

# Техническое задание на ИТ-решение

## Наименование проекта

Внедрение системы управления мобильными устройствами (Enterprise Mobility Management)

Наименование Бизнес-решения	Наименование Бизнес-системы
Система управления мобильными устройствами SafePhone EMM	SafePhone iOS клиент
	SafePhone APM администратора
	SafePhone сервер управления
	ГИС (OpenStreetMap)

## Общие сведения о проекте

Тип проекта	Сложный
Ценность проекта	Важный
Наименование проекта	Внедрение системы управления мобильными устройствами (Mobile Device Management) и защищенной электронной почты
Наименование программы	12-ДИТАТ/П.7. Управление ИТ. Создание эффективной организации направления ИТАТ "Газпром нефть" в соответствии с задачами ИТ стратегии и Бизнес-стратегии Компании
Наименование портфеля	12-ДИТАТ
Заказчик проекта	Кравченко К.Ю., Начальник ДИТАТ
Единое ответственное лицо	Антонов М.А., Начальник УКИТА
Руководитель проекта	Эрих И.С., Руководитель проектов
Архитектор ИТ-решения	Романов Д.В., Начальник отдела



## Содержание

1. Цели и задачи проекта .....	3
2. Назначение и цели создания Системы.....	3
2.1 Назначение системы .....	3
2.2 Цели создания Системы .....	4
3. Функционально-компонентная архитектура .....	5

## 1. Цели и задачи проекта

Основной целью данного проекта является построение системы централизованного управления МУ на основе решения SafePhone с обеспечением необходимого уровня защищенности.

Таблица 1. Цели и задачи проекта

№	Цель проекта	Задача проекта
1.	Обеспечение централизованного управления МУ (EMM) сотрудников Компании, используемых для доступа к корпоративной информации	Внедрение системы централизованного управления МУ сотрудников Компании
2.	Регламентирование процессов, обеспечивающих безопасное использование мобильных устройств для доступа к корпоративной информации.	Разработка или актуализация нормативно-методической документации Заказчика, регламентирующей процессы безопасного использования мобильных устройств для доступа к корпоративной информации

## 2. Назначение и цели создания Системы

### 2.1 Назначение системы

Назначение Системы – централизованное управление мобильными устройствами сотрудников Компании.

## 2.2 Цели создания Системы

Таблица 2. Цели создания Системы

№	Цель	Наименование КПЭ	Значение КПЭ	Критерий достижения цели
1.	Обеспечение централизованного управления мобильными устройствами (EMM) сотрудников Компании, используемых для доступа к корпоративной информации	Организация централизованного управления мобильными устройствами сотрудников Компании	Централизованное управление мобильными устройствами сотрудников Компании	Осуществление централизованного управления мобильными устройствами сотрудников Компании
2.	Регламентирование процессов, обеспечивающих безопасное использование мобильных устройств для доступа к корпоративной информации	Пакет документации на систему	Пакет документации на систему	Пакет документации на систему

### 3. Функционально-компонентная архитектура

Для обеспечения требуемой функциональности Система SafePhone EMM должна быть построена на базе ПО SafePhone и использовать следующие компоненты:

- SafePhone iOS клиент;
- SafePhone сервер управления;
- SafePhone APM Администратора;

В качестве дополнительного ПО используется ГИС (OpenStreetMap).

SafePhone iOS клиент должен обеспечивать интерфейс взаимодействия с сервером управления в части контроля исполнения профиля безопасности устройств (приём и передача управляющих сигналов между устройством и сервером управления, контроль установки и удаления приложений, определение местоположения, регистрация событий, статуса и др.).

SafePhone сервер управления должен обеспечивать централизованное управление мобильными устройствами пользователей путем управления потоками команд, осуществления сбора и обработки информации с мобильных устройств. Сервер управления SafePhone должен обеспечивать постоянный контроль состояния мобильных устройств.

SafePhone APM Администратора должен обеспечивать возможность своевременного получения данных Администраторами Системы и осуществления ими действий над мобильными устройствами и другими объектами Системы. APM Администратора должен иметь графический интерфейс.

ГИС (OpenStreetMap) должна использоваться в качестве средства визуализации географической информации, используемой для мониторинга местоположения МУ.

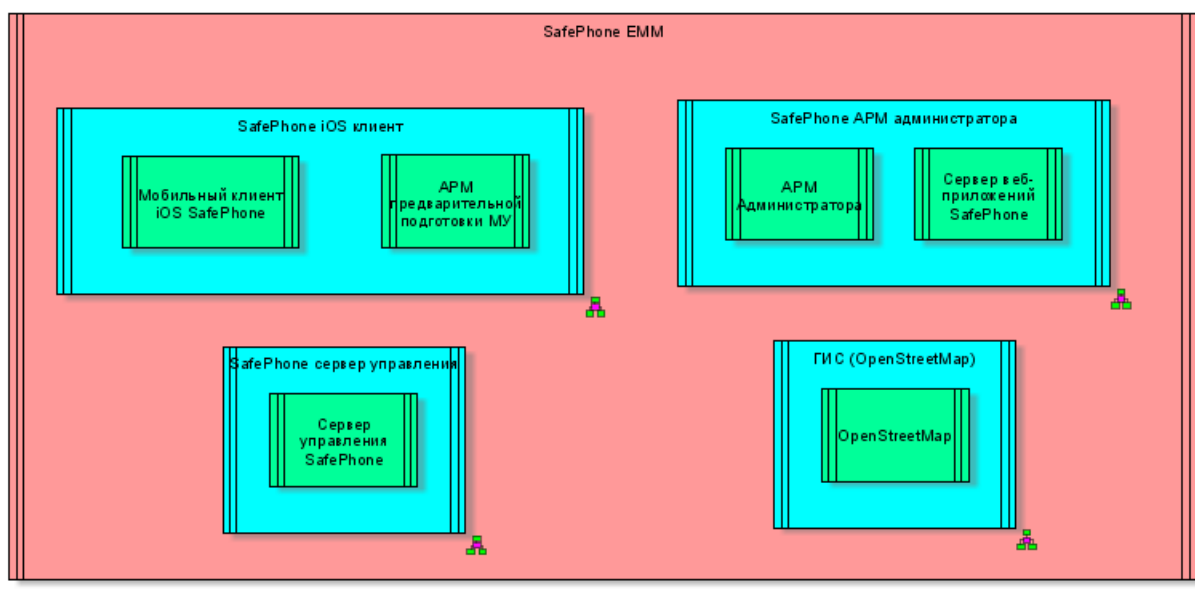


Рисунок 1. Диаграмма бизнес-решения

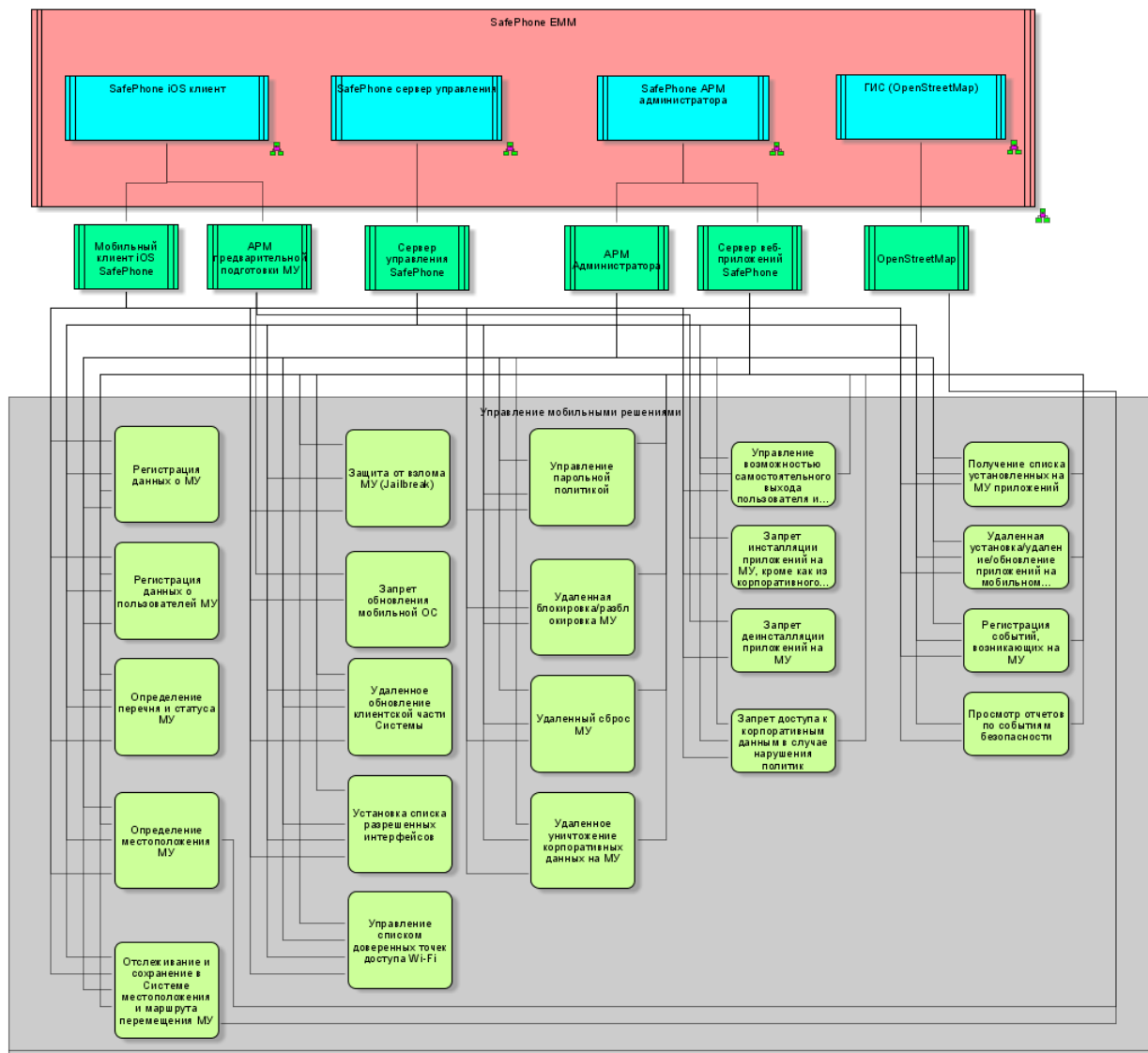


Рисунок 2. Функциональная модель бизнес-решения

Таблица 3. Функциональные требования к Системе SafePhone EMM

Функция	Требования к реализации	Реализующие бизнес-системы
<b>Учёт МУ</b>		
Регистрация данных о МУ	При регистрации устройства в Системе должны сохраняться следующие данные: <ul style="list-style-type: none"> <li>• марка и модель устройства;</li> <li>• аппаратный идентификатор устройства (UDID);</li> <li>• идентификатор модуля GSM (IMEI);</li> <li>• версия операционной системы, установленной на устройстве;</li> <li>• идентификатор SIM (ICCID).</li> </ul>	Мобильный клиент Сервер управления АРМ Администратора
Регистрация данных о пользователе МУ	При регистрации устройства в Системе должны сохраняться данные о ФИО пользователя МУ и месте его работы	Мобильный клиент Сервер управления АРМ Администратора
<b>Инвентаризация и отслеживание статуса МУ</b>		
Определение перечня и статуса МУ	Вывод информации о перечне зарегистрированных в Системе устройств, с указанием регистрационных данных (о МУ и пользователе), статуса активности и уровня заряда батареи	Мобильный клиент Сервер управления АРМ Администратора
Определение местоположения МУ	Определение и отслеживание текущих пространственных GPS-координат МУ, с отображением на географической карте, а также с возможностью вывода координат в отчёты по устройствам	Мобильный клиент Сервер управления АРМ Администратора Сервер ГИС
Отслеживание и сохранение в Системе местоположения и маршрута перемещения МУ	Функция необходима для поиска устройства при его утере или краже. Функция должна сохранять данные о перемещении только в периоды официально установленного рабочего времени. Данные о перемещениях во внерабочее время могут сохраняться только в особых случаях по требованию ДКЗ	Мобильный клиент Сервер управления АРМ Администратора Сервер ГИС



Функция	Требования к реализации	Реализующие бизнес-системы
<b>Управление безопасностью устройства и данных</b>		
Защита от взлома МУ (Jailbreak)	Система должна обеспечивать возможность автоматической блокировки доступа к корпоративным данным при обнаружении попыток взлома (Jailbreak) МУ	Мобильный клиент Сервер управления АРМ Администратора
Удаленное обновление клиентской части Системы (по команде Специалиста по управлению МУ)	Должна быть предусмотрена возможность удаленного обновления клиентской части Системы	Мобильный клиент Сервер управления АРМ Администратора
Установка списка разрешенных интерфейсов	Применение на МУ политики предоставления доступа и закрытия интерфейсов обмена данными по команде администраторов Системы	Мобильный клиент Сервер управления АРМ Администратора
Управление списком доверенных точек доступа Wi-Fi	Применение на МУ политики управления списком доверенных точек доступа Wi-Fi по команде администраторов Системы	Мобильный клиент Сервер управления АРМ Администратора
Управление парольной политикой	Должна быть предусмотрена возможность управления парольной политикой	Мобильный клиент Сервер управления АРМ Администратора
Удалённая блокировка / разблокировка МУ	Должна быть предусмотрена возможность удаленной блокировки / разблокировки МУ	Мобильный клиент Сервер управления АРМ Администратора
Удалённый сброс	Должна быть предусмотрена возможность удаленного сброса информации и всех настроек на МУ (удаленное форматирование МУ)	Мобильный клиент Сервер управления АРМ Администратора
Удаленное уничтожение корпоративных данных на МУ (по команде Специалиста по управлению МУ)	Функция должна использоваться в случае утери или кражи МУ, при наличии риска несанкционированного использования устройства посторонними лицами	Мобильный клиент Сервер управления АРМ Администратора
<b>Управление уровнем полномочий пользователя МУ</b>		

Функция	Требования к реализации	Реализующие бизнес-системы
Управление возможностью самостоятельного выхода пользователя из-под управления Системы	При выходе пользователя из-под управления Системы с его МУ должны быть удалены все установленные корпоративные приложения и настройки	Мобильный клиент Сервер управления АРМ Администратора
Запрет доступа к корпоративным данным в случае нарушения политик	В случае выявления случаев нарушения политик безопасности, в зависимости от их критичности, Система должна позволять закрыть доступ пользователю к использованию корпоративных данных с МУ	Мобильный клиент Сервер управления АРМ Администратора
<b>Управление приложениями на МУ</b>		
Получение списка установленных на МУ приложений	Специалист по управлению МУ должен иметь возможность просмотреть список установленных на МУ приложений	Мобильный клиент Сервер управления АРМ Администратора
Удалённая установка / удаление / обновление приложений на мобильном устройстве по команде Специалиста по управлению МУ	Специалист по управлению МУ должен иметь возможность удалённой установки / удаления / обновления одного или нескольких приложений на одном или многих МУ	Мобильный клиент Сервер управления АРМ Администратора
		Мобильный клиент Сервер управления АРМ Администратора
<b>Регистрация событий безопасности и иных событий, возникающих на МУ</b>		
Регистрация событий, возникающих на МУ	<p>Должна быть реализована возможность регистрации событий, возникающих на МУ:</p> <ul style="list-style-type: none"> <li>• смена SIM карты;</li> <li>• установка / обновление / удаление приложений;</li> <li>• изменение уровня заряда батареи;</li> <li>• взлом устройства (Jailbreak).</li> </ul>	Мобильный клиент Сервер управления АРМ Администратора

Функция	Требования к реализации	Реализующие бизнес-системы
Просмотр отчётов по событиям безопасности	Администраторы Системы должны иметь возможность просмотреть в Системе отчёты о событиях безопасности за выбранный период	АРМ Администратора

### 2.2.1.3 Пользователи и бизнес-роли

Таблица 6. Группы пользователей

№	Группа пользователей	Основной функционал группы
1.	Администратор платформы	Настройка параметров функционирования гостевых операционных систем
		Мониторинг работоспособности Системы
		Настройка и поддержание в рабочем состоянии виртуальной инфраструктуры гипервизора
		Настройка СУБД
		Контроль резервного копирования и восстановления
2.	Администратор Системы	Первичная регистрация мобильных устройств
		Регистрация в Системе организационно-штатной структуры
		Настройка сбора и регистрации событий МУ
		Настройка параметров функционирования Системы
		Настройка профилей мобильных устройств
		Управление корпоративными приложениями
		Аудит событий Системы
3.	Администратор ИБ	Аудит событий безопасности Системы
4.	Пользователь МУ	Использование мобильных устройств и установленных на них приложений

