toc399841747)

[4.4 СУБД MS SQL 32](#_Toc399841748)

[4.5 Шина DataPower & IBM MQ 32](#_Toc399841749)

[4.6 SAP Afaria 32](#_Toc399841750)

[5 Техническая архитектура 33](#_Toc399841751)

[5.1 Распределение нагрузки и обеспечение бесперебойности при синхронизации МУ 33](#_Toc399841752)

[6 Взаимодействие с окружением 36](#_Toc399841753)

[7 Информационная безопасность 37](#_Toc399841754)

[7.1 Ролевая модель 37](#_Toc399841755)

[7.2 Защита информации 38](#_Toc399841756)

[7.2.1 Аутентификация клиента и обмен данными 38](#_Toc399841757)

[7.2.2 Сертификаты, используемые при обмене данными 39](#_Toc399841758)

[7.2.3 Авторизация пользователя 39](#_Toc399841759)

[7.2.4 Безопасность данных на мобильном устройстве 39](#_Toc399841760)

[7.2.5 Политики безопасности на мобильном устройстве 39](#_Toc399841761)

[7.2.6 Категории информационной безопасности 41](#_Toc399841762)

[Приложение 1. Модель работы с данными в мобильных приложениях 42](#_Toc399841763)

[Приложение 2. Процедуры подготовки данных для выгрузки в БД SQLite 43](#_Toc399841764)

[Приложение 3. Источники сведений о времени последней модификации данных в БД MIS Портала 47](#_Toc399841765)

[Приложение 4. Способ формирования файлов на Sync Generator 48](#_Toc399841766)

[Приложение 5. Перечень файлов, используемых в мобильных отчётах 49](#_Toc399841767)

# Общие сведения

Номер документа по реестру УРАИТ: 179309

## Назначение документа

Данный документ содержит описание архитектуры автоматизированной системы «Мобильная версия стандартных форм управленческих отчетов, отражающих ключевые показатели деятельности (iNavigator) – Фаза 2».

Основанием для разработки архитектуры проекта являются бизнес-требования заказчика и концептуальная архитектура проекта.

Документ состоит из следующих разделов:

* Функциональная архитектура;
* Архитектура данных;
* Архитектура приложений;
* Техническая архитектура;
* Взаимодействие с окружением;
* Информационная безопасность.

## История изменений

|  |  |  |  |
| --- | --- | --- | --- |
| **№ ред.** | **Дата** | **Автор** | **Изменения** |
| 0.1 | 14.04.2014 | Григорьев Илья Леонидович | Документ разработан |
| 0.2 | 22.04.2014 | Григорьев Илья Леонидович | Доработан раздел «Техническая архитектура» |
| 0.3 | 06.05.2014 | Григорьев Илья Леонидович | Изменения по замечаниям разработчиков СБТ и Прогноза |
| 0.4 | 14.05.2014 | Григорьев Илья Леонидович | Правки по замечаниям разработчиков: доработаны диаграммы архитектуры приложений, потоков данных, скорректирована ролевая модель, прочее. |
| 0.5 | 18.06.2014 | Григорьев Илья Леонидович |  |
| 7 | 29.09.2014 | Гордиенко Максим Вячеславович | Актуализирован документ, добавлены разделы с описанием используемых сервисов и более подробно описан механизм онлайн запросов |

## Изменения по сравнению с прошлой редакцией

| **Раздел** | **Изменения** |
| --- | --- |
|  |  |

## Идентификация системы

|  |  |
| --- | --- |
|  | **Информация из АС ЦУП** |
| ID КЭ в Service Manager | 179309 |
| Наименование АС в архитектурном репозитории | iNavigator |
| Другие наименования АС | Мобильная версия стандартных форм управленческих отчетов, отражающих ключевые показатели деятельности – Фаза 2 |
| Подразделение-владелец АС | Департамент финансов |
| Подразделения-заказчики проекта | Департамент финансов |
| Класс критичности АС | Оперативная работа (Business Operational) |

## Основания для создания и история системы

Задача проекта – развитие системы мобильной управленческой отчетности. Предоставление руководству Банка доступа к управленческим отчетам MIS в режиме on-line с персональных мобильных устройств.

Проект выполняется в продолжение проекта «Реализация мобильной версии стандартных форм управленческих отчетов, отражающих ключевые показатели деятельности (iNavigator) – Фаза 1» ID 156637.

Задачами проекта являются:

* Создание инфраструктуры передачи данных MIS во внешнюю сеть для on-line доступа с мобильных устройств;
* Разработка мобильных компонент и шаблонов быстрой разработки типовых форм управленческих отчетов;
* Создание нетиповых форм отчетов в соответствии с текущими потребностями бизнес-подразделений в использовании управленческой информации на мобильных устройствах.

В результате внедрения АС, пользователям становятся доступны следующие типы управленческих отчётов.

* Доходность крупнейших клиентов
* Отчет на КПКИ CIB
* Выполнение бизнес-плана
* KPI CIB
* Прибыль CIB
* Отчеты PL Розничного блока (PL кредитных продуктов, PL ВСП и PL АТМ)
* Инструмент управления продажами
* Динамическая модель CIB
* Выполнение ППР/КПЭ руководителей
* Отчет по балансу Сбербанка
* Сравнение с конкурентами
* Специально публикуемые на MIS Портале отчёты в виде документов PDF, Word, Excel, PowerPoint

В системе не заложено создание не предопределённых (пользовательских) форм отчётов.

### Основания для создания системы

### Проекты, оказывающие влияние на АС

|  |  |  |  |
| --- | --- | --- | --- |
| **ID проекта** | **Название проекта** | **Влияние** | **Комментарий** |
| 156637 | Реализация мобильной версии стандартных форм управленческих отчетов, отражающих ключевые показатели деятельности (iNavigator) – Фаза 1 | Использована | Используются результаты проекта. Дорабатывается ПО, разработанное в рамках проекта. |
| 137596 | Создание стандартных форм управленческих отчетов для всех функциональных блоков и уровней управления - «Навигатор» | Использована | Источник данных |
| 147134 | Расчетный модуль MIS CIB | Использована | Источник данных для мобильных отчетов CIB |
| 99865 | СКАД | Использована | Управление жизненным циклом мобильных приложений |
| 111145, 163785 | АС «ЕРИБ» | Использована | SMS-сервис |

### Документы, регламентирующие создание и разработку АС

1. Функциональные бизнес требования
2. Решение Управляющего Комитета по реализации проекта iNavigator от 18.09.2014
3. Паспорт проекта
4. Концептуальная архитектура проекта

### Релизы АС

|  |  |  |  |
| --- | --- | --- | --- |
| **ID релиза** | **Дата внедрения** | **Влияние** | **Комментарий** |
| 1.0 | Июль 2014 | Создана | Пользователям доступны отчеты MIS Портала с мобильных устройств |

### Глоссарий

Таблица 1 - Перечень терминов и сокращений

| **Сокращение** | **Расшифровка сокращения** |
| --- | --- |
| MIS | Система управленческой отчетности (Management Information System), комплекс организационных мер и технологий, обеспечивающий менеджмент Банка (от Правления до внутренних структурных подразделений) критически важной информацией, необходимой для принятия управленческих решений |
| KPI, КПЭ | Key Performance Indicator – ключевой показатель эффективности. |
| АРМ | Автоматизированное рабочее место |
| AC | Автоматизированная система |
| Банк | Сбербанк России |
| КПЭ | Ключевой показатель эффективности, вычисленный в Системе на основе исходных данных. Сохраняется в Системе как новый KPI |
| ГОСБ | Головное отделение Сбербанка |
| Источник | Информационная система (уже существующая, либо разрабатываемая) или файл с данными – источник исходной информации |
| НСИ | Нормативно-справочная информация |
| ТБ | Территориальный банк Сбербанка России |
| ВСП | Внутреннее структурное подразделение банка |
| AD | Active Directory, централизованная база для управления политиками безопасности |
| УЦ | Удостоверяющий центр – служба, уполномоченная выпускать электронную цифровую подпись. |
| МУ | Мобильное устройство пользователя, например iPad |
| КТС | Комплекс Технических Средств |

# Функциональная архитектура



Рисунок 1. Диаграмма функциональной модели

Ключевые элементы диаграммы:

* Визуализация данных на мобильном устройстве. Обеспечивает следующий функционал:
  + Отображает полученные данные в виде интерактивных отчётов или дэшбордов
  + Производит аутентификацию пользователя по ПИН-коду
  + Формирует запросы на сервер для получения данных
  + Кэширует полученные данные для автономной (офлайн) работы с отчётами
* Модуль управления доступом и синхронизации данных (Sync Cache Server). Осуществляет основную работу по доставке данных на мобильное устройство. Выполняет следующие функции:
  + Производит аутентификацию по персональному почтовому сертификату пользователя
  + Обеспечивает проверку прав пользователя на доступа к тому или иному мобильному приложению и файлам данных, используемых мобильным приложением
  + Промежуточное хранение данных MIS Портала в собственном кэше для быстрого доступа к ним со стороны мобильных устройств (МУ)
  + Передачу файлов на мобильное устройство из кэша Sync Cache Server
  + Передачу запросов к БД MIS (через DataPower) и возврат результатов
  + Управляющие функции: изменение настроек, остановка и запуск сервисов, просмотр событий
* Модуль отслеживания и отправки актуальных данных с MIS Портала (Sync Generator). Поддерживает в актуальном состоянии кэш модуля синхронизации. Обеспечивает следующий функционал:
  + Через заданный промежуток времени производит проверку БД MIS Портала на наличие новых данных
  + Генерирует файлы формата SQLite с новыми данными и передаёт в модуль синхронизации через шлюз односторонней передачи данных (Файлоперекладчик)
  + Генерирует zip-архивы с отчетами из БД iRubricator и передаёт в Sync Cache Server через файлоперекладчик
  + Управляющие функции: принудительная (повторная) генерация файлов в файлоперекладчик, изменение настроек, остановка и запуск сервисов, просмотр событий
* Модуль выполнения онлайн запросов (SQL Proxy Server). Его основной функцией является выполнение онлайн запросов, формируемых на мобильном устройстве, и возврат результата.
* Модуль мониторинга. Отслеживает работоспособность остальных модулей, и извещает администраторов АС о нештатных ситуациях.
* Шлюз двусторонней передачи данных (DataPower). Его задачей является надёжная и безопасная передача данных между сетями Alpha и Sigma.
* Шлюз односторонней передачи данных (файловый перекладчик). Специальный сервис, который переносит данные в виде файлов из сети Alpha в сеть Sigma.
* Модуль управления жизненным циклом приложений. На него возложены функции:
  + Является первой точкой подключения мобильных устройств
  + Хранение настроек приложений для мобильных устройств
  + Хранение актуальных версий приложений для мобильных устройств
  + Установка, обновление и удаление мобильных приложений
  + Авторизация пользователя на предмет доступа к тому или иному мобильному приложению

## Визуализация данных

Модуль визуализации осуществляет функции отображения информации конечному пользователю в табличном виде, в виде графиков, дэшбордов или даёт возможность просмотра отчётов Финансового Департамента, выпускаемых в формате документов PDF, Word, Excel или PowerPoint. Источником данных для этого инструмента являются витрины MIS Портала, а методом доставки этих данных из закрытого сегмента Alpha чрез пространство Интернет до конечного мобильного устройства занимается специальная инфраструктура, обеспечивающая безопасную и оперативную доставку данных.

Пользователю не доступны инструменты для создания персонифицированного отчёта. Вместо этого ему предлагается заранее подготовленные виды отчётов с возможностью фильтрации или перехода к детальным сведениям. Ниже перечислены реализуемые компоненты модуля визуализации, каждый из которых выполнен в виде самостоятельного приложения для мобильного устройства.

### iNavigator

Предоставляет дэшборд по финансовым и нефинансовым показателям управленческой отчетности и оперативные прогнозы по показателям. В частности это такие данные как общий баланс банка, общий объём кредитного портфеля, в том числе расчёт прогнозных показателей, доходы банка в разрезе продуктов, размеры операционных расходов и т.д.

### iRubricator

Рубрикатор отчётов. Используется для просмотра стандартных отчётов, которые могут быть получены в виде документов PDF, Word, Excel или PowerPoint, подготовленных Департаментом Финансов. Примерами документов могут служить: еженедельная отчётность для Совета Директоров Сбербанка; квартальный пресс-релиз; ежемесячный мониторинг CIB и т.д.

Кроме этого здесь реализована возможность запускать любой отчёт из приложения MISMobile. Таким образом, iRubricator является единой точкой входа для разных типов отчётов.

### MISMobile

Приложение является каталогом интерактивных отчётов, и не предусматривает прямого взаимодействия с пользователем. Вместо этого доступ к отчётам производится по вызову из приложения iRubricator.

Базовым элементом здесь является MIS Mobile Engine Framework (MIS MEF) – конструктор отчётов, позволяющий разработчикам быстро настроить необходимое представление данных. Ключевой сущностью этого конструктора является конфигурационный файл для каждого отчёта, описывающий: источники, компоновку данных, элементы управления и логику взаимодействия с пользователем. В то же время, конструктор MIS MEF не предусматривает создание либо модификации отчётов непосредственно пользователем мобильного устройства.

В рамках этого приложения реализованы следующие отчёты:

* **Доходность крупнейших клиентов CIB** – предоставляет сведения о кредитах, РЕПО, облигациях, текущих счетах, счетах ЛОРО, комиссиях, продуктов IB, GM и MB в разрезе каждого клиента с детализацией до договора/счёта и с указанием остатка по счёту, суммы договора, процентной ставки. Отчёт также позволяет отобразить общую картину доходности по портфелю клиентов.
* **Отчёт на КПКИ CIB** – отображает сведения о кредитах клиентов с возможностью детализации по каждому клиенту и по каждой сделке в разрезе суммы, валюты, процентной ставки и срока кредита.
* **Выполнение бизнес-плана IBGM&MB** – отчёт содержит бизнес план по доходам подразделений GM, IBGM и MB в сравнении с фактически достигнутыми показателями доходов. Данные отображаются в разрезе продуктов банка с возможностью просмотра доходов по выбранному клиенту или территориальному подразделению.
* **Активы CIB**
* **Пассивы (Обязательства) CIB**
* **KPI CIB** – отображает ППР подразделений CIB в разрезе показателей ППР в фактических единицах и в сравнении с плановыми показателями.
* **Прибыль CIB** – отображает фактический доход подразделения CIB в сравнении с плановыми показателями в разрезе территориальных подразделений.
* **Отчёты PL Розничного блока, кредитные продукты** – отображает сводную информацию по статистке и динамике кредитных продуктов в разрезах продуктов, каналов и клиентов. Данные отображаются в количественных величинах: получено заявок, выдано кредитов, процент одобрения и т.д.
* **Отчёты PL Розничного блока, ATM** – отчёт предоставляет оценку эффективности устройств в количественных величинах: общее количество устройств в ВСП, количество неэффективных устройств, объём операций на одно устройство, количество операций на одно устройство и т.д. Данные отображаются в разрезе банка/ТБ/ОСБ /населённого пункта с разделением на банкоматы и ИПТ.
* **Отчёты PL Розничного блока, ВСП** – отображает сведения о месячной динамике доходов и баланса ВСП в разрезе продуктов с возможностью сравнения банков.

### Инструмент управления продажами

Используется региональными и территориальными менеджерами, отвечающими за продажи в ВСП. Визуализирует выполнение КПЭ продаж в разрезе продуктов и территориальных банков/подразделений в абсолютных и относительных по отношению к плану показателях, а также отображает географическое местоположение доп. офисов на карте с возможностью перейти к статистике КПЭ по выбранному доп. офису.

### Динамическая модель CIB

Предоставляет данные по портфелю клиентов в абсолютных показателях, как в суммарном выражении, так и в разрезе каждого клиента. Данные доступны по ряду показателей: наименование клиента, ИНН, активы, пассивы, доход, расход, ставки привлечения и размещения, нормы резервирования и т.д. Кроме этого приложение даёт возможность получения прогнозных показателей с онлайн расчётами на сервере MIS Портала путём ввода предстоящей сделки с клиентом. Введённые данные не сохраняются в БД MIS Портала, а полученные данные не сохраняются в мобильном устройстве.

### Выполнение ППР/КПЭ руководителей

Отчет отображает информацию по выполнению интегральных показателей ППР/КПЭ руководителей-членов Правления Сбербанка России – фактических и плановых значений – в том числе фотографии и оценки эффективности по каждому члену Правления. Данные для приложения сохраняются в мобильном устройстве для автономной работы.

### Отчёт по балансу Сбербанка

Отображает публичные сведения, касающиеся финансового состояния банка и дочерних банков: баланс и сведения о доходах и расходах. Отчёт позволяет проводить сравнения показателей за разные даты, а также по отношению к плановым показателям. Приложение сохраняет данные, полученные с сервера, на мобильном устройстве.

### Сравнение с конкурентами

Предоставляет возможности сопоставления публичных данных по балансу и сведений о доходах и расходах банка в сравнении конкурентами в абсолютных и относительных величинах с исторической ретроспективой. Отчёт также даёт возможность сравнивать финансовые коэффициенты банка с конкурентами. Данные для отчёта сохраняются в мобильном устройстве для автономной работы.

## Управление жизненным циклом мобильных приложений

Этот модуль состоит из двух компонентов: Сервера конфигураций (Configuration Server) и каталога приложений. Каталог приложений является частью внешней АС Afaria.

### Сервер конфигураций (Configuration Server)

В начале работы, а также каждые полчаса, мобильное приложение запрашивает адреса серверов синхронизации, с которым работает данное приложение. Полученные настройки используются в дальнейшем для подключения к серверу синхронизации (Sync Cache Server). Это позволяет гибко распределять нагрузку между несколькими серверами синхронизации, назначив выделенные узлы для каждого приложения МУ.

Также этот сервис проверят совместимость клиентской версии приложения с серверной инфраструктурой. В отношении каждой версии каждого мобильного приложения хранится настройка:

|  |  |  |
| --- | --- | --- |
| **Значение** | **Описание** | **Реакция сервиса** |
| ACTUAL | Рабочая версия | Продолжить работу |
| DEPRECATED | Устаревшая версия, но совместимая с серверным ППО | Продолжить работу и предупредить пользователя об устаревшей версии и о наличии обновления |
| DENIED | Устаревшая версия и несовместимая с серверным ППО | Прекратить работу с сообщением пользователю о необходимости обязательного обновления |

### Каталог приложений

Каталог приложений размещён на внешней АС – SAP Afaria.

Он обеспечивает хранение релизов и возможность их установки на мобильные устройства. Особенностью этого каталога является то, что различным пользователям могут быть доступны различные приложения в соответствии с их ролью. Клиентская часть на мобильном устройстве выполнена в виде отдельного приложения с графическим интерфейсом, позволяющим производить установку или обновление приложений.

Важным функционалом этого инструмента является удалённое управление МУ: соблюдение политик безопасности для предотвращения утечки данных, а также деинсталляция любого приложения АС iNavigator из МУ со всеми относящимися к нему данными. Функционал также позволяет производить рассылку широковещательных уведомлений, например, о необходимости обновить мобильное приложение.

## Модуль управления доступом и синхронизацией (Sync Cache Server)

Этот модуль состоит из следующих сервисов.

### Сервисы кэширования.

Сервисы кэширования файлов получают данные от сервисов транспортировки данных. Они делятся на сервисы:

* со статическим списком файлов, загружаемым из базы данных
* с динамическим списком файлов, который загружается из архивов для iRubricator

### Сервисы транспортировки данных.

Сервисы транспортировки данных бывают двух видов:

* Сервисы для работы со шлюзом односторонней передачи данных (файлоперекладчиком) – перемещают файлы с сетевой папки перекладчика на локальный диск.
* Сервисы для загрузки данных – загружают данные в память, делят их на части, архивируют и после этого обновляют данные в сервисах кэширования.

### Сервис SQL-запросов

Сервис SQL-запросов пересылает клиентский запрос в БД MIS Портала через шину двухсторонней передачи данных (DataPower). Сервис получает запросы в формате XML. Ответы также передаются в формате XML. Более подробная информация о методе передачи данных приведена в разделе «Потоки данных».

### Управляющая консоль

Административная консоль позволяет:

* Изменять настройки сервисов
* Останавливать и запускать сервисы
* Показывать последние ключевые события (не более 100)

### Функции безопасности

Производит аутентификацию пользователя в AD с использованием клиентского сертификата.

Производит авторизацию пользователя на предмет доступа к приложению, которое пытается получить данные с сервера. Поскольку данные о правах располагаются в БД MIS Портала, то запрос отправляется через двухсторонний шлюз обмена данными (DataPower).

### Функции журналирования событий

Все происходящие события вносятся в связанную БД в таблицу SYNC\_LOGS. Отслеживаемые события:

* Запрос мобильного устройства на получение конфигурации
* Запрос мобильного устройства на получение списка файлов
* Обновление файла в сервисе кеширования
* Все полученные запросы со стороны мобильного устройства
* Инциденты, связанные с нарушением в работе инфраструктуры
* Инциденты, связанные с отсутствием прав или доступов

### Перечень используемых сервисов

|  |  |  |
| --- | --- | --- |
| Название | Тип | Описание |
| Сервисы для работы с онлайн запросами | | |
| Online/misNotificationLogger | запускается по требованию | Сервис отправляет в альфу уведомления о загрузке или других изменениях в сигме. |
| Online/misSQLService | запускается по требованию | Данный сервис принимает и обрабатывает онлайн запросы от мобильных устройств |
| Online/misLdapUserCheckerService | Запускается автоматически | Сервис проверки прав на стороне LDAP |
| Online/misCachedSecurity | Запускается автоматически | Сервис кеширует результат проверки прав (misLdapUserCheckerService) для минимизации обращений в LDAP |
| Online/misDataPowerService | запускается по требованию | Сервис взаимодействия с Datapower |
| Online/misDataPowerSecurity | запускается по требованию | Сервис для проверки прав на стороне iRubrcator |
| Сервисы для работы с SQLITE файлами | | |
| Single/misFileLoader | Запускается автоматически | Данный сервис разбивает загруженные файлы на chunk и инициирует их загрузку в память (с помощью fileCache) |
| Single/misLocalInflater | Запускается автоматически | Данный сервис занимается разархивацией полученного из альфа SQLITE файла |
| Single/misFileService | запускается по требованию | Данный сервис обрабатывает запросы на скачивание файлов от мобильного устройства |
| Single/misFileCache | запускается по требованию | Данный сервис занимается загрузкой файлов разделенных на chunk в память. |
| Single/misDbFileLister | Запускается автоматически | Задача сервиса актуализировать список хостов в сигме на которые должны быть загружены файлы полученные из ALPHA |
| Single/misNetworkMover | Запускается автоматически | Данный сервис перемещает файлы из сетевой папки (ФП) в локальные папки сервера приложений для последующей загрузки в кеш сервер. Предполагается работа данного сервера в режиме кластера |
| Сервисы для работы с файлами iRubricator | | |
| Changeset/changesetFileCacheChecker | запускается по требованию | Данный сервис позволяет сравнить содержимое файлов рубрикатора в альфе и сигме и определить насколько данные рубрикатора синхронизированы с источником. |
| Changeset/changesetFileService | запускается по требованию | Данный сервис принимает запросы на скачивание файлов от мобильного устройства |
| Changeset/changesetFileCache | запускается по требованию | Данный сервис загружает в память кеш сервера все файлы рубрикатора |
| Changeset/misChangesetNetworkMover | Запускается автоматически | Данный сервис перемещает файлы из сетевой папки (ФП) в локальные папки сервера приложений для последующей загрузки в кеш сервер |
| Changeset/misMbrLoader | Запускается автоматически | Данный сервис разбивает полученные файлы рубрикатора на чанки и инициирует загрузку в память (с помощью changesetFileCache) |

## Модуль отслеживания и отправки актуальных данных с MIS Портала (Sync Generator)

Этот модуль состоит из следующих компонентов.

### SQLite Generator

На основе ETL-файла, представляющего собой XML с набором SQL-запросов, генерируется файл в формате SQLite, содержащий данные, возвращаемые SQL-запросами. Далее этот файл передаётся на одностороннюю шину передачи данных (файлоперекладчик), откуда он затем забирается модулем синхронизации.

### ChangeSet Generator

Извлекает данные из БД iRubricator и выкладывает их на диск в виде архива. Каждый архив содержит несколько файлов и XML-файл с описанием файлов. Далее этот архив также передаётся на одностороннюю шину передачи данных (файлоперекладчик), откуда он затем забирается модулем синхронизации.

### Управляющая консоль

Обеспечивает следующий функционал:

* Управление настройками сервисов
* Управление сервисами этого модуля: старт / остановка
* Управление генерацией SQLite файлов
* Показывать последние ключевые события (не более 100)

### Функции журналирования событий

Все происходящие события вносятся в связанную БД в таблицу sync\_log.

### Перечень используемых сервисов

|  |  |  |
| --- | --- | --- |
| Название | Тип | Описание |
| Общие сервисы | | |
| common/clusterManager | Запускается автоматически | На базе данного сервиса работает кластеризация. Он отслеживает статус текущего узла и при необходимости делает его активнымпассивным. |
| Сервисы необходимые для генерации SQLITE файлов и передачи их в сигма | | |
| Online/singleFileLister | Запускается автоматически | Данный сервис используется для загрузки и актуализации списка хостов на которые каждый SQLITE файл должен быть доставлен |
| Online/singleNetworkFileMover | Запускается автоматически | Данный сервис переносит сгенерированный файл в сетевую папку (ФП) для последующей отправки на сигму |
| Online/singleGenerator | Запускается автоматически | Основной сервис для генерации всех SQLITE файлов |
| Online/singleLocalDeflater | Запускается автоматически | Сервис архивирует файлы перед отправкой в сигму для уменьшения транспортных расходов |
| Сервисы необходимые для генерации файлов iRubricator и передачи их в сигма | | |
| changeset/changesetGenerator | Запускается автоматически | Данный сервис анализирует базу рубрикатора на предмет новых файлов и при необходимости генерирует changeset с архивом для передачи его в сигма |
| Changeset/changesetNetworkMover | Запускается автоматически | Данный сервис перемещается сгенерированный changeset-файл, содержащий один или несколько файлов рубрикатора на сетевой ресурс(ФП) |

## Модуль выполнения онлайн запросов (SQL Proxy Server)

В ждущем режиме, модуль не производит никакой работы. Вместо этого, ожидает подключения со стороны DataPower. DataPower присылает на этот модуль задание в формате XML. Задание содержит SQL-запрос, который формируется в приложении на мобильном устройстве. SQL-запрос имеет ссылку на ту или иную базу данных MIS Портала, поэтому такой запрос может выполнятся на любой (или нескольких) базах. Задача этого модуля – выполнить полученный SQL-запрос и вернуть результат также в формате XML обратно на шину DataPower.

Более подробно такие XML запросы описаны в разделе «Потоки данных».

## Модуль мониторинга (Alpha Monitor, Sigma Monitor)

Модуль состоит из двух независимых узлов – Alpha Monitor и Sigma Monitor – каждый в своём сегменте сети. В тоже время, их работа предполагается в связке, а общение – через шлюз двухстороннего обмена данными – DataPower. В каждом модуле имеется настройка, содержащая список почтовых адресов, по которым приходит уведомление при возникновении отслеживаемого события. Кроме того, Alpha Monitor имеет дополнительный модуль – DP SMSProxy – позволяющий рассылать SMS уведомления о возникновении нештатной ситуации. Список телефонных номеров также указывается в настройках.

### Alpha Monitor

Контролирует:

* Процесс генерации файлов в модуле отслеживания и отправки актуальных данных (SQLite Generator). В настройках по каждому SQLite файлу сохранено ожидаемое время генерации. При превышении этого времени, инициируется событие мониторинга.
* Доступность шлюза односторонней передачи данных – файлоперекладчика. С некоторой периодичностью происходит измерение размера сетевой папки файлоперекладчика. Если размер папки превышает заданный в настройках лимит или папка не доступна, инициируется событие мониторинга.
* Доставку файла в сегмент Sigma. При этом в базу данных уведомлений записывается сообщение о том, что файл не доставлен в сигму с датой актуальности +30 минут. Если в течение 30 минут файл не будет доставлен до сигмы и сервер в сигме не отправит запрос через Datapower для удаления данного уведомления – оно будет отправлено службе поддержки.
* Работоспособность Alpha Monitor. Через заданный промежуток времени сервис мониторинга вызывают команду ping - обновляя в своей локальной базе данных информацию о дате последней доступности сервера. В случае, если это дата отличается более чем на 5 минут от текущей, будет послано уведомление об ошибке.

### Sigma Monitor

Контролирует:

* Доступность шлюза односторонней передачи данных – файлоперекладчика. С некоторой периодичностью происходит измерение размера сетевой папки файлоперекладчика. Если размер папки превышает заданный в настройках лимит или папка не доступна, инициируется событие мониторинга.
* Доставку файла в сегмент Sigma. При получении файла, отправляет подтверждение в Alpha Monitor с указанием MD5 сигнатуры полученного файла. Событие мониторинга инициируется в Alpha Monitor.
* Работоспособность Sigma Monitor. Через заданный промежуток времени сервис мониторинга отправляет команду ping - обновляя в базе данных MSSQL Alpha информацию о дате последней доступности сервера. В случае, если это дата отличается более чем на 5 минут от текущей, будет послано уведомление об ошибке.
* Доступность Шлюза двухсторонней передачи данных – DataPower. Производится косвенная проверка, т.к. опрос Sigma Monitor производится именно через него.

# Архитектура данных

Необходимо учитывать, что основной задачей системы является доставка существующих данных из внутренних ресурсов Банка на мобильные устройства пользователей. Поэтому система не предполагает выделенного хранилища данных.

## Источники данных

Источниками данных являются различные витрины БД MIS Портала, которые на момент составления этого документа развёрнуты на сервере finik1. Данные могут быть представлены в виде фактов, хранящихся в таблицах БД, либо в бинарном виде как файлы PDF, Word, Excel, PowerPoint, хранящихся также в таблицах БД. Загрузка, консолидация, обсчёт этих данных лежит за пределами работы АС iNavigator.

АС не оказывает влияния на данные в БД – не инициирует загрузку, обсчёт, изменение первичных данных. Хотя при экспорте из MIS Портала происходит некоторая трансформация данных, но результат этих трансформаций используется исключительно АС iNavigator. Более подробно об этих трансформациях описано в потоках передачи данных при оффлайн визуализации.

Ниже представлен список витрин, используемых в качестве основного источника. Вспомогательными источниками являются различные справочники на MIS Портале.

* MIS\_RETAIL\_ATM, MIS\_MOBILE – используется для отчётов АТМ;
* MIS\_RETAIL\_CRED, MIS\_MOBILE – используется для отчётов розничного бизнеса;
* MIS\_PCA\_DKK\_TD, MIS\_PCA\_DKK\_DATA, MIS\_MOBILE – используется для отчётов CIB;
* MIS\_NAVIGATOR\_KPI, MIS\_NAVIGATOR\_DATA – используется для iNavigator;
* MIS\_RUBRICATOR – база для Рубрикатора отчётов, где хранятся файлы отчётов, каталог и настройки;
* MIS\_IUP\_KPI, MIS\_IUP\_DATA – используется для отчёта ИУП;
* MIS\_DYNAMIC\_MODEL – база для отчётов динамической модели CIB;
* MIS\_COMPETITORS\_NT – используется для отчётов по сравнению с конкурентами;
* DASHBOARD\_PPR – отчёт КПЭ/ППР руководителей;
* MIS\_RETAIL\_VSP\_MOBILE – отчёт по PL ВСП.
* MIS\_BALANCE – отчет по Балансу

## Потоки данных

В АС выделяются следующие типы потоков данных в зависимости от их природы:

* Исходные данные – первичные данные для визуализации на МУ;
* Метаданные, настройки – потоки данных, включающие служебную информацию о правах доступа пользователей, форматировании данных, настойки конфигурации.

Кроме того, в зависимости от решаемых задач потоки данных могут быть разделены на:

* Потоки передачи данных в кэш мобильного устройства;
* Потоки передачи данных при онлайн запросе;
* Потоки модификации отчётов.

На рисунке представлена общая схема потоков данных АС, которая описывает межкомпонентные взаимодействия на уровне архитектуры в целом. Потоки данных пронумерованы для последующей идентификации и описания, а также окрашены в соответствующий их типу цвет (см. легенду).



Рисунок 2. Диаграмма потоков данных

### Консолидация данных

Консолидация данных не входит в область задач АС, а приведена здесь для полноты картины.

Наполнение источников происходит при помощи специальных процедур с различной периодичностью времени. Само событие обновления данных не передаётся в АС iNavigator, а только обновляется информация о наличии новых данных.

Наполнение источника для приложения iRubricator в части документов PDF, Word, Excel, PowerPoint, а также изменение каталога этих отчётов выполняется вручную сотрудником Департамента Финансов через специальный интерфейс. Загрузка документов приводит к обновлению информации о наличии нового отчёта.

Структура данных некоторых источников не позволяет эффективно их использовать на мобильном приложении, поэтому на заключительном этапе подготовки данных в источнике происходит их трансформация к приемлемому виду. Приложение 2 перечисляет процедуры, используемые для проведения таких трансформаций для каждого конкретного отчёта. Результат всех этих преобразований консолидируется в БД MIS\_MOBILE.

### Потоки передачи данных в кэш мобильного устройства (МУ) – офлайн визуализация

С учётом специфики работы АС такой как передача существенных объёмов данных по каналам с ограниченной пропускной способностью, предусмотрено промежуточное хранение данных с максимальным сближением к МУ. В данном случае используется хранилище непосредственно в сети Sigma, а также специальный функционал поддерживающий актуальность данных в нём.

По этой модели построена работа всех отчётов, которые позволяют работать в офлайн режиме. Приложение 1 содержит список таких приложений.

**Поток 1.1.a** Модуль отслеживания актуальных данных (Sync Generator) с заданной периодичностью проверяет время последней модификации данных на MIS Портале. Затем он сравнивает это время со временем последней выгрузки данных. При обнаружении более актуальных данных в источнике, запускается процесс экспорта. Приложение 3 содержит список объектов, которые возвращают сведения о времени модификации данных в источнике в зависимости от приложения МУ. Все они собраны в процедуре SP\_IPAD\_GET\_ACTUAL\_DATE базы данных MIS\_IPAD, как в единой точке для модуля Sync Generator. Сведения о времени последней выгрузки хранятся в таблице IPAD\_JOBS базы данных этого модуля (MIS\_IPAD\_GENERATOR).

После окончания выгрузки данных, обновляются сведения о времени выгрузки в таблице IPAD\_JOBS.

**Поток 1.1.b** Альтернативно предусмотрен ручной запуск процедуры экспорта данных из MIS Портала. Это реализуется в модуле отслеживания актуальных данных (Sync Generator) через специальную панель управления Оператором данных, где он может также отслеживать ход процедуры.

Приложение 4 содержит список файлов, для которых предусмотрен только ручной, либо автоматический (с возможностью ручного запуска) способ генерации файла.

**Поток 1.2.** В модуле выгрузки данных (Sync Generator) существуют ETL-файлы для каждого мобильного приложения, которые описывают сценарий формирования каждого SQLite-файла. Пример ETL-файла показан ниже, а сценарий генерации SQLite-файла приведён в тэге etl-action-pattern.

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<etl-config>

<etl-action dataFile="mis\_iup\_kpi.sqlite" patternName="MIS\_IUP\_KPI" autoRun="true" manualRun="true" generationMode = "ON\_CONDITION" />

<etl-action-pattern patternName="MIS\_IUP\_KPI" application="IUP" jndi="jdbc/finik1" database="mis\_iup\_kpi">

<name seriesIndex="0" seriesName="Dashboards"/>

<query>SELECT \* FROM Dashboards</query>

<name seriesIndex="1" seriesName="Default\_params"/>

<query>SELECT \* FROM Default\_params</query>

<name seriesIndex="2" seriesName="Iup\_role"/>

<query>SELECT \* FROM Iup\_role</query>

<name seriesIndex="3" seriesName="Links"/>

<query>SELECT \* FROM Links</query>

<name seriesIndex="4" seriesName="UnitIdDept"/>

<query>SELECT \* FROM UnitIdDeprt</query>

<name seriesIndex="5" seriesName="DATA"/>

<query>EXECUTE GET\_MOBILE\_DATA</query>

<change-type seriesIndex="5" fields="dt" newDataType="92"/>

<name seriesIndex="7" seriesName="KPI"/>

<query>EXECUTE GET\_MOBILE\_KPI</query>

<name seriesIndex="8" seriesName="MEASURE"/>

<query>EXECUTE GET\_MOBILE\_MEASURE</query>

<query>CREATE UNIQUE INDEX PK\_DATA ON DATA(DEPRT\_ID COLLATE BINARY ASC,DynType COLLATE BINARY ASC,DT COLLATE BINARY ASC,KPI\_ID COLLATE BINARY ASC)</query>

</etl-action-pattern>

</etl-config>

Перечень генерируемых файлов в разрезе каждого отчёта, а также имена ETL-файлов и БД-источников привёден в Приложение 5.

Отчёты Рубрикатора, хранящиеся в источнике как файлы DOC, XLS, PDF, PPT импортируются через прямой запрос к БД MIS\_RUBRICATOR. Выгруженные файлы упаковываются в архив с добавлением XML-файла – описания архива.

select top 1 res, operation, id, file\_name, change\_date, data

from (

      select b.resource\_id res, 'u' operation, a.id , r.file\_name, a.change\_date, r.data

      from report a ,report\_resource b,resource r

      where a.change\_date>=? and a.report\_Type in (

            select id

            from report\_type

            where ident in ('mis\_report', 'doc')

            )

      and a.id= b.report\_id and b.resource\_id = r.id

      union

      select c.resourceId res, c.operation, c.resourceId id, filename\_ file\_name, c.date\_ change\_date, null data

      from changelog c, (select resourceId, max(date\_) date\_ from changelog where date\_>=? group by resourceId) l

      where c.date\_=l.date\_ and c.resourceId=l.resourceId and c.operation='d'   ) qry

where change\_date > ? or id > ?   order by change\_date, id

**Поток 1.3.** Сформированные на шаге 1.2 файлы упаковываются в архив, а затем через файлоперекладчик переносятся в сетевую папку сети Sigma. Файлы SQLite и отчёты Рубрикатора располагаются в двух различных папках. Упаковка в архив с одной стороны снижает нагрузку и скорость передачи через файлоперекладчик, а с другой – гарантирует целостность файла, т.к. при распаковке проверяется его сигнатура.

На этом шаге происходит перенос файла из сети Alpha в сеть Sigma на зеркальную сетевую папку.

Модуль синхронизации (Sync Cache Server) с интервалом времени 60 секунд просматривает эту папку на предмет наличия файлов. При их обнаружении, производит копирование в своё локальное хранилище, а затем распаковку.

В том случае, если файл должен быть доставлен на 2 и более серверов sync cache server, с помощью создания файлов FILE\_NAME.HOST.SYNC.START.LOK и FILE\_NAME.HOST.SYNC.FINISH.LOK контролируется, что файл был доставлен на все требуемые хосты.

Хранилище модуля синхронизации (Sync Cache Server) представляет собой локальную папку. Файлы здесь хранятся в архивированном состоянии и разбиты на части для повышения надёжности передачи по каналам связи в случае обрыва. При сохранении в этом хранилище нового файла с именем уже существующего файла, старый файл заменяется новым. Для ускорения загрузки файлов на мобильное устройство, все файлы загружаются в память при запуске приложения. Вновь загруженные или обновленные файлы обновляются в памяти в процессе работы.

**Поток 1.4.** При старте или при разворачивании приложения в МУ, но не реже чем 1 раз в 30 минут, происходит обращение по фиксированному адресу для получения адреса сервера синхронизации. Передача настроек выполняется одинаково для всех приложений, но в зависимости от приложения, ему может быть возвращён тот или иной адрес, что позволяет распределять нагрузку между несколькими серверами синхронизации. Состав параметров конфигурации для каждого приложения может быть различным.

**Поток 1.5.** Используя полученные настройки, на следующем шаге запускается синхронизация. Приложение обращается к серверу синхронизации и тот возвращает реестр всех файлов, хранящихся на нём. В отношении каждого файла содержатся сведения:

* К какому мобильному приложению относится файл
* Дата последней модификации
* Имя файла
* Хэш-сумма файла
* Количество частей, на которое разбит файл

Благодаря этим сведениям, приложение способно определить список необходимых ему файлов, а также сравнить по хэш-сумме и дате последней загрузке актуальность файлов, хранящихся на устройстве.

При обнаружении более актуальной версии файла на сервере, приложение инициирует его скачивание.

**Поток 1.6.** Сервер синхронизации авторизует пользователя на наличие соответствующей роли, прописанной в БД MIS\_BASE2 на MIS Портале. Более подробное этого механизма и ролей приведено в разделе Информационная безопасность.

Поскольку проверка доступа происходит в сегменте сети Sigma, то система отправляет свой запрос на шину DataPower аналогично, как это описано в шагах 2.4 – 2.6 в модели онлайн запросов с той разницей, что запрос формируется и получателем результата является сервер синхронизации.

**Поток 1.7.** Так как файл на сервере хранится в виде архива, разбитого на части, то приложению на МУ необходимо получить все части, распаковать архив и сохранить полученный файл в своё хранилище. Каждое приложение на МУ имеет своё независимое хранилище необходимых файлов.

**Поток 1.8.** При открытии приложения/отчёта на МУ, извлекаются конфигурационные сведения, которые указывают: из какого источника и какие данные необходимо предоставить.

**Поток 1.9.** В зависимости от функционального назначения того или иного приложения на МУ, открываются документы PDF, Word, Excel, PowerPoint или происходит запрос к закэшированной БД SQLite.

**Поток 1.10.** Пользователь получает необходимые сведения.

### Потоки передачи данных при онлайн визуализации

Некоторым приложениям на МУ при работе может потребоваться самая актуальная информация, для чего необходимо выполнить запрос непосредственно на самой БД MIS Портала. Учитывая специфику системы, где визуализация происходит за пределами инфраструктуры банка, а источник данных – в защищённом сегменте Alpha, построен механизм надёжного и безопасного двухстороннего обмена данными (запрос-ответ) между МУ и БД MIS Портала. Выполнение норм безопасности, пропускная способность каналов связи и многозвенность цепочки элементов в этом процессе накладывает ограничения на объёмы передаваемых данных и своевременность отклика системы.

По этой модели построены отчёты, которые предполагают интерактивное взаимодействие с БД MIS Портала. Приложение 1 содержит список таких приложений.

**Поток 2.1.** На первом шаге приложение получает настройки конфигурации аналогично, как это происходит на шаге 1.6. в процессе кеширования файлов.

**Поток 2.2.** Приложение на МУ в зависимости от своей логики формирует SQL-запрос и в составе XML-файла отправляет на сервер. Одним из атрибутов этого XML-файла является указание на целевой источник – DATAPOWER. Таким образом, сервер синхронизации определяет необходимость передачи этого запроса для выполнения на БД MIS Портала.

Ниже представлен пример XML запроса с МУ на MIS Портал:

**<?xml version="1.0" encoding="UTF-8" standalone="yes"?>**

<request>

<stored-procedure>

select ? as dt, ? as varchr from \_tUser where userid=?

</stored-procedure>

<arguments>

<argument>

<index>1</index>

<type>DATE</type>

<value>2014-03-31</value>

</argument>

<argument>

<index>2</index>

<type>STRING</type>

<value>мой текст</value>

</argument>

<argument>

<index>3</index>

<type>NUMBER</type>

<value>5</value>

</argument>

</arguments>

<Fields>

<Field Name="dt" Type="DATE"/>

<Field Name="varchar" Type="STRING"/>

</Fields>

<provider>DATAPOWER</provider>

<service>finik1</service>

</request>

**Поток 2.3.** Сервер синхронизации авторизует пользователя аналогично, как это происходит на шаге 1.8 в процессе кеширования файлов.

**Поток 2.4.** Шина, которая представляет собой связку – DataPower в сети Sigma, IBM MQ в сети Sigma, IBM MQ в сети Alpha, DataPower в сети Alpha – производит валидацию полученного XML-файла по заранее сохранённой XSD-схеме.

**Поток 2.5.** На следующем шаге специальный модуль, расположенный в сети Alpha и имеющий возможность подключиться непосредственно к базе MIS Портала, выполняет полученный SQL-запрос. Логика этого запроса формируется в приложении МУ в зависимости от поставленной задачи.

**Поток 2.6.a и 2.6.b.** Результат, полученный на БД, возвращается обратно на шину, затем на сервер синхронизации и в конечном итоге приложению на МУ.

Время, когда сервер синхронизации передаёт запрос на шину, затем передаётся по шине из сети Sigma в сеть Alpha, потом выполняется на БД MIS Портала и, наконец, возвращается обратно через шину на сервер синхронизации, ограничено таймаутом шины. При истечении этого таймаута, шина обрывает запрос сервера синхронизации, а клиент получает ошибку соединения.

Ниже представлен пример ответа при успешном выполнении SQL-запроса:

**<?xml version="1.0" encoding="UTF-8" standalone="yes"?>**

**<Response Result="OK">**

**<Metadata RowCount="3">**

**<Field Name="kpi\_id" Type="NUMBER"/>**

**<Field Name="item\_id" Type="NUMBER"/>**

**<Field Name="ord" Type="NUMBER"/>**

**<Field Name="pokType" Type="NUMBER"/>**

**<Field Name="addMenu" Type="NUMBER"/>**

**<Field Name="pok\_id" Type="NUMBER"/>**

**</Metadata>**

**<Dataset>**

**<R>**

**<F>14792</F>**

**<F>7</F>**

**<F>1</F>**

**<F/>**

**<F>0</F>**

**<F>12859</F>**

**</R>**

**<R>**

**<F>14792</F>**

**<F>7</F>**

**<F>1</F>**

**<F/>**

**<F>0</F>**

**<F>12860</F>**

**</R>**

**<R>**

**<F>14792</F>**

**<F>1525</F>**

**<F>2</F>**

**<F/>**

**<F>0</F>**

**<F>12859</F>**

**</R>**

**</Dataset>**

**</Response>**

При проблемах с каналом передачи данных возвращается примерно такой ответ:

**<?xml version="1.0" encoding="UTF-8" standalone="yes"?>**

**<Response Result="FAIL">**

**<Error>Error while processing request to DataPower Error sending request to http://10.21.7.238:4004</Error>**

**</Response>**

В случае не корректного SQL-запроса возвращается примерно такой ответ:

**<?xml version="1.0" encoding="UTF-8" standalone="yes"?>**

**<Response Result="FAIL">**

**<Error>PreparedStatementCallback; bad SQL grammar [select \* from tablename]; nested exception is com.microsoft.sqlserver.jdbc.SQLServerException: Invalid object name 'tablename'.</Error>**

**</Response>**

**Поток 2.7.** Пользователь получает необходимые сведения.

Ниже, будет дано более подробное описание XML-взаимодействия при онлайн запросах.

Каждый запрос представляет собой XML документ соответствующий некоторой XSD схеме. Схема настроена на Datapower на стороне Sigma и используется для валидации входящего запроса.

**<?xml version="1.0" ?>**

**<xs:schema attributeFormDefault="unqualified" elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema">**

**<xs:element name="request">**

**<xs:complexType>**

**<xs:sequence>**

**<xs:element name="sql-template">**

**<xs:simpleType>**

**<xs:restriction base ="xs:string">**

**<xs:maxLength value="64"/>**

**<xs:pattern value="[0-9A-Za-z\_.]\*"/>**

**</xs:restriction>**

**</xs:simpleType>**

**</xs:element>**

**<xs:element minOccurs="0" name="arguments">**

**<xs:complexType>**

**<xs:sequence>**

**<xs:element maxOccurs="unbounded" minOccurs="0" name="argument">**

**<xs:complexType>**

**<xs:sequence>**

**<xs:element maxOccurs="1" minOccurs="1" name="index">**

**<xs:simpleType>**

**<xs:restriction base="xs:integer">**

**<xs:minInclusive value="1"/>**

**</xs:restriction>**

**</xs:simpleType>**

**</xs:element>**

**<xs:element maxOccurs="1" minOccurs="1" name="type">**

**<xs:simpleType>**

**<xs:restriction base="xs:string">**

**<xs:enumeration value="DATE"/>**

**<xs:enumeration value="NUMBER"/>**

**<xs:enumeration value="STRING"/>**

**<xs:enumeration value="BLOB"/>**

**</xs:restriction>**

**</xs:simpleType>**

**</xs:element>**

**<xs:element maxOccurs="1" minOccurs="0" name="value">**

**<xs:simpleType>**

**<xs:restriction base="xs:string">**

**<xs:maxLength value="4000000"/>**

**<xs:pattern value="[0-9A-Za-z\_,.&amp;\&lt;\&gt;&quot;&apos;@\?!\/\\=\[\]\s\S\t\v\n\r]\*"/>**

**</xs:restriction>**

**</xs:simpleType>**

**</xs:element>**

**</xs:sequence>**

**</xs:complexType>**

**</xs:element>**

**</xs:sequence>**

**</xs:complexType>**

**</xs:element>**

**<xs:element maxOccurs="1" minOccurs="0" name="Fields">**

**<xs:complexType>**

**<xs:sequence>**

**<xs:element maxOccurs="unbounded" name="Field">**

**<xs:complexType>**

**<xs:attribute name="Name" use="required">**

**<xs:simpleType>**

**<xs:restriction base="xs:string">**

**<xs:maxLength value="64"/>**

**</xs:restriction>**

**</xs:simpleType>**

**</xs:attribute>**

**<xs:attribute name="Type" use="required">**

**<xs:simpleType>**

**<xs:restriction base="xs:string">**

**<xs:enumeration value="DATE"/>**

**<xs:enumeration value="NUMBER"/>**

**<xs:enumeration value="STRING"/>**

**<xs:enumeration value="BLOB"/>**

**</xs:restriction>**

**</xs:simpleType>**

**</xs:attribute>**

**</xs:complexType>**

**</xs:element>**

**</xs:sequence>**

**</xs:complexType>**

**</xs:element>**

**<xs:element maxOccurs="1" name="provider" type="xs:string" minOccurs="0" />**

**<xs:element maxOccurs="1" minOccurs="0" name="alpha-web-host">**

**<xs:simpleType>**

**<xs:restriction base="xs:string">**

**<xs:maxLength value="64"/>**

**</xs:restriction>**

**</xs:simpleType>**

**</xs:element>**

**<xs:element maxOccurs="1" minOccurs="0" name="alpha-db-host">**

**<xs:simpleType>**

**<xs:restriction base="xs:string">**

**<xs:maxLength value="64"/>**

**</xs:restriction>**

**</xs:simpleType>**

**</xs:element>**

**</xs:sequence>**

**</xs:complexType>**

**</xs:element>**

**</xs:schema>**

Описание полей дано в таблице

|  |  |
| --- | --- |
| Поле | Описание |
| sql-template | Имя шаблона в БД Alpha. Имя шаблона может состоять из   * латинских символов * Точек * нижнего подчеркивания * цифр   и иметь длину не более 64 символов. |
| Arguments | Параметры шаблона. В случае если шаблон содержит входящие параметры, они должны передаваться внутри данного тега. |
| Provider | На текущий момент может принимать два значения:   * DISPATCHER( если XML отправляется в datapower приложением или вручную) * DATAPOWER ( если XML отправляется из мобильного приложения) |
| alpha-web-host | Наименование хоста прокси сервера в Alpha, на который будет передан XML документ. |
| alpha-db-host | Название группы настроек (например finik1-new или finik2-new) для подключения к базе данных на которой будет выполнен запрос. |

В целях удовлетворения требованиям безопасности, по сети не отправляются SQL запросы – вместо этого используется механизм шаблонов. Шаблон, это объект хранимый в БД Alpha. Он имеет название и тело. Название будет использоваться в поле sql-template, поэтому должно учитывать ограничения на это поле. Тело - это любой SQL скрипт, в котором возможно использовать параметры. Для хранения шаблонов на сервере используется таблица SQL\_TEMPLATES.

### Потоки модификации отчётов

**Поток 3.1.** Администратор мобильных приложений отправляет в каталог Afaria пакет мобильного приложения, включающий метаданные отчёта.

**Поток 3.2.** Пользователь МУ через каталог Afaria получает доступные ему приложения.

**Поток 3.4.** При установке или обновлении приложения обновляются метаданные соответствующих отчётов.

# Архитектура приложений

Система реализуется следующим набором программных средств:

* Приложения на мобильном устройстве
* Приложения Java EE
* Сервер приложений
* СУБД MS SQL Server
* Шина DataPower & IBM MQ



Рисунок 3. Диаграмма взаимодействия приложений

## Приложения на мобильном устройстве

АС реализована следующим набором приложений для работы на платформе iOS:

* iNavigator
* iRubricator
* MISMobile
* ИУП (Инструмент управления продажами)
* Динамическая модель CIB
* Выполнение ППР/КПЭ руководителей
* Отчёт по балансу Сбербанка
* Сравнение с конкурентами

Основной задачей всех приложений является визуализация данных в зависимости от своего функционального предназначения. Визуализация может быть в виде таблиц, графиков, дэшбордов, карты местности, просмотра документов или комбинацией этих возможностей. Например, при просмотре дэшборда может быть возможность открыть документ PDF при клике на каком-либо элементе.

Дополнительно каждое приложение несёт задачу по проверке наличия свежих данных на сервере и загрузке этих данных на устройство.

Каждое приложение имеет средства аутентификации, описанные в разделе «Защита информации».

## Приложения Java EE

Java EE – это технология создания высокопроизводительных приложений для серверной части, открывающая возможности по масштабируемости и переносимости созданных модулей. Средствами Java EE реализованы:

* Configuration Server
* Sync Cache Server
* Sync Generator
* SQL Proxy Server
* Monitor Alpha
* Monitor Sigma

Дистрибутив каждого приложения собран в виде WAR-пакета для развёртывания его на одном или нескольких серверах.

Все приложения Sync имеют пользовательский web-интерфейс для изменения и управления своими функциями. В составе каждого приложения запускается ряд служб – потоков, выполняющих все основные действия. Верхнеуровневое управление осуществляется из административной консоли сервера приложений.

Аутентификация в web-интерфейсе производится с использованием реестра пользователей, сохранённого в каждом приложении.

Более подробная информация по управлению и настройке содержится в соответствующей документации этих приложений.

## Сервер приложений

В роли сервера приложений выступает IBM Web Application Server (IBM WAS) (<http://ibm.com/software/webservers/appserv/was/was-library/>), который обеспечивает хостинг JEE приложений.

Управление сервером производится стандартными средствами – административной консолью: установка/деинсталляция Java EE приложений, запуск/остановка приложений, управление кластерным механизмом, связывание с БД и т.д.

Аутентификация производится с помощью встроенных учётных записей.

## СУБД MS SQL

Хранит настройки серверных приложений и журнал событий. Предусмотрено создание отдельной БД для каждого приложения. При работе серверного приложения в режиме кластера, обе ноды этого приложения используют одну БД.

В составе СУБД MS SQL Server используется компонент Database Engine, который представляет собой основную службу для хранения, обработки и обеспечения безопасности данных. Этот компонент обеспечивает управляемый доступ к ресурсам и быструю обработку транзакций.

Контроль прав доступа на уровне БД осуществляется стандартными средствами MS SQL Server.

## Шина DataPower & IBM MQ

Обеспечивает надёжный и безопасный двухсторонний обмен данными между двумя сегментами сети Alpha и Sigma. Используется при выполнении онлайн запросов, поступающих из мобильного устройства или из сервера синхронизации, расположенного в сети Sigma, в адрес БД MIS Портала, расположенного в защищённой сети Alpha. Подключение к DataPower осуществляется по протоколу HTTP, а само сообщение может быть в формате XML для передачи данных или в формате BASE64 для передачи бинарных данных, таких как документы PDF и т.п.

Управление шиной производится через стандартную веб-страницу административной консоли этой шины.

## SAP Afaria

SAP Afaria не входит в состав АС iNavigator, а является внешней системой. Тем не менее, она выполняет ключевую роль в управлении приложениями на мобильных устройствах: установка, обновление, удаление, соблюдение политик безопасности на мобильном устройстве. Существует возможность оповещать пользователей о доступных обновлениях через механизм широковещательных уведомлений. Также Afaria позволяет удалённо деинсталлировать приложения с мобильного устройства вместе с сохранённым кэшем данных.

Управление системой – публикация дистрибутивов приложений, выдача прав пользователям и т.д. – производится через администраторов этой АС.

# Техническая архитектура

Для функционирования АС требуется следующий набор технических средств:

| **Компонент архитектуры** | **Требования к техническим характеристикам** | **Требования к программному обеспечению** | **Комментарий по использованию** |
| --- | --- | --- | --- |
| WAS Alpha - генерация данных | Тип: виртуальный  ЦП: 4 ядер  ОЗУ: 24 Гб  ПЗУ: 100+160 Гб | OS: Windows 2008 R2  IBM WebSphere AS 7.1  - Sync Generator | Модуль отслеживания актуальных данных |
| WAS Alpha - online-запросы | Тип: виртуальный  ЦП: 6 ядер  ОЗУ: 24 Гб  ПЗУ: 100 Гб | OS: Windows 2008 R2  IBM WebSphere AS 7.1  - SQL Proxy Server | Модуль выполнения онлайн запросов |
| WAS Sigma - Configuration Server & Online | Тип: виртуальный  ЦП: 6 ядер  ОЗУ: 24 Гб  ПЗУ: 100 Гб | OS: Windows 2008 R2  IBM WebSphere AS 7.1  - Configuration Server  - Sync Cache Server | Размещение сервера конфигураций модуля управления приложениями  Модуль управления данными – онлайн отчёты (См. Приложение 1) |
| WAS Sigma – Offline (несколько серверов) | Тип: виртуальный  ЦП: 4 ядер  ОЗУ: 48 Гб  ПЗУ: 100+150 Гб | OS: Windows 2008 R2  IBM WebSphere AS 7.1  - Sync Cache Server | Модуль управления данными – офлайн отчёты (См. Приложение 1) |
| MSSQL Sigma | Тип: виртуальный  ЦП: 4 ядер  ОЗУ: 32 Гб  ПЗУ: 100+135 Гб | OS: Windows 2008 R2  MS SQL 2012 | Хранение настроек Configuration Server и журнала пользовательской активности Sync Cache Server |
| MSSQL Alpha | Тип: виртуальный  ЦП: 4 ядер  ОЗУ: 32 Гб  ПЗУ: 100+1024 Гб | OS: Windows 2008 R2  MS SQL 2012 | Хранение логов генерации и онлайн запросов + настройки для всех приложений в альфа |
| Мобильные устройства пользователей |  | iOS версии не ниже 7 | Визуализация у конечного пользователя |
| Комплект DataPower/IBM MQ | – | – | Шина передачи данных между сегментами Alpha - Sigma |
| Файлоперекладчик | ПЗУ: 30 Гб (Alpha) + 30 Гб (Sigma) | – | Перенос больших файлов из Alpha в Sigma |
| Рабочее место администратора |  | Web-браузер Internet Explorer версии не ниже 8.0 | Управление модулями: конфигураций, распределения прав SyncGenerator |
| Рабочее место оператора данных |  | Web-браузер Internet Explorer версии не ниже 8.0 | Запуск заданий генерации файлов SyncGenerator |

## Распределение нагрузки и обеспечение бесперебойности при синхронизации МУ

Синхронизации данных предшествует извлечение настроек с сервера конфигураций, как это описано в потоках передачи данных при офлайн и онлайн визуализации раздела «3.2 Потоки данных». Сервер конфигураций определяет: какое мобильное приложение производит синхронизацию, а затем, возвращает ему тот или иной список серверов Sync Cache Server. В каждом таком списке содержится как минимум два сервера. МУ пытается подключиться к первому серверу из списка, а при неудаче – переходит к следующему серверу в списке.

Сопоставление мобильных приложений к разным серверам Sync Cache Server производится эмпирическим методом, в зависимости от общей нагрузки на каждое приложение, и сохранено в административной консоли модуля Configuration Server.

Обеспечение бесперебойности реализуется при помощи кластеризации. Каждый сервер имеет две ноды, которые работают в следующих режимах:

* Active-Active – обе ноды работают в активном режиме независимо.
* Active-Passive – одна нода ведущая, вторая – спящая.

|  |  |  |
| --- | --- | --- |
| **Ресурс** | **Режим работы** | **Обеспечение бесперебойности** |
| WAS Alpha - генерация данных | Active-Passive | Обеспечивается программными средствами SyncGenerator. |
| WAS Alpha - online-запросы | Active-Active | Обеспечивается средствами балансировщика сети Alpha между DataPower и SQL Proxy Server |
| WAS Sigma - Configuration Server & Online | Active-Active | Адреса обеих нод Configuration Server сохранены на мобильном устройстве и при неудачной попытке, оно пытается подключиться к другой ноде.  Аналогично с Sync Cache Server: мобильное устройство получает адреса всех нод. |
| WAS Sigma – Offline (несколько серверов попарно связаны в несколько кластеров) | Active-Active | Мобильное устройство получает адреса обеих нод Sync Cache Server и при неудачной попытке, оно пытается подключиться к другой ноде. |
| MSSQL Sigma | Active-Passive | Ноды серверов приложений работают с СУБД своей площадки |
| MSSQL Alpha | Active-Passive | Ноды серверов приложений работают с СУБД своей площадки |
| DataPower/IBM MQ | Active-Active | Определение активной ноды производится программными средствами Sync Cache Server |
| Файлоперекладчик | Active-Active | Оба файлоперекладчика функционируют независимо. Бесперебойность реализована средствами серверных приложений: Sync Generator и Sync Cache Server |

Рисунок 4. Диаграмма кластерного решения

# Взаимодействие с окружением

В своей работе АС утилизирует модули собственной и внешних систем. В таблице отражены модули системы и их зависимость от других компонентов окружения.

|  |  |  |  |
| --- | --- | --- | --- |
| **Модуль** | **Внешняя доступность функций** | **Потребляет сервисы подсистем** | **Потребляет сервисы внешних АС** |
| Мобильные приложения | Нет | Сервер конфигураций  Сервер синхронизации | Afaria |
| Сервер конфигураций | Да |  |  |
| Сервер синхронизации | Да | Sync Generator  SQL Proxy Server | Служба каталогов Active Directory  Файловый ресурс сети Sigma  Файловый перекладчик Alpha-Sigma  Шина передачи данных Alpha-Sigma |
| Sync Generator | Нет |  | База данных MIS Портала на finik1  Файловый ресурс сети Alpha |
| SQL Proxy Server | Да |  | База данных MIS Портала на finik1 |

# Информационная безопасность

## Ролевая модель

АС предполагает использование нескольких ролей. Их описание приведено в таблице.

|  |  |  |
| --- | --- | --- |
| **Роль** | **Описание роли** | **Функции** |
| Администратор АС | Осуществляет управление серверными приложениями: Configuration Server, Sync Cache Server, Sync Generator | * Запуск / Остановка сервисов * Изменение настроек конфигурации * Управление доступом к SyncGenerator |
| Оператор данных | Осуществляет управление генерацией файлов на SyncGenerator | * Ручной запуск заданий на генерацию файлов * Прерывание работающих заданий * Мониторинг работы заданий |
| Пользователь отчётов | Использование инструмента визуализации | * Просмотр отчётов |

В свою очередь, пользователи отчётов также разделяются на роли, приведённые в следующей таблице.

|  |  |  |
| --- | --- | --- |
| **Роль** | **Описание роли** | **Функции** |
| iNavigator | Способен просматривать все отчёты в приложении iNavigator | * Доступ к приложению iNavigator * Просмотр всех отчётов в приложении |
| Динамическая модель CIB | Способен просматривать все отчёты в приложении Динамическая модель CIB | * Доступ к приложению Динамическая модель CIB * Получение любых данных в рамках приложения |
| iRubricator | Способен просматривать все отчёты в приложении iRubricator | * Доступ к приложению iRubricator * Просмотр всех отчётов в приложении |
| ИУП - Региональный менеджер | Способен просматривать отчёты в приложении ИУП, относящиеся к своей роли | * Доступ к приложению ИУП * Просмотр отчётов в приложении, относящихся к своей роли |
| ИУП – Руководитель | Способен просматривать отчёты в приложении ИУП, относящиеся к своей роли | * Доступ к приложению ИУП * Просмотр отчётов в приложении, относящихся к своей роли |
| ППР/КПЭ | Способен просматривать все отчёты в приложении ППР/КПЭ | * Доступ к приложению ППР/КПЭ * Просмотр всех сведений в приложении |
| Баланс Сбербанка | Способен просматривать все отчёты в приложении Баланс Сбербанка | * Доступ к приложению Баланс Сбербанка * Просмотр всех отчётов в приложении |
| Сравнение с конкурентами | Способен просматривать все отчёты в приложении Сравнение с конкурентами | * Доступ к приложению Сравнение с конкурентами * Просмотр всех отчётов в приложении |

Управление ролями в приложении осуществляется с помощью стандартного функционала MIS Портала. Права доступа к отчетам мобильного приложения Рубрикатор могут быть настроены в специальном веб-приложении RubricatorAdmin. Идентификация пользователей в мобильной версии осуществляется по Email, хранящимся в персональном сертификате пользователя на мобильном устройстве.

## Защита информации

Меры по защите информации в АС учитывают специфику, которая подразумевает передачу чувствительных данных во внешнюю среду – Интернет, а затем хранение её на персональных мобильных устройствах.

### Аутентификация клиента и обмен данными

Процесс обмена данными производится по защищённому протоколу HTTPS/SSL с двухсторонним шифрованием. Процесс аутентификации клиента происходит следующим образом.

1. При открытии любого мобильного приложения АС, пользователю необходимо ввести ПИН-код. ПИН-код задаётся при первом запуске любого приложения, а затем используется совместно всеми приложениями. При неправильном вводе ПИН-кода 5 раз подряд, он блокируется, что влечёт невозможность открыть ни одно приложение.

Для разблокировки или сброса ПИН-кода необходимо обратиться в службу поддержки АС.

При компрометации ПИН-кода или при иной необходимости, если ПИН-код известен и не заблокирован, пользователь имеет возможность самостоятельно сменить ПИН-код через приложение iNavigator.

ПИН-код хранится в МУ в специальном защищённом контейнере – [KeyChain](https://developer.apple.com/library/ios/documentation/security/Conceptual/keychainServConcepts/02concepts/concepts.html#//apple_ref/doc/uid/TP30000897-CH204-TP9).

1. При подключении клиента к серверу Сбербанка, он получает идентификатор сессии в свойствах cookies.
2. Клиент получает серверный сертификат, подписанный международным доверенным УЦ.
3. Так как мобильное устройство хранит корневой сертификат этого УЦ, то приложение способно проверить, что полученный серверный сертификат принадлежит достоверному серверу Банка.
4. Используя открытый ключ, полученный с серверным сертификатом, клиент шифрует сообщение с полной уверенностью, что только сервер имеет возможность расшифровать его.
5. В ответ, клиент отправляет сертификат приложения, который соответствует сертификату почты в домене Sigma.
6. Сервер проверяет действительность клиентского сертификата в УЦ Банка.
7. Далее следуют процедуры авторизации, соответствующие конкретному приложению.

### Сертификаты, используемые при обмене данными

В процессах взаимодействия между клиентским устройством и сервером банка используются 2 типа сертификата:

* Серверный сертификат. Является сертификатом международного доверенного УЦ, что позволяет клиенту проверять его надёжность и собственного банка корневых сертификатов. Такой вид сертификата устанавливается на все сервера, с которыми взаимодействует пользователь: Configuration Server, Sync Cache Server.
* Клиентский сертификат. Является сертификатом УЦ Банка (на текущий момент, средство получения - <https://pki.sberbank.ru/pfx>). Данный сертификат используется одновременно всеми приложениями i-Navigator, а также стандартным почтовым клиентом МУ. Будучи установленным на МУ, сертификат позволяет аутентифицировать пользователя, а сама проверка осуществляется сервером через УЦ Банка.

### Авторизация пользователя

После успешной аутентификации пользователя, сервер отправляет запрос в БД источника сведения, полученные из клиентского сертификата, а также название мобильного приложения инициирующего получение данных. Администратором БД источника ведётся реестр пользователей и уровень доступа, который они имеют по каждому приложению. Уровень доступа зависит от логики приложения, и может быть реализован как на уровне приложения в целом, так и на уровне ролей внутри приложения.

В ответ на запрос сервера из БД может быть возвращено подтверждение или отказ в авторизации. В первом случае сервер приступает к передаче данных, а во втором – сообщает клиенту ошибку и обрывает соединение.

### Безопасность данных на мобильном устройстве

В соответствии с требованиями Управления Безопасности Информационной Инфраструктуры (УБИИ) все мобильные устройства, на которые передаются корпоративные данные, должны быть подключены к корпоративной системе управления мобильными устройствами (SAP Afaria) и соответствовать утвержденной политике безопасности (пункт 7.2.5).

Приложения на МУ спроектированы для работы на платформе iOS версии не ниже 7. Эта версия подразумевает принудительное аппаратное шифрование для всех данных приложения. Процесс шифрования лежит за пределами функций АС.

### Политики безопасности на мобильном устройстве

**Парольная политика мобильного устройства**

|  |  |
| --- | --- |
| Блокировка экрана устройства | + |
| Простой пароль | - |
| Сложный пароль | + |
| Минимальная длина пароля | 4 |
| Количество специальных символов | 0 |
| Срок действия пароля (дней) | 42 |
| Автоматическая блокировка (мин) | 3 |
| История паролей | 10 |
| Количество неправильных вводов пароля | 10 |

**Ограничения**

|  |  |
| --- | --- |
| Установка приложений | + |
| Разрешить камеру | + |
| Разрешить FaceTime | + |
| Разрешить скриншот | - |
| Автоматическая синхронизация в роуминге | + |
| Использование Siri | + |
| Использование Siri на заблокированном устройстве | + |
| Голосовой набор | + |
| Использование Passbook на заблокированном устройстве | + |
| Покупки в приложениях | + |
| Принудительный ввод пароля iTunes Store для всех покупок | + |
| Использование | + |
| Разрешить Game Center | + |
| Разрешить YouTube | + |
| Разрешить iTunes Store | + |
| Разрешить Safari | + |
| Авто заполнение | - |
| Разрешить JavaScript | + |
| Блокировать всплывающие окна | + |
| Принимать куки | - |

**iCloud**

|  |  |
| --- | --- |
| Разрешить резервное копирование | + |
| Разрешить синхронизацию документов | - |
| Разрешить фотопоток | + |
| Разрешить доступ к фотопотокам | + |

**Безопасность**

|  |  |
| --- | --- |
| Отправка диагностической информации | + |
| Разрешить установку недоверенных TLS сертификатов | + |
| Шифрование резервных копий | + |

**Content ratings**

|  |  |
| --- | --- |
| Разрешить music, podcasts и iTunes U | + |

### Категории информационной безопасности

|  |  |  |
| --- | --- | --- |
| **Приложение** | **Категория ИБ** | **Примеры используемой информации** |
| iNavigator | И-2 | Финансовые и нефинансовые показатели управленческой отчетности и оперативные прогнозы по показателям такие как общий баланс банка, общий объём кредитного портфеля, в том числе расчёт прогнозных показателей, доходы банка в разрезе продуктов, размеры операционных расходов и т.д. |
| iRubricator | И-2 | Еженедельная отчётность для Совета Директоров Сбербанка; квартальный пресс-релиз; ежемесячный мониторинг CIB и т.д. Кроме опубликованных документов, приложение в рамках интерактивных отчётов предоставляет сведения о клиентах (кредиты, облигации, текущие счета, комиссии, процентные ставки), о выполнение бизнес-планов (прогнозные и фактические показатели), KPI розничного блока и CIB. |
| Инструмент управления продажами | И-4 | Выполнение КПЭ продаж в разрезе продуктов и территориальных банков/подразделений, а также отображает географическое местоположение доп-офисов на карте. |
| Динамическая модель CIB | И-2 | Наименование клиента, ИНН, активы, пассивы, доход, расход, ставки привлечения и размещения, нормы резервирования и т.д. Полученные данные не сохраняются в мобильном устройстве. |
| Выполнение ППР/КПЭ руководителей | И-2 | Показатели ППР/КПЭ руководителей-членов Правления Банка. |
| Отчёт по балансу Сбербанка | И-4 | Публичные сведения, касающиеся финансового состояния банка и дочерних банков: баланс и сведения о доходах и расходах. |
| Сравнение с конкурентами | И-4 | Публичные данные по балансу Банка и сведения о доходах и расходах в сравнении с публичными данными конкурентов. |

# Модель работы с данными в мобильных приложениях

|  |  |
| --- | --- |
| **Приложение** | **Режим работы** |
| iNavigator | Офлайн |
| iRubricator – статические отчёты | Файлы – офлайн  Каталог отчётов – онлайн |
| iRubricator – интерактивные отчёты | Офлайн |
| Инструмент управления продажами | Онлайн |
| Динамическая модель CIB | Онлайн |
| Выполнение ППР/КПЭ руководителей | Офлайн |
| Отчёт по балансу Сбербанка | Офлайн |
| Сравнение с конкурентами | Офлайн |

# Процедуры подготовки данных для выгрузки в БД SQLite

|  |  |  |  |
| --- | --- | --- | --- |
| **Отчет** | **Процедура подготовки данных** | **Таблица** | **Назначение таблицы** |
| KPI CIB | p\_mobile\_upd\_CIB\_KPI | t\_900\_CIB\_KPI\_DefaultParams | Значения параметров по умолчанию |
| t\_900\_CIB\_KPI\_AllData\_Table | Значения для отчета |
| Прибыль CIB | p\_mobile\_upd\_CIB\_MARGIN | t\_900\_CIB\_MARGIN\_blocksData | Значения по Корп. блоку |
| t\_900\_CIB\_MARGIN\_blocksData\_plan | Плановые значения по Корп. блоку |
| t\_900\_CIB\_MARGIN\_CIBData | Значения по CIB |
| t\_900\_CIB\_MARGIN\_CIBData\_plan | Плановые значения по CIB |
| t\_900\_CIB\_MARGIN\_cib\_products | Справочник продуктов |
| t\_900\_CIB\_MARGIN\_Default\_Params | Значения параметров по умолчанию |
| Отчет «Статистика по устройствам самообслуживания» | p\_mobile\_upd\_retail\_atm | "t 000 020 hier\_bank" | Справочник ТБ |
| "t 000 030 ATM type\_heirarchy" | Справочник |
| "t 000 040 Transaction type\_heirarchy" | Справочник транзакций |
| "t 002 005 norm" | Значения для таблицы |
| "t 002 007 norm" | Значения для таблицы |
| Отчет «Кредитные продукты» | p\_mobile\_upd\_retail\_cred | "stat\_ch\_hier" | Иерархия по каналам продаж |
| "stat\_client\_hier" | Иерархия по клиентам |
| "stat\_prod\_hier" | Иерархия по продуктам |
| "t 000 020 CredType" | Справочник типов кредитов |
| "t 000 100 depart hierarchy" | Справочник подразделений |
| "t 100 010 Requests Pvt" | Таблица с данными |
| Отчет «Кредитные продукты. Кредитный портфель» | p\_mobile\_upd\_retail\_cred\_bag | "t 000 020 CredType" | Справочник типов кредитов |
| "t 000 090 IndType" | Справочник показателей |
| "t 000 100 depart hierarchy" | Справочник подразделений |
| "t 200 010 Volume Sums Pvt" | Данные по кредитному портфелю |
| CIB IBGM | p\_mobile\_upd\_CIB\_IBGM | t\_900\_CIB\_IBGM\_default\_params | Значения параметров по умолчанию |
| t\_900\_CIB\_IBGM | Таблица с данными |
| CIB KPKI | p\_mobile\_upd\_CIB\_KPKI | t\_900\_CIB\_KPKI\_AllData\_TableCredit\_contract | Значения для экрана "Кредиты клиента"-данные с выводом договора |
| t\_900\_CIB\_KPKI\_AllData\_TableCredit\_NoContract | Значения для экрана "Кредиты клиента"-данные без вывода договоров |
| t\_900\_CIB\_KPKI\_AllData\_TableProduct | Значения для экрана "Все продукты клиента" |
| t\_900\_CIB\_KPKI\_Contract | Справочник контрактов |
| t\_900\_CIB\_KPKI\_DefaultParams | Значения параметров по умолчанию |
| t\_900\_CIB\_KPKI\_Mapping\_GroupClient | Таблица вхождения юридического лица в конкретный тип клиента |
| Активы CIB | p\_mobile\_upd\_CIB\_Actives | t\_900\_CIB\_Actives\_Dynamics\_CIB | Данные по активам СIB для экрана "Динами активов" |
| t\_900\_CIB\_Actives\_Dynamics\_Corp | Данные по активам Корп. блоку для экрана "Динами активов" |
| t\_900\_CIB\_Actives\_Slice\_CIB | Данные по активам CIB в разрезах ТБ/кредитующих/клиентских подразделений |
| t\_900\_CIB\_Actives\_Slice\_Corp | Данные по активам Корп. блоку в разрезах ТБ/кредитующих/клиентских подразделений |
| t\_900\_CIB\_Actives\_Term\_Currency | Данные по активам в разрезе сроков и валют |
| t\_900\_CIB\_Actives\_Term\_Currency\_Terr | Данные по активам в разрезе сроков/валют/ТБ |
| t\_900\_CIB\_Actives\_Concentration | Данные по концентрации активов в разрезе клиентов |
| t\_900\_CIB\_Actives\_Concentration\_Total | Данные по концентрации активов |
| t\_900\_CIB\_Actives\_Quality | Данные по качеству активов |
| Пассивы CIB | p\_mobile\_upd\_CIB\_Passives | t\_900\_CIB\_Passives\_Concentration\_Client | Данные по концентрации пассивов СIB в разрезе клиентов |
| t\_900\_CIB\_Passives\_Concentration\_Client\_Bank | Данные по концентрации пассивов СIB в разрезе клиентов/банков |
| t\_900\_CIB\_Passives\_Concentration\_Total | Данные по концентрации пассивов СIB |
| t\_900\_CIB\_Passives\_Dynamics\_CIB | Данные по пассивам CIB для экрана Динамика |
| t\_900\_CIB\_Passives\_Dynamics\_Corp | Данные по пассивам Корп. блока для экрана Динамика |
| t\_900\_CIB\_Passives\_Slice\_CIB | Данные по пассивам СIB в разрезе ТБ/клиентских подразделений |
| t\_900\_CIB\_Passives\_Slice\_Corp | Данные по пассивам Корп. Блока ТБ/клиентских подразделений |
| t\_900\_CIB\_Passives\_Term\_Curr\_Terr | Данные по пассивам в разрезах сроков и валют |
| Доходность CIB. Пассивы | p\_mobile\_upd\_cib\_profit\_passive | t\_900\_CIB\_Profit\_Passive\_Clients | Данные по подразделениям и клиентам |
| t\_900\_CIB\_Profit\_Passive\_Contracts | Данные по контрактам |
| t\_900\_CIB\_Profit\_Passive\_Default\_Params | Значения по умолчанию |
| Доходность CIB. Продукты | p\_mobile\_upd\_cib\_profit\_products\_comm | t\_900\_cib\_products\_commissions | Значения для экрана "Комиссионные продукты" |
|  | t\_900\_CIB\_Profit\_Products\_Default\_Params | Значения параметров по умолчанию |
| p\_mobile\_upd\_cib\_profit\_products\_IB | t\_900\_cib\_product\_ib | Значения для экрана "Продукты IB" |
| p\_mobile\_upd\_cib\_profit\_products\_GM | t\_900\_cib\_product\_gm | Значения для экрана "Продукты GM" |
| p\_mobile\_upd\_cib\_profit\_products\_MB | t\_900\_cib\_product\_mb | Значения для экрана "Продукты MB" |
| Доходность CIB. Итого | p\_mobile\_upd\_CIB\_PROFIT\_TOTAL | t\_900\_CIB\_Profit\_Total | Значения для экрана "Итого" |
| t\_900\_CIB\_Profit\_Total\_Default\_Params | Значения по умолчанию |
| Доходность CIB. Концентрация | p\_mobile\_upd\_CIB\_PROFIT\_CONCENTRATION | t\_900\_CIB\_PROFIT\_CONCENTRATION\_sums | Данные просуммированные по категориям (TOP, BOTTOM) |
| t\_900\_CIB\_PROFIT\_CONCENTRATION\_Default\_Params | Значения параметров по умолчанию |
| Доходность CIB. Активы | p\_mobile\_upd\_CIB\_PROFIT\_ACTIVE | t\_900\_CIB\_PROFIT\_ACTIVE\_all\_contracts | Справочник договоров |
| t\_900\_CIB\_PROFIT\_ACTIVE\_cl\_bagg | Агрегированные данные по кредитам |
| t\_900\_CIB\_PROFIT\_ACTIVE\_clients\_mapping | Таблица маппинга клиентов |
| t\_900\_CIB\_PROFIT\_ACTIVE\_contracts | Данные по кредитным договорам |
| t\_900\_CIB\_PROFIT\_ACTIVE\_sec\_cl | Агрегированные данные по облигациям |
| t\_900\_CIB\_PROFIT\_ACTIVE\_sec\_contracts | Данные по контрактам с облигациями |
| t\_900\_CIB\_PROFIT\_ACTIVE\_Default\_Params | Значения параметров по умолчанию |

# Источники сведений о времени последней модификации данных в БД MIS Портала

|  |  |
| --- | --- |
| **Отчёт** | **Объект БД** |
| iNavigator | MIS\_NAVIGATOR\_DATA. GetLastLoaddate (3)  MIS\_NAVIGATOR\_DATA. GetLastLoaddate (4) |
| Инструмент управления продажами | MIS\_IUP\_KPI.dbo.default\_params (‘last\_load’) |
| Отчёт по балансу Сбербанка | Подотчёт «Баланс»:  MIS\_PL\_GROUP\_SB.f\_GetActualReportDate ( 102 ,0 ,'w')  Подотчёт «ОПУ»:  MIS\_PL\_GROUP\_SB.f\_GetActualReportDate ( 101 ,0 ,'m') |
| Сравнение с конкурентами | MIS\_COMPETITORS\_NT.f\_GetActualReportDate ('100','1','M') |
| Отчеты CIB | [MIS\_MOBILE].[dbo].f\_mobile\_upd\_cib\_lastupdate() |

# Способ формирования файлов на Sync Generator

|  |  |
| --- | --- |
| **Мобильное приложение** | **Метод формирования файлов** |
| iRubricator (Каталог отчетов) | Вручную |
| iNavigator (мобильная версия АС Навигатор) | Вручную |
| ИУП (Инструмент управления продаж) | Автоматически + Вручную |
| Динамическая модель CIB | Используется прямой on-line доступ к витрине MIS-портала |
| КПЭ/ППР руководителей | Вручную |
| Баланс Сбербанка | Автоматически + Вручную |
| Конкуренты | Автоматически + Вручную |
| Отчеты РБ на фреймворке:   * P&L Розничного блока, кредитные продукты * Эффективность АТМ | Автоматически + Вручную |
| * P&L Розничного блока, ВСП | Используется прямой on-line доступ к витрине MIS-портала |
| Отчеты CIB на фреймворке:   * Доходность крупнейших клиентов CIB * Отчет на КПКИ * Выполнение бизнес-плана IBGM&MB * KPI CIB * Прибыль CIB * Оперативная отчетность CIB * Обязательства CIB | Автоматически + Вручную |

# Перечень файлов, используемых в мобильных отчётах

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Приложение / Отчёт** | **SQLite-файл** | **ETL файл** | **База - источник** | **Примерный размер файла, Мб** |
| iNavigator | MIS\_NAVIGATOR\_KPI.sqlite  MIS\_NAVIGATOR\_KPI\_W.sqlite | etl-devkpi.xml | mis\_navigator\_kpi | 1500 |
| Инструмент управления продажами | MIS\_IUP\_KPI.sqlite | etl-iup.xml | mis\_iup\_kpi | 168 |
| Сравнение с конкурентами | COMPETITORS.sqlite | etl-competitors.xml | mis\_competitors | 7 |
| Отчёт по балансу Сбербанка | BALANCE.sqlite | etl-balance.xml | mis\_balance | 200 |
| Выполнение ППР/КПЭ руководителей | DASHBOARD\_PPR\_MOBILE.sqlite | etl-dashboard-ppr-mobile.xml | dashboard\_ppr\_mobile | 20 |
| MIS Mobile / KPI CIB | CIB\_KPI.sqlite | etl-cib-and-retail.xml | mis\_balance | 4 |
| MIS Mobile / Прибыль CIB | CIB\_MARGIN.sqlite | etl-cib-and-retail.xml | mis\_balance | 12 |
| MIS Mobile / Отчёты PL Розничного блока, ATM | RETAIL\_ATM.sqlite | etl-cib-and-retail.xml | mis\_balance | 648 |
| MIS Mobile / Отчёты PL Розничного блока, кредитные продукты | RETAIL\_CRED.sqlite | etl-cib-and-retail.xml | mis\_balance | 1600 |
| MIS Mobile / Отчёты PL Розничного блока, кредитные продукты | RETAIL\_CRED\_BAG.sqlite | etl-cib-and-retail.xml | mis\_balance | 1800 |
| MIS Mobile / Активы CIB | CIB\_ASSETS.sqlite | etl-cib-and-retail.xml | mis\_balance | 50 |
| MIS Mobile / Пассивы (обязательства) CIB | CIB\_LIABILITIES.sqlite | etl-cib-and-retail.xml | mis\_balance | 140 |
| MIS Mobile / Выполнение бизнес-плана IBGM&MB | CIB\_IBGM.sqlite | etl-cib-and-retail.xml | mis\_balance | 4 |
| MIS Mobile / Отчёт на КПКИ CIB | CIB\_KPKI.sqlite | etl-cib-and-retail.xml | mis\_balance | 1236 |
| MIS Mobile / Доходность крупнейших клиентов CIB | CIB\_PROFIT\_ACTIVE.sqlite | etl-cib-and-retail.xml | mis\_balance | 720 |
| CIB\_PROFIT\_PASSIVE.sqlite | 360 |
| CIB\_PROFIT\_PRODUCT.sqlite | 110 |
| CIB\_PROFIT\_CONCENTRATION.sqlite | 560 |
| CIB\_PROFIT\_TOTAL.sqlite | 50 |