Приложение № 1
к Закупочной документации по проведению
открытого запроса предложений в электронной форме на право заключения договора на
выполнение работ по модернизации опытного
образца комплекса программных средств «О7.УМНЫЙ ДОМ»

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

ВЫПОЛНЕНИЕ РАБОТ ПО МОДЕРНИЗАЦИИ ОПЫТНОГО ОБРАЗЦА КОМПЛЕКСА ПРОГРАММНЫХ СРЕДСТВ «О7.УМНЫЙ ДОМ»

2016г.

Содержание

Терминология

В настоящем документе используются следующие определения и сокращения:

Сокращение/Термин	Наименование/Определение
АСР	Автоматизированная система расчетов, программно-технический комплекс, предназначенный для тарификации услуг
ЕИП	Единая интеграционная платформа
ЕЛК	Единый личный кабинет - система, обеспечивающая Абонентам интерфейс для удаленного управления различными услугами ПАО «Ростелеком»: контролировать состояние лицевого счёта, получать информацию о выставленных счетах и оплаченных услугах, производить оплату различными способами и одним платежом за все услуги, добавлять и удалять услуги;
Интерфейс Продукта	WEB-ресурс для управления услугой «Умный дом». Выполняет функции регистрации контроллера, настройки сценариев пользования и уведомлений, подключения новых датчиков и т.д. Доступен из Интернет после авторизации
Клиент	Объект в АСР, атрибутом которого являются лицевой счет. К одному Клиенту могут относиться несколько Абонентов;
Контроллер	Часть абонентского оборудования Услуги, которая осуществляет сбор информации с подключенных абонентом датчиков и взаимодействие с КПС
КПС	Комплекс программных средств «Умный дом» и ОП
ЛС	Лицевой счет
НОП или ОП	Национальная облачная платформа ПАО «Ростелеком»
Продукт	Продукт с рабочим названием «Умный дом»
Режим	Под режимом понимается определенный набор выполняемых сценариев. Если котроллер находится в каком-либо из режимов, то при наступлении определенных условий будут отрабатываться только те сценарии, которые были ассоциированы с выбранным режимом.
Сервис	Программа, принимающая сообщения от приставок по определенному протоколу взаимодействия. Во время работы сервис может находиться в режиме ожидания сообщений от управляющего контроллера или в режиме обмена сообщениями.
Событие	Сообщение от управляющего контроллера о произошедших действиях, таких как: добавление устройства, удаление устройства, изменение состояния устройства, различные типы уведомлений, посылаемые устройствами от управляющего контроллера, выполнение сценариев и т. д.
ССПД	Система сбора и предобработки данных (Система Предбиллинга), эксплуатируемая в Корпоративном центре РТК, осуществляющая прием и обработку исходных тарификационных данных, собранных с Облачной платформы РТК

Сокращение/Термин	Наименование/Определение
Сценарий	Функциональность, позволяющая создавать задачи, которые будут выполнены при наступлении определённых условий. Сценарий содержит следующие общие компоненты: • метаданные - содержат следующее описание сценария: имя сценария, признак «включен» или «отключен», определяемые пользователем, а также уникальный идентификатор и признак корректности сценария, определяемые автоматически; • условия - одно или несколько простых или сложных (состоящих из нескольких условий, объединенных при помощи логических операций И, ИЛИ) условий, при наступлении которых выполняется сценарий; • действия - совокупность действий, которые выполняются при выполнении заданного сценария. Системой предусмотрены два типа действий: обновление статуса устройства либо оповещение пользователя.
ТПО	Точка продаж и обслуживания клиентов РТК
Услуга	Услуга «Умный дом»

1 Общие сведения

1.1 Основание для выполнения работ

Программа инновационного развития ПАО «Ростелеком».

1.2 Заказчик работ

Заказчик: ПАО «Ростелеком».

1.3 Сведения об источниках и порядке финансирования

Источник финансирования определяется Заказчиком.

1.4 Цель выполнения работ

Работы по настоящему Договору выполняются с целью пилотного запуска услуги «Умный дом» в двух макрорегиональных филиалах ПАО «Ростелеком» - МРФ «Северо-Запад» и МРФ «Волга».

Для внедрения комплекса программных средств «Умный дом» необходимо выполнить доработку НОП и опытного образца КПС, провести развертывание КПС в НОП и осуществить интеграцию КПС с информационными системами ПАО «Ростелеком» для обеспечения коммерческой эксплуатации.

1.5 Состав работ

По настоящему Договору Исполнитель выполняет перечисленные ниже работы:

1) Разработка промышленного образца КПС;
2) Доработка НОП;
3) Развертывание КПС;
4) Разработка дизайна мобильных приложений;
5) Разработка технического задания на разработку мобильных приложений.

1.6 Сроки выполнения работ

В таблице 1 представлены этапы выполнения работ по Договору.

Таблица 1 - Этапы выполнения работ

№ этапа	Наименование этапа	Срок сдачи работ	Результат работ
1	Разработка промышленного образца комплекса программных средств «Умный дом»	Не более 60 дней, точный срок определяются при проведении закупочной процедуры	– Техническое задание на разработку мобильных приложений; – Описание API Контроллера; – Промышленный комплекс программных средств «Умный Дом» – Комплект документов технического проекта – Комплект документов эксплуатационной документации – Программа и методика испытаний – Протокол проведения предварительных испытаний – Исходные коды комплекса программных средств «Умный дом» – Исходные коды НОП
2	Проведение опытной эксплуатации комплекса программных средств «Умный Дом»	В течении всего срока опытной эксплуатации, но не более 4 месяцев. Точный срок определяются при заключении договора.	– Отчет о проведении опытной эксплуатации – Протокол проведения приемо-сдаточных испытаний

1.7 Место выполнения работ

Работы выполняются на территории Российской федерации.

2 Назначение комплекса программных средств «Умный дом»

Комплекс программных средств «Умный дом» должен представлять собой единый ресурс для управления автоматизированной системой жилища и процессами жизнеобеспечения. На базе комплекса ПАО «Ростелеком» будет предоставлять услугу «Умный дом». Пользователь услуги должен иметь доступ к информации об устройствах, установленных в жилище, возможность просмотра уведомлений от этих устройств и управления ими в режиме реального времени посредством веб-интерфейса и в приложениях для мобильных устройств.

3 Описание услуги «Умный дом»

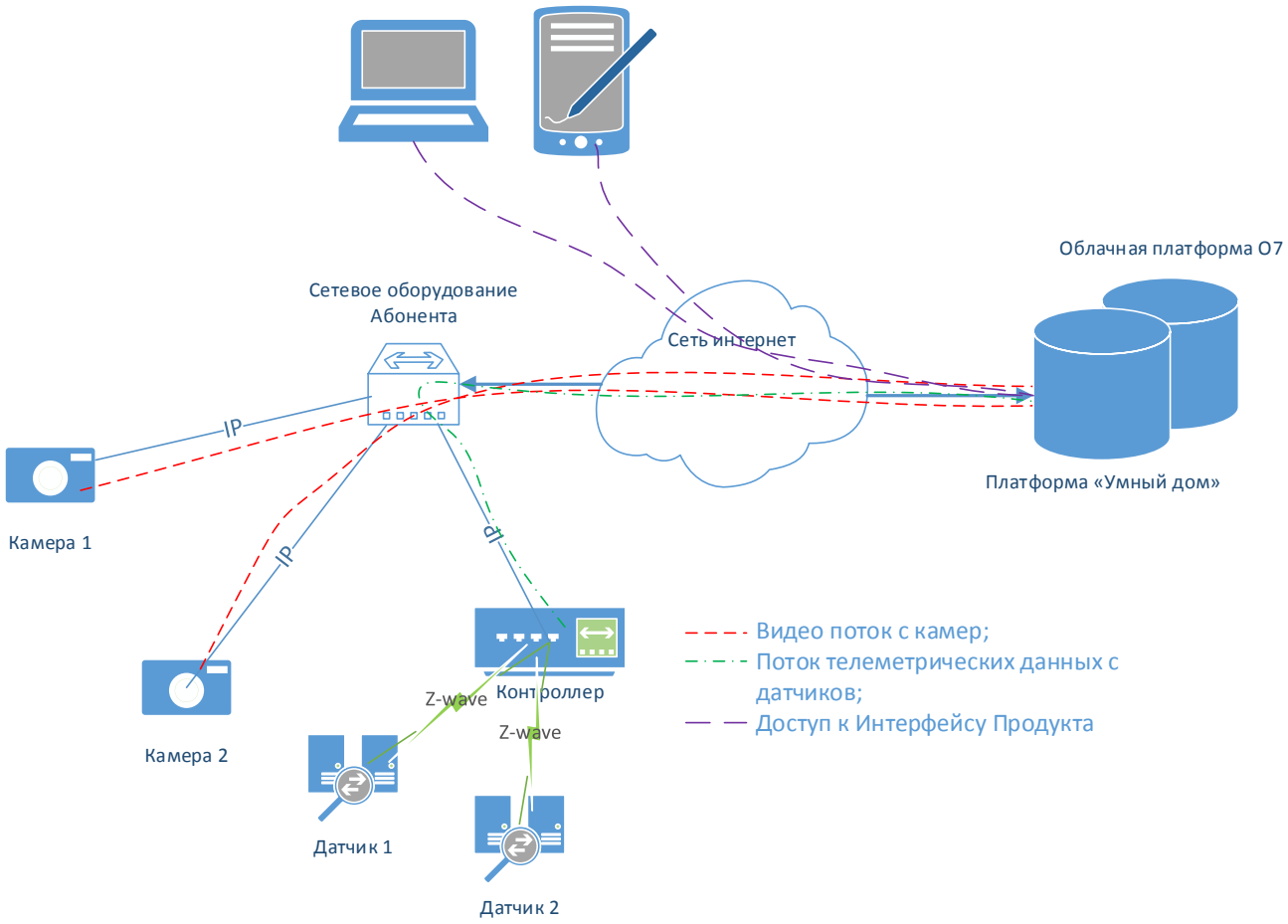
3.1 Схема предоставления услуги «Умный дом»

В помещении Абонента устанавливается Контроллер с набором беспроводных датчиков. Датчики подключаются к Контроллеру по протоколу Z-wave. Количество и тип датчиков может меняться. Контроллер получает показания с подключенных к нему датчиков и передаёт их КПС для обработки хранения и отображения Абоненту Услуги.

Подключенные Абонентом камеры регистрируются в КПС и транслируют видео поток.

Абонент с использованием web-браузера подключается к КПС и может пользоваться Услугой. Пользование Услугой также возможно с использованием мобильного приложения под платформы iOS или Android.

Рисунок 1. Типовая схема оказания услуги «Умный дом».



3.2 Архитектура КПС

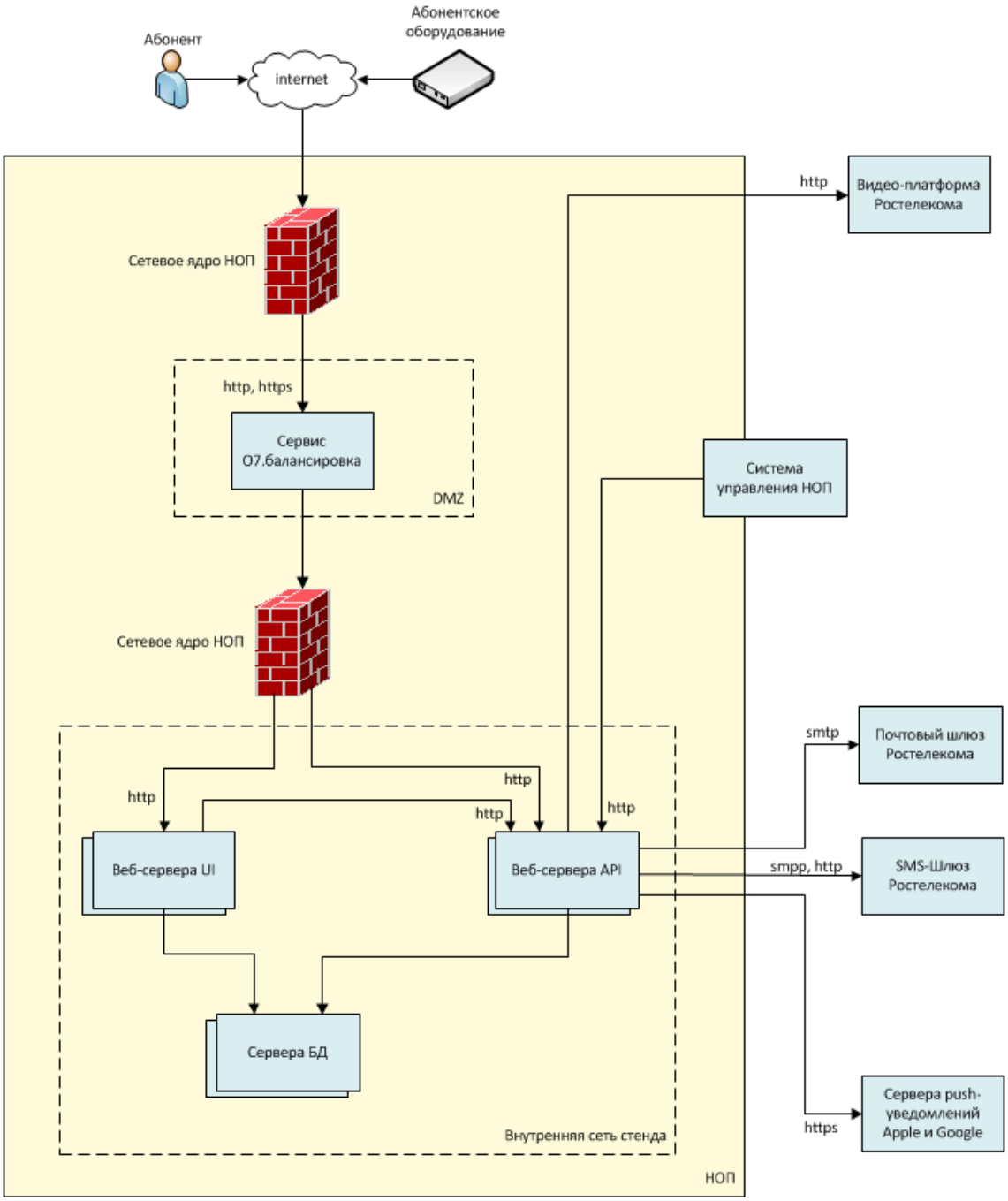
Архитектура КПС должна разрабатываться с учетом размещения компонентов КПС в облачной платформе Ростелеком. Общедоступные сервисы должны быть размещены в отдельном сегменте сети.

Пользовательские интерфейсы и базы данных должны быть размещены на отдельных серверах.

Все компоненты КПС должны горизонтально масштабироваться. Масштабирование каждой компоненты КПС должно выполняться независимо от других компонент.

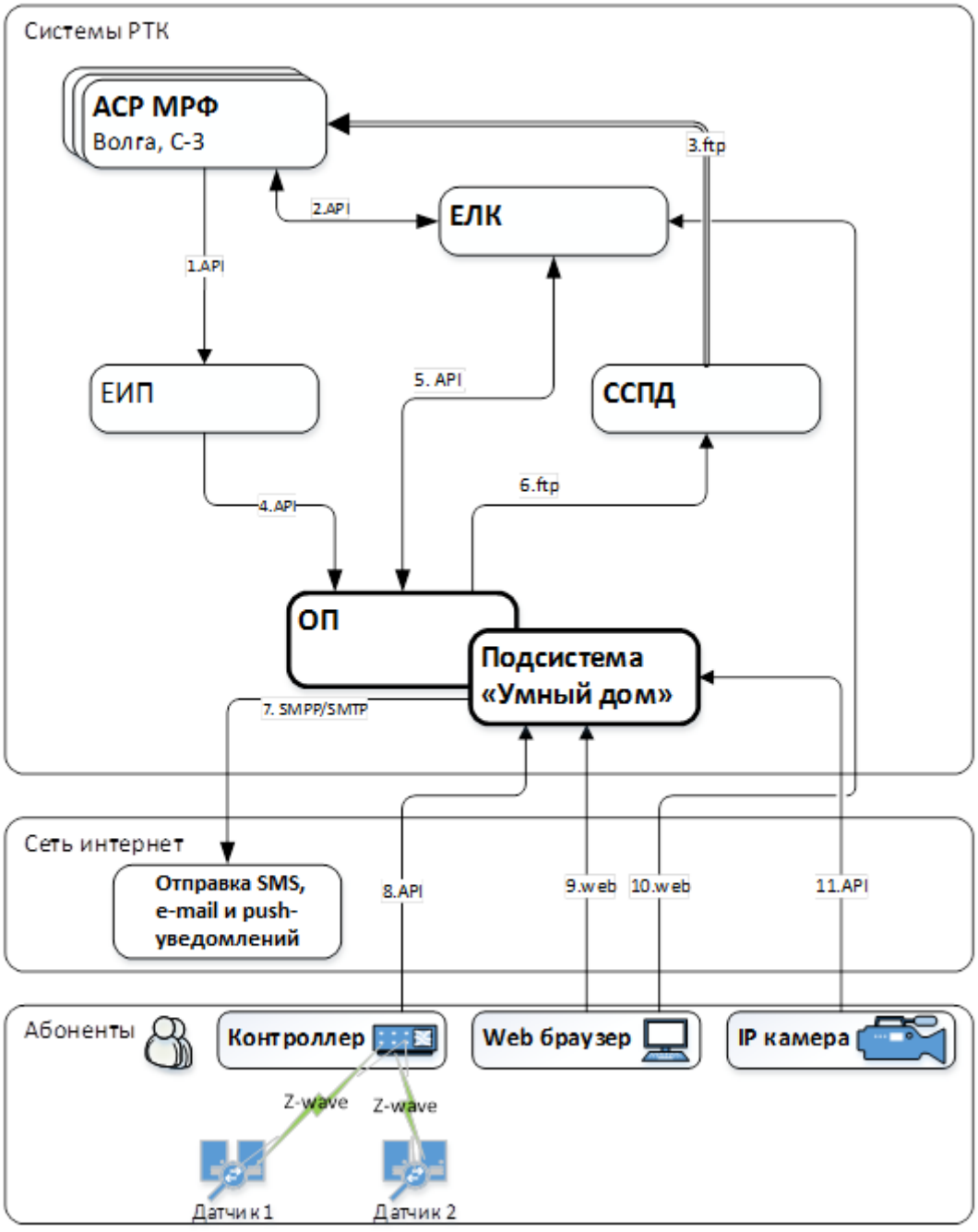
На следующих двух рисунках схематично показана архитектура, которая должна быть у промышленного КПС. При необходимости текущая архитектура опытного образца и связанных подсистем НОП могут быть предоставлены по запросу участника закупочной процедуры.

Рисунок 2-1. Верхне-уровневая схема прикладного п/о КПС



В результате внедрения КПС должна быть обеспечена поддержка бизнес-процессов подключения, эксплуатации, тарификации (включая блокировку/разблокировку Услуги за неуплату) и абонентского обслуживания на всех этапах жизненного цикла продукта.

Рисунок 2-2. Верхне-уровневая схема интеграции для пилотного запуска.



3.3 Сценарии использования услуги «Умный дом»

3.3.1 Подключение Услуги абонентом через ЕЛК. Пилотная зона.

Действующие лица:	Абонент
Объекты взаимодействия:	ЕЛК, АСР, ЕИП, ОП
Примечание:	
Предусловия:	У Абонента есть подключенная услуга ШПД, есть учётная запись в ЕЛК
Инициируется:	Абонентом
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария: 1) Абонент посредством web-интерфейса ЕЛК запрашивает подключение Услуги; 2) ЕЛК проверяет наличие ранее подключенной Услуги на ЛС услуги ШПД; 3) Если Услуга на ЛС услуги ШПД не подключена, то процесс подключения продолжается; 4) Если Услуга на ЛС услуги ШПД подключена, то процесс подключения прерывается. Абоненту выводится сообщение об ошибке; 5) ЕЛК отправляет запрос на подключение Услуги в АСР (выбирается та же АСР, где подключена услуга ШПД); 6) В АСР создаётся абонент Услуги на существующем Клиенте ШПД 7) АСР отправляет через ЕИП команду на создание профиля (подключение) Услуги в ОП. На ЕИП передаются данные о Клиенте (включая номер ЛС, идентификатор МРФ, идентификатор АСР); 8) В ОП создаётся технологическая учётная запись для подключающегося абонента Услуги; 9) После успешного завершения запроса подключения услуги (п.1) Пользователь получает возможность перейти по ссылке в Интерфейс Продукта. При первом входе в Интерфейс Продукта выполняются следующие действия: a. Процедура обязательной смены пароля учетной записи Пользователя в Интерфейсе Продукта; b. Процедура связывания технологической учетной записи ОП и учетной записи в ЕЛК; c. Запрос данных Пользователя в ЕЛК (телефон, e-mail и проч.); 10) В дальнейшем Абонент может аутентифицироваться напрямую в Интерфейсе Продукта; 11) Услуга полностью подключена.	
Расширение сценария:	
Принципы учета и тарификации:	Не тарифицируется

3.3.2 Подключение Услуги оператором

Действующие лица:	Оператор, Абонент
Объекты взаимодействия:	АСР, ЕИП, ОП
Примечание:	У Абонента есть подключенная услуга ШПД
Предусловия:	
Инициируется:	Абонентом
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария: 1) Оператор проверяет наличие ранее подключенной Услуги на ЛС услуги ШПД; 2) Если Услуга на ЛС услуги ШПД подключена, то процесс подключения прерывается;	

3) Если Услуга на ЛС услуги ШПД не подключена, то процесс подключения продолжается; 4) Оператор подключает в АСР Услугу существующему Абоненту ШПД; 5) В АСР создаётся абонент Услуги на существующем Клиенте ШПД; 6) АСР отправляет через ЕИП команду на создание профиля (подключение) Услуги в ОП. На ЕИП передаются данные о Клиенте (включая номер ЛС, идентификатор МРФ, идентификатор АСР); 7) В ОП создаётся технологическая учётная запись для подключающегося абонента Услуги; 8) В ЕЛК появляется ссылка на Интерфейс Продукта; 9) Далее абонент должен в обязательном порядке перейти из ЕЛК в Интерфейс Продукта для завершения процедуры создания учетной записи в ОП (связывается ранее созданная технологическая учётная запись ОП и учётная запись в ЕЛК); 10) В дальнейшем Абонент может аутентифицироваться напрямую в Интерфейсе Продукта; 11) Услуга полностью подключена.	
Расширение сценария:	
Принципы учета и тарификации:	Не тарифицируется

3.3.3 Отключение Услуги абонентом через ЕЛК.

Действующие лица:	Абонент
Объекты взаимодействия:	ЕЛК, АСР, ЕИП, ОП
Примечание:	
Предусловия:	У Абонента есть подключенная Услуга
Инициируется:	Абонентом
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария: 1) Отключение услуги через ЕЛК не производится; 2) Для отключения услуги абонент должен посетить ТПО РТК.	
Расширение сценария:	
Принципы учета и тарификации:	

3.3.4 Отключение услуги оператором.

Действующие лица:	Оператор
Объекты взаимодействия:	АСР, ЕИП, ОП
Примечание:	У Абонента есть подключенная Услуга
Предусловия:	
Инициируется:	Оператором
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария: 1) Оператор в ТПО через АСР отключает Услугу существующему Абоненту; 2) Производится закрытие абонента в АСР; 3) При закрытии абонента из АСР на ЕИП отправляется команда отключение профиля в ОП; 4) ОП блокирует профиль и отключает Услугу; 5) В АСР абонент закрывается стандартно; 6) Услуга полностью отключена.	
Расширение сценария:	
Принципы учета и тарификации:	

3.3.5 Блокировка Услуги по балансу.

Действующие лица:	
Объекты взаимодействия:	АСР, ЕИП, ОП
Примечание:	
Предусловия:	У Абонента подключена Услуга
Инициируется:	АСР
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария: 1) АСР принимает решение о финансовой блокировке Услуги; 2) АСР отправляет на ЕИП команду на блокировку профиля в ОП; 3) ОП ограничивает предоставление Услуги.	
Расширение сценария:	
Принципы учета и тарификации:	Не тарифицируется

3.3.6 Разблокировка Услуги по балансу.

Действующие лица:	
Объекты взаимодействия:	АСР, ЕИП, ОП
Примечание:	
Предусловия:	У Абонента подключена Услуга
Инициируется:	АСР
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария: 1) После изменения баланса АСР принимает решение о снятии финансовой блокировки Услуги; 2) АСР отправляет на ЕИП команду на разблокировку профиля в ОП; 3) ОП оказывает Услугу в полном объёме.	
Расширение сценария:	
Принципы учета и тарификации:	Не тарифицируется

3.3.7 Тарификация Услуги.

Действующие лица:	
Объекты взаимодействия:	АСР, ЕИП, ОП
Примечание:	
Предусловия:	У Абонента подключена Услуга
Инициируется:	ОП
Нефункциональные требования:	
Диаграмма:	

Основные шаги сценария: 1) После оказания Услуги в течение отчетного периода ОП ежедневно выкладывает CDR на FTP-сервер 2) CDR скачиваются ССПД и передаются в АСР. 3) После скачивания CDR ССПД должна удалить скаченные CDR с FTP-сервера ОП. CDR передается ежедневно. 4) АСР с учетом тарифных классов, указанных в CDR, рассчитывает стоимость потребленных услуг.	
Расширение сценария: 1) В случае наличия тестового периода при подключении услуги, тарификация начинается после его окончания.	
Принципы учета и тарификации:	По прейскуранту

3.3.8 Начало тарификации Услуги.

Действующие лица:	Абонент
Объекты взаимодействия:	Интерфейс Продукта, ОП
Примечание:	
Предусловия:	У Абонента подключена Услуга
Инициируется:	Абонент
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария: 1) Услуга успешно подключена в АСР и в ОП (создан профиль Услуги в ОП). 2) Услуга в ОП находится в статусе ожидания активации абонентского оборудования Услуги (статус Услуги в АСР не меняется), тарификация не проводится. 3) Абонент успешно проходит аутентификацию в Интерфейсе Продукта. 4) В Интерфейсе Продукта Абонент делает регистрацию (привязку к аккаунту) абонентского оборудования Услуги (Контроллера или Видеокамеры, по Идентификатору продукта или автоматически по IP адресу) в профиле услуги. 5) После успешной регистрации абонентского оборудования Услуги в профиле Услуги в ОП, Услуга в ОП переходит в активный статус (информация ни в ЕЛК, ни в АСР не передаётся). 6) Начинается тарификация Услуги в ОП.	
Расширение сценария:	
Принципы учета и тарификации:	По прейскуранту

3.3.9 Смена тарифа и подключение тарифных опций Услуги.

Действующие лица:	Абонент
Объекты взаимодействия:	Интерфейс Продукта, ОП
Примечание:	
Предусловия:	У Абонента подключена Услуга, идёт тарификация
Инициируется:	Абонент
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария:	

1) Абонент успешно проходит аутентификацию в Интерфейсе Продукта. 2) В Интерфейсе Продукта Абонент делает изменение тарифа и/или тарифных опций (например: измерение состава абонентского оборудования или увеличение времени хранения видеоархива с камер). 3) Изменения сохраняются в профиле Услуги в ОП (в АСР и ЕЛК изменения не передаются). 4) На основании внесённых в профиль Услуги изменений ОП формирует CDR файлы согласно прейскуранту с учетом тарифных классов.	
Расширение сценария:	
Принципы учета и тарификации:	По прейскуранту

3.3.10 Аутентификация на Интерфейсе Продукта при переходе из ЕЛК.

Действующие лица:	Абонента
Объекты взаимодействия:	ЕЛК, ОП
Примечание:	
Предусловия:	У Абонента подключена Услуга, есть учётная запись в ЕЛК
Инициируется:	Абонентом
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария: 1) Абонент проходит аутентификацию в web-интерфейсе ЕЛК с использование учетной записи ЕЛК. 2) Переходит в форму управления Услугой 3) Для управления опциями Услуги в интерфейсе ЕЛК должен быть визуальный элемент – ссылка на Интерфейс Продукта 4) При клике на ссылку абонент переходит на страницу аутентификации пользователя в Интерфейсе Продукта. .	
Расширение сценария:	
Принципы учета и тарификации:	Не тарифицируется

3.3.11 Аутентификация на Интерфейсе Продукта.

Действующие лица:	Абонента
Объекты взаимодействия:	ЕЛК, ОП
Примечание:	
Предусловия:	У Абонента подключена Услуга, есть учётная запись в ЕЛК
Инициируется:	Абонентом
Нефункциональные требования:	
Диаграмма:	
Основные шаги сценария: 1) Абонент открывает Интерфейс Продукта.	

2) Вводит логин и пароль учетной записи 3) Проводится аутентификация с использованием введённых данных 4) В случае успешной аутентификации (логин/пароль верный) Абонент переходит на web-портал Услуги и сразу попадает в свой профиль Услуги. 5) В случае не успешной аутентификации (логин/пароль не верный) Абонент переходит на URL с сообщением об ошибке.
Расширение сценария:

Принципы учета и тарификации:	Не тарифицируется

3.3.12 Регистрация абонентского оборудования Услуги.

Действующие лица:	Абонент
Объекты взаимодействия:	Интерфейс Продукта, ОП
Примечание:	
Предусловия:	У Абонента подключена Услуга Подключение Абонента (мобильное устройство или браузер) и абонентского оборудования (контроллер или видеокамера) происходит через одну и ту же точку доступа.
Инициируется:	Абонент
Нефункциональные требования:	

Диаграмма:

Основные шаги сценария:

1) Абонент подключает контроллер к локальной сети;
2) Контроллер устанавливает соединение с Интерфейсом Продукта;
3) Интерфейс Продукта поддерживает список контроллеров, которые еще не были зарегистрированы Абонентом. Контроллеры в списке идентифицируются по публичному ip-адресу;
4) Абонент успешно проходит аутентификацию в Интерфейсе Продукта;
5) Интерфейс Продукта отображает Контроллер, находящийся в той же локальной сети, что и Абонент, то есть с таким же публичным ip-адресом.
6) В Интерфейсе Продукта Абонент делает регистрацию абонентского оборудования (в АСР и ЕЛК изменения не передаются).
7) Изменения сохраняются в профиле Услуги в ОП (в АСР и ЕЛК ничего не передаётся).

Расширение сценария:

5.1) Если Интерфейс Продукта не отображает Контроллер (в списке контроллеров нет Контроллера с подходящим ip-адресом), то у Абонента есть возможность добавить Контроллер по mac адресу Контроллера.

Регистрация видео камер:
На этапе пилотного запуска будут использоваться видеокамеры только одной модели. Факт активации видеокамеры фиксируется на КПС, где Абонент должен согласиться с новым Тарифом для того, чтобы услуга видеонаблюдение для новой камеры стала активной.

Примечание:
У каждого Абонента Услуги в Интерфейсе Продукта может быть зарегистрирован один контроллер.

Принципы учета и тарификации:	По прейскуранту

4 Требования к системе

4.1 Функциональные требования

КПС должен предоставлять Пользователям следующие возможности:

- доступ к функциям камеры;
- просмотр статусов и событий;
- отображение состояния датчиков, счетчиков;
- управление сценариями и режимами;
- управление подключенными устройствами;
- управления основными функциями КПС с мобильных устройств;
- рассылка уведомлений.

Для выполнения возложенных функций, КПС должен включать в себя следующие функциональные подсистемы:

1) Подсистема авторизации и аутентификации пользователей;
2) Подсистема видеонаблюдения;
3) Подсистема регистрации и хранения событий;
4) Подсистема взаимодействия с управляющим контроллером;
5) Подсистема управления сценариями и режимами;
6) Подсистема регистрации подключенных устройств;
7) Подсистема уведомлений;
8) Веб-интерфейс пользователя;
9) Веб-интерфейс администратора;
10) Интерфейс для взаимодействия с мобильными приложениями;
11) Интерфейс для поддержки провиженинга и биллинга услуги «Умный дом».

4.1.1 Авторизация и аутентификация пользователей

Процесс авторизации пользователей выполняется по логину и паролю в КПС. Смена пароля и иные действия с учётной записью проводятся средствами облачной платформы. При успешной аутентификации и авторизации ЕЛК передает на ОП и КПС контактные данные абонента, его л/с в АСР, идентификатор АСР и аутентификационные данные. Данные передаются по протоколу HTTPS.

В КПС должен быть реализован механизм управления личными данными пользователя. Пользователь должен иметь возможность редактировать следующие данные:

- E-mail;
- номер телефона.

Подсистемы КПС должны функционировать по мультитенантной модели (одна система на множество пользователей). Под Тенантом подразумевается совокупность данных внутри системы, принадлежащих одному пользователю.

4.1.2 Видеонаблюдение

В КПС должны быть реализованы следующие функции в части доступа к функциям камеры:

- регистрация абонентского видео-оборудования (web-камеры установленные на PC и IP камеры) в профиле пользователя;
- выбор элемента видеонаблюдения;
- редактирование названия элемента видеонаблюдения;
- просмотр потокового видео от выбранного источника видеонаблюдения;
- сохранение видеопотока с абонентского оборудования;
- просмотр видеопотока в режиме реального времени;
- доступ к архивам записей с помощью удобного навигатора (календарь);
- выгрузка видеоматериала на устройство клиента в популярных форматах;
- сохранение отдельных кадров видеоматериала на устройство клиента;
- анализ движения и освещенности, уведомление о движении.

Спецификация протокола предоставляется Заказчиком.

4.1.3 Просмотр статусов и событий

В КПС должны быть реализованы следующие функции в части просмотра и управления статусами и событиями:

- отображение статуса соединения Контроллера с сервисом;
- просмотр последних событий с отображением списка сохраненных скриншотов и записей камеры и с возможностью их просмотра;
- возможность группировки событий по дате и времени;
- фильтрация событий по периодам;
- выбор типов оповещений для событий общего типа:
  - по электронной почте;
  - смс сообщениями;
  - push-уведомления.

События должны быть разделены на следующие группы:

- Системные события (включая критические события) – отражают изменения параметров устройств, факт выполнения сценариев и событий, которые требуют срочного внимания пользователя;
- Пользовательские события - отражают изменения, которые сделал пользователь.

4.1.4 Взаимодействие с контроллером

В КПС должны быть реализованы следующие функции в части взаимодействия с управляющим контроллером:

- регистрация управляющего контроллера;
- взаимодействие с управляющим контроллером умного дома посредством прямого постоянно открытого соединения;
- оповещение пользователя о потере связи с управляющим контроллером;
- регистрация датчиков, счетчиков, IP-видеокамер подключенных к Управляющему контроллеру с возможностью автоматического определения типа устройства;
- доступ к функциям датчиков, счетчиков.

4.1.5 Управление сценариями и режимами

В сервисе «Умный дом» должны быть реализованы следующие функции в части управления сценариями:

- создание, изменение, удаление и хранение сценариев взаимодействия локальных устройств;
- должна быть реализована возможность выбора следующих элементов сценария:
  - выбор простых условий;
  - выбор сложных условий;
  - выбор режимов, в которых данный сценарий будет выполняться;
  - выбор дополнительных условий;
- отображение списка сценариев;
- активация и деактивация сценариев;
- хранение базы шаблонов типовых сценариев;
- передача созданных сценариев и настроек в управляющий контроллер.

В части управления режимами в сервисе «Умный дом» должны быть реализованы следующие функции:

- создание, изменение, удаление и хранение режимов работы;
- отображение списка режимов работы;
- возможность переключение между преднастроенными режимами;
- создание пользователем собственного режима.

В сервисе «Умный дом» должны быть реализованы следующие режимы:

- «отключено»;
- «я дома»;
- «вне дома»;
- «персональный»;
- «в отъезде».

Точный список режимов должен быть составлен на этапе разработки промышленного образца комплекса программных средств «Умный дом».

4.1.6 Управление устройствами

Устройства в КПС должны быть разделены на типы, например:

- сенсоры;
- датчики тревоги;
- помещение;
- климат.

Точный список типов должен быть составлен на этапе разработки промышленного образца комплекса программных средств «Умный дом».

Каждое устройство должно быть определено совокупностью признаков. Каждый признак должен быть описан в соответствующем поле. При этом, следующие поля должны быть обязательными для всех устройств:

- идентификатор устройства;
- идентификатор приставки;
- имя устройства;
- расположение устройства;
- производитель;
- идентификатор продукта;
- тип устройства.

Также должна быть реализована возможность изменения списка обязательных и необязательных полей в зависимости от типа устройства.

В КПС должна быть реализована следующая функциональность в части управления подключенными устройствами:

- активация устройства;
- деактивация устройства;
- просмотр статусов подключенных устройств;
- просмотр информации о подключенных устройствах;
- подключение новых устройств;

4.1.7 Учет показателей счетчиков ЖКХ

В рамках пилотного проекта требования к учету показателей счетчиков ЖКХ не предъявляются.

4.1.8 Уведомления о событиях

В части рассылки уведомлений должна быть реализована возможность отправки в реальном времени сообщений на электронную почту, смс-сообщений и push-уведомлений а также уведомлений посредством вывода сигнализирующей информации на страницах веб-сервиса.

При этом рассылка уведомлений должна происходить с учетом настроек пользователя (адрес электронной почты, номер телефона) в части получения уведомлений по различным событиям.

Уведомления по электронной почте отправляются через почтовый сервер Заказчика по протоколу SMTP.

Уведомления в виде смс-сообщений отправляются через смс-шлюз Заказчика по одному из указанных ниже протоколов:

- протокол SMPP v.3.4 или выше
- HTTP протокол (спецификация протокола предоставляется Заказчиком).

4.1.9 Веб-интерфейс пользователя

Веб-сервис пользователя должен состоять из следующих информационных блоков, предоставляющих доступ к функциям сервиса «Умный дом»:

- Блок «Рабочий стол» должен содержать следующие компоненты:
  - окно камеры (с элементами управления и доступа к функциям камеры);
  - просмотр последних событий с фильтром по времени;
  - блок с отображением состояния датчиков и сигналов, содержащий управляющие элементы и быстрый доступ к устройствам;
  - блок с возможностью активации и деактивации режимов;
  - блок с отображением критичных оповещений;
- Блок «События» должен содержать все типы событий с возможностью фильтрации по дате, по типу событий и по устройству:
- Блок «Мои устройства» должен содержать:
  - информацию о подключенных устройствах;
  - информацию о статусе подключенных устройств;
  - возможность добавления новых устройств;
  - возможность управления подключенными устройствами;
  - возможность управления названием и расположением подключенных устройств;
  - информацию с датчиков подключенных устройств;

  - информацию о подключенном абонентском видео-оборудовании, с возможностью добавления новых устройств;
  - возможность настройки элементов видеонаблюдения;
  - просмотр потока/скриншотов для выбранного элемента видеонаблюдения.
  - Блок «Сценарии» должен содержать:отображение списка сценариев с фильтрацией по режимам;
  - полнотекстовый поиск по списку сценариев;
  - запуск сценария вручную;
  - блок с отображением текущих созданных сценариев с указанием статуса (задействован или не задействован);
  - управление сценариями (включение, отключение, редактирование и удаление).
- Профиль пользователя;
  - изменение фотографии;
  - изменение и добавление номеров телефонов;
  - изменение и добавление адресов электронной почты;
  - изменение адреса;
  - изменение пароля отмена аутентификации пользователя в мобильном приложении.
- Блок «Настройки» должен содержать:
  - Управление рассылкой уведомлений;
  - Управление мобильными устройствами для рассылки push-уведомлений;
  - Управление активными сессиями с возможностью их остановки.
- Блок «Помощь» должен содержать:
  - Возможность ведения списка часто задаваемых вопросов;
  - Возможность отображения списка часто задаваемых вопросов.

4.1.10 Веб-интерфейс администратора

Должен быть разработан интерфейс администраторов КПС, обеспечивающий взаимодействие специалистов службы эксплуатации Заказчика с КПС. В интерфейсе администраторы должны быть доступны следующие функции:

- Просмотр верхнеуровнего состояния системы;
- Просмотр параметров подключенных абонентов;
- Просмотр системных событий;
- Просмотр состояния подключенного оборудования.

Веб-интерфейс администраторов должен состоять из следующих разделов:

- Пользователи (тенанты);
- Устройства;
- Состояние системы;
- Настройки.

4.1.11 Интерфейс для мобильных приложений

Основные функции КПС должны быть доступны пользователям через мобильные приложения на устройствах под управлением ОС Android и iOS.

В КПС должен быть реализован следующий интерфейс взаимодействия (API) в части управления функциями с помощью мобильных устройств:

- авторизация в КПС;
- добавление контроллера;
- управление контроллером;
- добавление и удаление пользовательских устройств;
- управление подключенными устройствами;
- получение событий;
- получение справочников;
- возможность активации и деактивации режимов работы сервиса;
- отображение трансляции видеокамеры и сохраненных кадров, в том числе в полноэкранном режиме;
- включение и выключение записи видеотрансляции;
- включение и выключение активных сценариев.

4.1.12 Интерфейс для взаимодействия с контроллером

В КПС должен быть реализован следующий интерфейс взаимодействия (API) в части управления контроллером:

- авторизация в КПС;
- управление контроллером;
  - получение информации о контроллере;
  - текущее состояние;
  - версия прошивки;
  - восстановление конфигурации контроллера.
- добавление/удаление устройств;
- управление устройствами;
- получение информации о изменении состояния устройств;
- работа с режимами;
- работа с сценариями;

4.1.13 Поддержка провиженинга и биллинга услуги «Умный дом»

В КПС должен быть реализован следующий функционал в части поддержки провиженинга и биллинга услуги «Умный дом»:

- Создание/удаление профиля пользователя;
- Блокировка/разблокировка профиля пользователя;
- Получение списка пользователей;
- Получение статуса и данных по профилю пользователя;
- Получение информации о подключенных пользователем устройствах;
- Получение информации об отправленных уведомлениях;
- Получение информации о размере видеоархива.

4.2 Нефункциональные требования

4.2.1 Требования к надежности

Разработка должна выполняться с учетом необслуживаемого функционирования КПС в режиме 24/7/365.

Уровень надежности должен достигаться согласованным применением организационных, организационно-технических мероприятий и программно-аппаратных средств.

Надежность должна обеспечиваться за счет:

- применения технических средств, системного и базового программного обеспечения, соответствующих классу решаемых задач;
- своевременного выполнения процессов администрирования;
- соблюдения правил эксплуатации и технического обслуживания программно-аппаратных средств;
- предварительного обучения пользователей и обслуживающего персонала.

КПС должен сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих аварийных ситуаций:

- при сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке ОС, восстановление программы должно происходить после перезапуска ОС и запуска;
- при ошибках в работе аппаратных средств (кроме носителей данных и программ) восстановление функций возлагается на ОС;
- при ошибках, связанных с программным обеспечением, восстановление работоспособности возлагается на ОС.

В рамках пилотного проекта комплекс программных средств «Умный дом», развернутый на инфраструктуре Заказчика должен обеспечивать функционирование при обслуживании до 2000 абонентов, из расчета на абонента: 1 видеокамера, от 2-х до 10-ти Z-Wave устройств.

Должна быть разработана методика масштабирования решения при увеличении нагрузки до 72 000 пользователей.

На этапе пилота при установке обновлений КПС допускается прерывание сервиса для клиентов. В промышленной эксплуатации установка обновлений не должна приводить к прерыванию сервиса.

На этапе пилота должно быть обеспечено резервное копирование виртуальных машин для всех компонентов КПС. В промышленной эксплуатации резервирование всех компонентов КПС должно обеспечиваться применением кластерных решений. Политики резервного копирования должны быть согласованы с Заказчиком и отражены в эксплуатационной документации.

4.2.2 Требования к устойчивости функционирования

КПС должен разрабатываться с учетом Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования, утвержденных Приказом Министерства связи и массовых коммуникаций Российской Федерации № 104 от 25.08.2009.

Устойчивость функционирования должна обеспечиваться:

- разработкой мер при проектировании, направленных на выполнение требований к показателям надежности;
- соблюдением условий эксплуатации, установленных в технической и эксплуатационной документации соответствующих технических и программных средств;
- выполнением требований в части технического обслуживания ее технических и программных средств;
- выполнением требований к управлению в части контроля функционирования и анализа технических неисправностей.

В соответствии с приказом Министерства связи и массовых коммуникаций Российской Федерации от 25.08.2009 N 104 комплекс программных средств «Умный дом» относится к информационным системам общего пользования класса II, поэтому к нему предъявляются следующие требования:

- должна обеспечиваться защита от воздействий на технические и программные средства, в результате которых нарушается их функционирование, и защита от несанкционированного доступа к помещениям, в которых размещены данные средства;
- должна осуществляться регистрация действий обслуживающего персонала.

4.2.3 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов

Устанавливаются следующие общие требования к условиям эксплуатации и техническому обслуживанию:

- эксплуатация и техническое обслуживание средств должно осуществляться эксплуатационным персоналом, требования к численности, квалификации и режиму работы которого определены в разделе 4.2.11;
- размещение технических средств и организация автоматизированных рабочих мест пользователей должно быть выполнено в соответствии с требованиями санитарных норм и правил в соответствии с ГОСТ 21958-76;
- условия эксплуатации, а также виды и периодичность обслуживания технических средств должны соответствовать требованиям по эксплуатации, техническому обслуживанию, ремонту и хранению, изложенным в документации их производителя.

Обязательной составляющей регламентных работ технического обслуживания должно быть периодическое резервное копирование информационных ресурсов, в том числе базы данных, исполняемых и исходных кодов программного обеспечения, областей дискового пространства, содержащих информацию, необходимую для нормального функционирования.

Для обеспечения сохранности программного обеспечения должна быть создана и передана на хранение Заказчику эталонная копия дистрибутива прикладного программного обеспечения. Обновление эталонной копии может производиться Исполнителем по согласованному с Заказчиком регламенту.

4.2.4 Требования к информационной безопасности

4.2.4.1 Общие требования к информационной безопасности

В ходе создания системы должны быть проведены работы по разработке механизмов защиты персональных данных, а также работы по оценке необходимости и возможности применения в системе средств криптографической защиты информации по ГОСТ.

Все компоненты и прикладное ПО КПС на этапе передачи в промышленную эксплуатацию, должны быть стабильных последних версий, либо должны быть установлены обновления до тех версий, которые обеспечивают максимальную защищённость системы (отсутствие известных уязвимостей).

4.2.4.2 Требования к аутентификации и авторизации

КПС должен иметь возможность для каждого пользователя создавать уникальную учетную запись.

КПС должен включать в себя механизм аутентификации. Аутентификация должна проводиться с использованием одного из следующих средств:

- Логин/Пароль;

В КПС должен присутствовать механизм авторизации пользователей. При этом должно поддерживаться разделение прав доступа к информации/данным и функциям внутри КПС.

КПС должна поддерживать предоставление пользователям прав доступа на основании групповой или ролевой модели.

КПС должен предоставлять доступ к своим ресурсам только после успешного прохождения процесса аутентификации пользователя, в соответствии с его правами доступа. Данное требование не распространяется на ресурсы, которые должны находиться в публичном доступе.

Учетная запись пользователя в КПС должна создаваться в процессе подключения услуги. После аутентификации в ЕЛК пользователь может выполнить первый вход в систему с новой учетной записью.

На этапе пилотного проекта к процессу аутентификации предъявляются следующие требования. КПС должен:

- Предоставлять пользователям возможность самостоятельно устанавливать свой пароль и менять его в любое время;
- Проверять качество вводимого пароля. Пароль пользователя должен содержать не менее 8 символов, из которых как минимум 1 символ является заглавной буквой и как минимум один символ является цифрой;
- Предоставлять возможность обязательной смены заданного администратором пароля при первом входе в систему;
- Иметь возможность автоматической блокировки учётной записи, в случае если ее пароль до установленной даты не был изменён;
- Иметь возможность блокировки учётной записи на заранее определенный срок после заданного количества неудачных попыток аутентификации;
- Иметь возможность установки срока длительности простоя пользовательской сессии, после которого сессия должна принудительно завершаться;
- Иметь возможность ограничить множественный вход в систему под одной учетной записью пользователя.

Для ввода КПС в промышленную эксплуатацию дополнительно предъявляются следующие требования. КПС должен:

- Проверять качество вводимого пароля в соответствии с требованиями парольной политики;
- Иметь возможность задавать параметры парольной политики для группы пользователей, а также возможность назначать их отдельно для каждой отдельной учетной записи;
- Позволять администраторам отключать возможность смены пароля у отдельных пользователей;
- Обеспечивать принудительную смену пароля через установленный промежуток времени;
- Иметь возможность заблаговременно оповещать пользователей о необходимости смены пароля (посредством сообщений/подсказок или почтовых рассылок на электронные адреса пользователей);
- Обеспечивать хранение истории паролей пользователей, как минимум, за последние 12 месяцев для предотвращения повторного их использования.

Пароли должны храниться и передаваться только в зашифрованном виде. При хранении и передаче должны использоваться современные криптографические алгоритмы или алгоритмы хеширования

На этапе пилотного проекта пользовательские интерфейсы КПС не должны выдавать информации о типе и версии системы или ее компонент до успешного завершения процедур аутентификации и авторизации. Для ввода КПС в промышленную эксплуатацию данное требование должно выполняться для всех интерфейсов КПС.

В процессе аутентификации проверка введенной информации (логин, пароль) должна осуществляется только после полного ее ввода. В случае обнаружения ошибки, система не должна уточнять, какие именно данные введены неправильно. Пароль не должен отображаться при вводе.

КПС и его компоненты не должны содержать жестко запрограммированных учетных записей.

Компоненты КПС в случае сетевого взаимодействия через публичные сети (интернет), должны проходить процедуру взаимной аутентификации .

КПС Проверка учетных данных пользователя должна проводиться на стороне серверных компонент ИС.

Все неиспользуемые для штатной работы КПС учетные записи (установленные по умолчанию, тестовые, сервисные) должны быть удалены или заблокированы до начала передачи ИС в эксплуатацию.

Пароли от предустановленных учетных записей и сервисов должны быть изменены сразу после установки КПС в продуктивную среду.

Все действия в КПС должны производиться с использованием учетных записей, наделенных минимально необходимыми привилегиями.

4.2.4.3 Требования к аудиту

Компоненты КПС должны синхронизировать системное время с NTP-сервером, являющимся частью инфраструктуры сети ОАО Ростелеком (допустимая погрешность не более 5 секунд). Серверы NTP и доступ к ним обеспечивает Заказчик.

КПС должен поддерживать следующие механизмы протоколирования событий:

- Должны поддерживаться регистрация, хранение и просмотр событий стандартными средствами операционной системы;
- Должны быть реализованы регистрация и отправка событий во внешние системы по протоколу syslog. Формат сообщений должен быть описан в документации.

В КПС должно осуществляться протоколирование следующих событий:

- Успешные и неуспешные попытки аутентификации пользователя в системе;
- Действия привилегированных пользователей по настройке и изменению конфигурации ИС (в том числе изменение настроек аудита);
- Любой доступ пользователей к данным конфиденциального характера;
- Успешные и неуспешные попытки доступа пользователя к данным системы и другим ресурсам;
- Доступ к записям журнала протоколирования событий (требование не является обязательным на этапе пилотного проекта);
- Запуск и остановка ИС;
- Создание и удаление объектов системного уровня (учетные записи, профили поддерживаемого оборудования, шаблоны сценариев и т.п.).

Журналы событий должны содержать, как минимум, следующую информацию:

- Идентификатор пользователя, выполнившего операцию;
- Источник события (IP-адрес, идентификатор рабочей станции, ID источника и т.д.);
- Название или тип выполненного события;
- Дату и время события;
- Результат события;
- Объект, над которым была выполнена операция;

Журналы аудита КПС не должны содержать данных конфиденциального характера (паролей или другой закрытой информации в открытом или преобразованном виде и.т.д.).

Для ввода КПС в промышленную эксплуатацию должна быть обеспечена защита журналов аудита от несанкционированных изменений.

4.2.4.4 Требования к сетевому взаимодействию

Любой процесс обмена конфиденциальной информацией Заказчика через публичные сети должен осуществляться по зашифрованному каналу передачи данных. При этом допустимо использование следующих стандартов и протоколов:

- TLS/SSL (не ниже версии 3);
- SFTP;
- FTPS;
- SSH-2
- WSS;
- S/M IME с использованием сертификатов x.509 v3;
- VPN (IPSEC, L2TP, PPTP и т.д.).

При невозможности использовать указанные выше способы передачи передаваемые данные должны быть зашифрованы с применением современных стойких криптографических алгоритмов.

Если КПС необходим доступ к системам или базам данных, расположенным во внутренней сети Заказчика (КСПД), то обмен данными между ними должен осуществляться с использованием защищенных протоколов.

Сетевое взаимодействие между компонентами КПС, а также взаимодействие с внешними системами, должно проходить с использованием защищенных протоколов, если это технически возможно.

4.2.4.5 Требования к конфиденциальности, целостности и доступности данных

Любые изменения конфиденциальных или прикладных данных в КПС должны носить характер транзакционно-ориентированных, т.е. выполняющихся в целом от начала до конца либо, в случае сбоя транзакции, не выполняющихся совсем.

КПС должен обладать возможностью балансирования нагрузки между отдельными компонентами и модулями ИС. При этом выход из строя отдельных узлов ИС не должен сказываться на общей функциональности системы.

Данные конфиденциального характера, хранящиеся в КПС, должны быть защищены с использованием стойких алгоритмов шифрования.

В пользовательских интерфейсах КПС должна поддерживаться валидация (проверка) входных данных. Должна обеспечиваться возможность ввода только тех значений, которые являются допустимыми для данных форм/применений.

Должно осуществляться кодирование входных данных до их передачи ИС и ее внешним компонентам (LDAP-сервер, база данных, web-браузер и т.д.).

КПС должны поддерживать режим обработки ошибок, при котором пользователю не сообщается детальная информация об ошибке (версии подсистем, таблицы БД, сетевые адреса компонент ИС и т.д.) в случае сбоя приложения.

В КПС должны быть предусмотрены механизмы резервного копирования и восстановления данных с использованием системы резервного копирования Заказчика. Для реализации резервного копирования должен быть составлен перечень объектов, требующих резервирования. Настройка системы резервного копирования Заказчика лежит вне рамок данного технического задания.

Для обеспечения работы внешней системы резервного копирования КПС не должен постоянно работать с данными в монопольном режиме. Должны быть предусмотрены временные интервалы, в которые КПС будет снимать блокировки с данных.

4.2.4.6 Дополнительные требования к web-компонентам

КПС должен поддерживать интеграцию своих подсистем аутентификации с централизованными системами управления учетными данными и правами пользователей. Указанное требование не распространяется на процесс аутентификации клиентов B2C. Указанное требование не является обязательным в рамках пилотного проекта.

КПС должен обеспечивать возможность завершения сессии пользователя из любой страницы системы. Для ввода КПС в промышленную эксплуатацию дополнительно должно быть обеспечено закрытие сессии пользователя при неаварийном закрытии браузера.

На web-серверах КПС должен быть заблокирован доступ ко всем типам файлов MIME, которые не предназначены к обработке в ИС.

4.2.5 Требования по сохранности информации при авариях

При возникновении сбоев в аппаратном обеспечении, включая аварийное отключение электропитания, КПС должен автоматически восстанавливать свою работоспособность после устранения сбоев и корректного перезапуска аппаратного обеспечения (за исключением случаев повреждения рабочих носителей информации с исполняемым программным кодом).

К КПС предъявляются следующие общие требования по сохранности информации и восстановлению работоспособности после устранения последствий сбоев:

- должно осуществляться резервное копирование информации, периодичность проведения которого должна определяться Заказчиком и устанавливаться административными настройками резервного копирования;

- средствами резервного копирования и восстановления данных должно обеспечиваться восстановление информации в состояние, соответствующее используемой резервной копии. При этом допускается приостановка функционирования некоторых средств на время проведения операций по восстановлению информации либо перевод отдельных ее компонентов в режим автономной работы.

КПС должен обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях КПС должен выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных. Для предотвращения наступления аварийных ситуаций в случаях, когда это допустимо, должны использоваться следующие элементы интерфейса:

- drag-and-drop;
- выпадающие списки;
- другие элементы, предполагающие выбор из существующего списка значений.

4.2.6 Требования к защите от влияния внешних воздействий

В помещениях с размещенными техническими средствами, на которых будет функционировать КПС, должны быть обеспечены климатические условия, определяемые требованиями производителей используемых технических средств.

4.2.7 Требования к патентной чистоте

По всем техническим и программным средствам, применяемым при разработке КПС, должны соблюдаться условия лицензионных соглашений и обеспечиваться патентная чистота.

4.2.8 Требования по стандартизации и унификации

Разработка прикладного программного обеспечения КПС должна быть основана на применении принципов объектно-ориентированного программирования и модульной архитектуры с использованием типовых программных компонент, реализующих одни и те же функции (фрагменты функций). Должны применяться тиражные инструментальные средства разработки программного обеспечения, общепринятые (стандарты де-факто) языки программирования, стандартные технические и программные средства общего назначения и процедуры информационного взаимообмена.

При создании КПС должно использоваться тиражное стандартное общесистемное программное обеспечение, лицензированное установленным порядком.

Исходный программный код должен быть самодокументируемым, то есть имена переменных, процедур, функций, объектов и т. д. должны объяснять свое наименование и назначение. Данный код позволит сформировать в автоматизированном режиме полное описание всех переменных, процедур, функций, объектов и т. д. в единую документацию. Исходные коды должны быть написаны с использованием понятных имен классов, их свойств, методов и переменных.

Все классы в исходном коде должны иметь комментарий, в котором указывается назначение данного класса. Все методы классов должны включать в себя:

- комментарий, содержащий назначение данного метода (описание входных параметров метода; возможные значения возвращаемого результата; перечисление исключительных ситуаций, которые могут возникнуть при использовании этого метода);
- примеры использования метода (применимо в отдельных случаях, которые могут быть уточнены на этапе проектирования).

Пользовательский интерфейс должен обеспечивать необходимое качество взаимодействия человека с машиной и комфортность работы пользователей.

Должно применяться серийно выпускаемое оборудование и аппаратные средства ведущих мировых производителей, сертифицированное для применения в Российской Федерации.

4.2.9 Требования к режимам функционирования

КПС должен поддерживать следующие режимы функционирования:

Режим функционирования	Характеристика
Штатный режим	Основной режим функционирования. В штатном режиме функционирования: — обеспечивается возможность функционирования в режиме 24/7; — исправно работает оборудование, составляющее комплекс технических средств; — исправно функционирует системное, базовое и прикладное программное обеспечение. Для обеспечения штатного режима функционирования необходимо выполнять требования и выдерживать условия эксплуатации программного обеспечения и комплекса технических средств
Аварийный режим	Аварийный режим функционирования характеризуется отказом одного или нескольких компонентов программного и (или) технического обеспечения
Регламентный режим	Используется для проведения регламентных работ

4.2.10 Требования по диагностированию программного средства

КПС должен включать в себя инструмент (скрипт и/или API) диагностики. Инструмент диагностики должен позволять контролировать корректность работы всех внешних и внутренних интерфейсов системы, включая подключения к БД и очередям. Технология реализации инструмента диагностики и список интерфейсов, подлежащих диагностике, должны быть согласованы с Заказчиком и отражены в эксплуатационной документации.

Метрики для диагностики, нормальные значения и аварийные диапазоны должны быть согласованы с Заказчиком и отражены в эксплуатационной документации.

4.2.11 Требования к численности и квалификации персонала

Весь персонал, эксплуатирующий КПС, может быть разделен на две группы:

- пользователи;
- обслуживающий персонал.

Пользователи должны иметь опыт работы с персональным компьютером на уровне квалифицированного пользователя.

Обслуживающим персоналом является системный администратор. Системный администратор должен иметь навыки по установке, настройке и администрированию программных и технических средств, перечисленных в п. 4.2.12 настоящего ТЗ и обладать высоким уровнем квалификации в следующих областях:

- администрирование технических средств (серверы, рабочие станции, приставки);
- администрирование программного обеспечения операционных систем и систем управления базами данных;
- разработка, управление и реализация эффективной политики информационной безопасности;
- доработка программных и технических средств.

Работа с КПС организована с помощью средств вычислительной техники, результаты отображаются на мониторах и дисплеях, поэтому требования к организации труда и режима отдыха при администрировании должны устанавливаться, исходя из требований к организации труда и режима отдыха при работе с этим типом средств вычислительной техники согласно СП 2.2.2.1327-03 «Гигиенические требования к организации технологических процессов, производственному оборудованию и рабочему инструменту».

4.2.12 Требования к составу и параметрам технических средств серверной части

Выбор оборудования должен осуществляться с учетом следующих требований:

- прекращение или сбой электропитания на время до 15 минут не должен приводить к прекращению функционирования;
- должны использоваться технические средства повышенной отказоустойчивости;
- должна быть предусмотрена возможность структурного резервирования;
- комплекс технических средств должен быть обеспечен комплектом запасных изделий и приборов (ЗИП);
- носители информационных массивов должны быть продублированы.

Комплекс технических средств серверной части должен включать следующие компоненты:

- веб-сервер;
- сервер приложений;
- сервер балансировки;
- сервер баз данных (БД).

Компоненты серверной части КПС должны быть реализованы на базе свободного программного обеспечения.

Требования к техническим характеристикам серверной группы:

Компонент	Конфигурация
Тип сервера	Виртуальный сервер
Процессор	не менее 4 ядер
Оперативная память	веб-сервер – не менее 16 Гб сервер приложений – не менее 16 Гб

Компонент	Конфигурация
	сервер балансировки – не менее 4 Гб сервер баз данных – не менее 16 Гб
Дисковая подсистема	веб-сервер – не менее 300 Гб SAS сервер приложений – не менее 300 Гб SAS сервер балансировки – не менее 200 Гб SAS сервер баз данных – не менее 300 Гб SAS, дополнительный диск - не менее 1 Тб SAS

4.2.13 Требования к составу и параметрам рабочих станций

Аппаратное обеспечение стационарного рабочего места системного администратора должно удовлетворять следующим минимальным требованиям:

Компонент	Конфигурация
Центральный процессор	Intel 3 ГГц
Оперативная память	2 Гб и выше
Жесткий диск	80 Гб
Привод чтения компакт дисков	CD/DVD
Монитор	SVGA 1280x1024

Работоспособность основных функций веб-сервиса должна обеспечиваться в интернет-обозревателях:

- Microsoft Internet Explorer версии 11.0 и выше;
- Mozilla Firefox версии 21.0 и выше;
- Google Chrome версии 26.0 и выше;
- Opera 11.0 и выше.

Веб-сервис должен обеспечивать комфортную работу при удаленном доступе в сетях передачи данных со скоростью не менее 512 Кб/сек.

Мобильные устройства под управлением ОС семейств Android и iOS, подключаемые к веб-сервису с использованием удаленного доступа через Интернет, должны поддерживать технологии GPRS/EDGE/3G.

4.2.14 Требования к информационной и программной совместимости

Целостность сервиса «Умный дом» должна обеспечиваться совместимостью протоколов взаимодействия и совместимостью интерфейсов технических средств (физической совместимостью). Функциональная и физическая совместимость технических и программных средств должна обеспечиваться выполнением требований, устанавливаемых в технической и эксплуатационной документации.

Информационное взаимодействие между компонентами КПС должно осуществляться с использованием общей базы данных.

Для взаимодействия со смежными системами, интерфейсы КПС должны быть построены на основе открытых стандартов, позволяющих произвести выгрузку данных или обмен информацией с другими сервисами.

Информационная совместимость со смежными системами должна достигаться за счет использования стандартного протокола обмена структурированными сообщениями SOAP/HTTP.

4.3 Требования к интеграции

4.3.1 Интеграция с платформой видео-наблюдения

Функции видео-наблюдения в КПС должны быть реализованы на базе внешней платформы видео-наблюдения. Платформа видео-наблюдения предоставляется Заказчиком. Описание API платформы видео-наблюдения может быть предоставлено по запросу участника закупочной процедуры.

4.3.2 Интеграция с НОП

Функции поддержки провиженинга и биллинга, реализуемые в КПС, предназначены для использования из соответствующих подсистем НОП. Описание API для поддержки указанных функций разрабатывает Исполнитель с учетом требований настоящего технического задания и архитектуры связанных подсистем НОП.

4.3.3 Интеграция с почтовым шлюзом и SMS-шлюзом

Функции отправки уведомлений по электронной почте и с помощью SMS-сообщений должны быть реализованы на базе шлюзов, предоставляемых Заказчиком. При необходимости описание протоколов взаимодействия с почтовым шлюзом и SMS-шлюзом Заказчика могут быть предоставлены по запросу участника закупочной процедуры.

4.3.4 Интеграция с серверами Push-уведомлений

Функции отправки Push-уведомлений должны быть реализованы на базе публичных шлюзов, поддерживаемых компаниями Apple и Google.

5 Состав и содержание работ по доработке программных средств

5.1 Разработка промышленного комплекса программных средств «Умный дом»

Целевое решение должно быть разработано на основе опытного образца комплекса программных средств «О7.Умный Дом». Целевое решение должно выполнять функции, необходимые для пилотного запуска коммерческой эксплуатации решения.

Должны быть выполнены необходимые интеграции с системами ПАО «Ростелеком».

В качестве технологической платформы должна быть использована НОП ПАО «Ростелеком». При интеграции с НОП должны также быть выполнены доработки НОП, необходимые для запуска целевого решения сервиса «Умный Дом».

Пользовательские интерфейсы целевого решения должны дорабатываться с учетом концепции и стилистики опытного образца веб-сервиса «О7.Умный дом». При необходимости может быть выполнен редизайн интерфейсов промышленного решения:

- Изменения в дизайне веб-интерфейса должны быть согласованы с Заказчиком;
- В части мобильного приложения должен быть разработан дизайн и техническое задание для мобильного приложения Умный дом.

При проведении редизайна интерфейсов, состав и содержание конкретных страниц и разделов интерфейсов, приведенный разделе 4 «Требования к системе», может быть изменен на этапе технического проектирования с целью повышения удобства, эргономичности и эффективности интерфейсов.

5.1.1 Требования к поддержке процессов провиженинга и биллинга услуги «Умный дом»

Исполнитель должен разработать API для провиженинга и биллинга ресурсов со следующими функциями:

- Создание/удаление тенанта;
- Блокировка/разблокировка тенанта;
- Получение списка тенантов;
- Получение информации о тенанте (о его конфигурации и состоянии).

5.1.2 Требования к доработке подсистемы уведомлений

При промышленной эксплуатации КПС, в том числе и в период реализации пилотного проекта отправка сообщений электронной почты и смс-сообщений должна выполняться через промышленные шлюзы Заказчика. КПС должен обеспечивать возможность отправки уведомлений пользователям при помощи следующих сервисов доставки сообщений:

- Сервис Push-уведомлений;
- Сервис SMS-уведомлений;
- Сервис отправки email.

5.1.3 Требования к доработке подсистемы видеонаблюдения

Должно быть выполнено изменение реализации подсистемы видеонаблюдения КПС. Для обеспечения функций видеонаблюдения должна быть обеспечена возможность подключения внешней системы видеонаблюдения через API.

Подсистема видеонаблюдения платформы Умный дом должна обеспечивать с API системы видеонаблюдения:

- Подключение опции видеонаблюдения;
- Единую авторизацию абонентов через Интерфейс продукта;
- регистрацию абонентского видео-оборудования (IP камеры) в профиле пользователя на платформе Умный дом;
- сохранение получаемого с абонентского оборудования видеопотока;
- просмотр видеопотока в режиме реального времени;
- Доступ к архивам записей с помощью удобного навигатора (календарь);
- Выгрузка видеоматериала на устройство клиента в популярных форматах;
- Сохранение отдельных кадров видеоматериала на устройство клиента;
- Анализ движения и освещенности, уведомление о движении.

Внешняя система, реализующая функции видеонаблюдения и предоставляющая API, предоставляется Заказчиком.

5.1.4 Требования к доработке подсистема взаимодействия с управляющим контроллером

Подсистема взаимодействия с управляющим контроллером должна быть доработана с учетом следующих требований:

- Должна быть проработана схема безопасного взаимодействия контроллеров и мобильных устройств с API, реализованы методы аутентификации и авторизации при вызове API;
- Должен быть разработан открытый API, обеспечивающий возможность интеграции КПС с оборудованием широкого круга сторонних производителей контроллеров и сервисов, а именно:
  - В описании API не должно быть требований о полном или частичном использовании закрытых протоколов (кроме протокола Z-Wave);
  - Описание API должно быть независимо от каких-либо аппаратных решений (за исключением радио-модуля Z-Wave).
- Подсистема взаимодействия с управляющим контроллером должна быть доработана с учетом требований указанного выше API контроллера.

5.1.5 Требования к доработке веб-интерфейсов

Веб-интерфейсы КПС должны быть доработаны с учетом следующих требований:

- Должно быть реализовано взаимодействие по протоколу HTTPS
- При запросе к API по протоколу HTTP веб-сервер КПС выполняет http-редирект на аналогичный URL, но с протоколом HTTPS.
- Для аутентификации и авторизации при работе HTTP(s) REST API должны использоваться данные из ЕЛК, кроме пароля.

5.2 Доработка мобильных приложений

В состав работ, выполняемых по Договору, входит разработка макетов мобильных приложений, а так же разработка технического задания на разработку мобильных приложений.

Разработка мобильных приложений не входит в состав работ по Договору.

5.3 Требования к интеграции с НОП

КПС должен обладать API для провиженинга услуги «Умный дом»:

- Создание/удаление тенанта;
- Блокировка/разблокировка тенанта;
- Получение списка тенантов;
- Получение информации о тенанте (о его конфигурации и состоянии).

5.4 Доработка НОП

5.4.1 Поддержка процессов для пользователей услуги «Умный дом»

В НОП должна быть добавлена поддержка учетных записей пользователей услуги «Умный дом». Для поддержки процессов, связанных с предоставлением услуги «Умный дом», необходимо реализовать в НОП следующие функциональные возможности:

- Создание/удаление профиля абонента физического лица;
- Блокировка/разблокировка профиля абонента физического лица;
- Создание/удаление связи профиля в НОП с профилем в ЕЛК;
- Создание/удаление связи профиля в НОП с лицевыми счетами в АСР;
- Авторизация пользователя по логину и паролю в КПС;
- Подключение/отключение пользователю услуги «Умный дом»;
- Блокировка/разблокировка пользователю услуги «Умный дом».

5.4.2 Требования тарификации

Для тарификации должна использоваться модель тарификации, аналогичная предоставлению облачных услуг НОП, использующим кредитный метод оплаты.

Должна быть реализована схема покупки пользователем пакетов SMS-уведомлений, аналогичная существующей в НОП. Купленные пакеты SMS-уведомлений должны тарифицироваться по схеме разового платежа.

Стоимость услуги УД должна рассчитываться исходя из следующих параметров:

- Абонентская плата за сутки за использование услуги;
- Сумма стоимостей используемых Пользователем ресурсов за сутки.

Примером тарифицируемых ресурсов могут являться:

- Количество подключенных контроллеров;

- Количество сценариев автоматизации;
- Количество подключенных датчиков.

5.4.3 Требования к интеграции

5.4.3.1 Общая архитектура решения по интеграции ЕИП

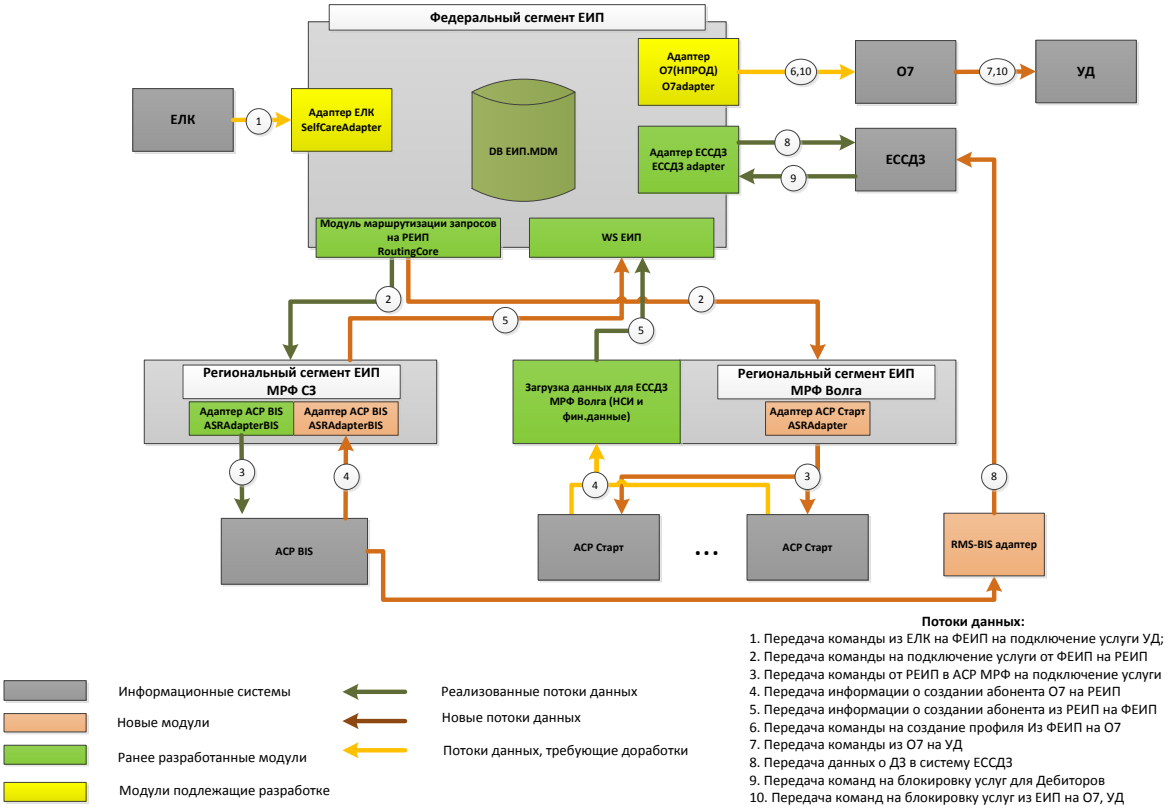
На данный момент в ЕИП разработано интеграционное решение (ИР) «Программы лояльности», которое позволяет подключать услуги в АСР в обмен на бонусные баллы, накопленные абонентом.

На данный момент разработан функционал по загрузке информации об изменении абонентской картотеки и функционал по управлению услугами в НОП по юридическим лицам.

На данный момент для системы ЕССДЗ реализован функционал по загрузке информации для расчета задолженности, выполнения работ с дебиторами и формирования команд для автоматического обзвона, блокировки/разблокировки услуг.

Реализация процессов, связанных с предоставлением услуги «Умный дом», предполагается с использованием ранее разработанного функционала.

Рисунок 3. Схема интеграции ЕИП с поддержкой работы с дебиторами



Запрос на подключение услуги поступает от ЕЛК и трансформируется модулем «адаптер ЕЛК» во внутреннюю модель данных ЕИП. Создается заявка на отправку данных в региональные системы. Заявка поступает в модуль маршрутизации и далее обработка происходит аналогично действующему функционалу ИР «Программы лояльности». Из АСР МРФ в ФЕИП.MDM через РЕИП поступает информация о подключении услуги, аналогично, как это реализовано при создании профиля на О7 для юридических лиц. Далее на О7 создается профиль и подключается услуга «Умный дом». Параллельно производится взаимодействие с системой ЕССДЗ в части планов работ с дебиторами и управления услуг. При возникновении задолженности и при переходе на стадию блокировки услуг в ЕССДЗ через ЕИП на О7 отправляются команды на блокировку профиля. Соответственно, при поступлении платежей, закрывающих задолженность у клиента, отправляются команды на разблокировку профиля на О7.

Описание API для взаимодействия НОП с ЕИП может быть предоставлено по запросу участника закупочной процедуры.

5.4.3.2 Требования к интеграции с сервисом «Умный дом»

В части интеграции целевого решения сервиса «Умный дом» с НОП должны быть реализованы следующие функции:

- провиженинг сервиса «Умный Дом»;
- тарификация доработанного сервиса, согласно существующему механизму интеграции облачных сервисов, НОП и АСР (в результате интеграции в АСР должны передаваться файлы в формате, описанном в разделе Приложение А).

6 Состав и содержание работ по развертыванию

6.1 Требования к выполнению развертывания на инфраструктуре Заказчика

КПС должен быть развернут на виртуальных серверах в НОП ПАО «Ростелеком». При развертывании должно быть развернуто 2 экземпляра решения:

- Тестовая среда, интегрированная с тестовой средой НОП;
- Промышленная среда, интегрированная с промышленной средой НОП.

Опытная эксплуатация Системы должна проводиться на экземпляре, развернутом в НОП.

Развертывание решения должно производиться с использованием системы контроля конфигураций НОП, должны быть разработаны сценарии развертывания для системы контроля конфигураций.

При разработке решения должен использоваться итеративный подход с передачей промежуточных результатов в виде Релизов ПО. Релизы ПО должны сопровождаться описанием по форме описанной в разделе Приложение Б.

Виртуальная инфраструктура предоставляется Заказчиком.

7 Порядок контроля и приемки

7.1 Предварительные испытания

Предварительные испытания проводятся согласно разработанной Программы и методики испытаний. По результатам предварительных испытаний составляется протокол проведения предварительных испытаний.

7.2 Опытная эксплуатация

Опытная эксплуатация проводится с целью проверки работоспособности сервиса в реальных (либо приближенным к реальным) условиях эксплуатации. Определяются количественные и качественные характеристики сервиса, готовность персонала к работе с сервисом, при необходимости корректируется документация.

По завершению опытной эксплуатации оформляется отчет о проведении опытной эксплуатации.

В процессе опытной эксплуатации могут быть выявлены замечания, которые отражаются в отчете о проведении опытной эксплуатации и должны быть исправлены Исполнителем на этапе Опытной эксплуатации.

Решение о возможности проведения приемо-сдаточных испытаний принимается только в том случае, когда по результатам опытной эксплуатации представители рабочей группы подтверждают работоспособность сервиса в реальных (либо приближенным к реальным) условиях эксплуатации, а также соответствие разработанной системы требованиям проектной документации.

7.3 Приемо-сдаточные испытания

На приемо-сдаточных испытаниях оцениваются результаты опытной эксплуатации.

Приемо-сдаточные испытания проводятся на площадке в г. Москва.

Испытания проводится согласно Программе и методике приемо-сдаточных испытаний, разработанной в рамках работ по проектированию и согласованной с Заказчиком.

В случае нарушения заявленной функциональности, испытания прерываются с оформлением соответствующего протокола. Исполнитель примет меры по устранению выявленных несоответствий. После устранения неисправностей/неточностей в реализации решения, испытания повторяются. В случае отсутствия замечаний в Протоколе и достижении характеристик, описанных в Программе и методике приемо-сдаточных испытаний составляется Акт о проведении приемо-сдаточных испытаний и сдачи-приемки выполненных работ.

8 Гарантийная поддержка

Исполнитель должен предоставить доступ к службе поддержки пользователей, а также доступ к персоналу, ответственному за работу с клиентами, для сообщения информации о неисправностях в системе и получения помощи по использованию системы по электронной почте.

Исправление Исполнителем ошибок в работе сервисов, а также функциональных расширений по мере их появления (время реагирования определяется степенью критичности ошибки и составляет от 1 до 5 рабочих дней дней). Исправление ошибок осуществляется в сроки, не ниже следующих:

Вид запроса	**Максимальное допустимое время устранения инцидента, в зависимости от приоритета**		
	Критичный	**Высокий**	**Стандартный**
Инцидент	1 рабочий день	3 рабочих дня	5 рабочих дней

Приём запросов в техническую поддержку должен осуществляться Исполнителем круглосуточно, 24 часа в сутки, 7 дней в неделю.

Приоритет - критерий важности и срочности решения инцидента, с учётом влияния, оказываемого на пользователей ИС. В ходе эксплуатации Сервиса, должны быть выделены не менее 3-х типов приоритетов для возникающих инцидентов.

Приоритет инцидента	**Описание**
1-го приоритета (Критичный)	Аварийная внештатная ситуация, связанная с полной или частичной потерей более 50% функционала работоспособности сервиса
2-го приоритета (Высокий)	Частичная потеря работоспособности ПО, не приводящая к потере критичного (основного) функционала, возможны альтернативные варианты выполнения основных функций сервиса
3-го приоритета (Стандартный)	Снижение производительности, не приводящие к потере функциональности Сервиса

Срок гарантийной поддержки: 1 год с момента выполнения обязательств по выполнению работ (определяется датой подписания акта сдачи-приемки).

9 Требования к программной документации

9.1 Требования к составу документации

В рамках выполнения работ должны быть разработаны следующие документы:

- Комплект документов технического проекта, в составе:
  - Ведомость технического проекта;
  - Пояснительная записка;
- Комплект документов эксплуатационной документации, в составе:
  - Руководство пользователя;
  - Руководство администратора;
  - Методика масштабирования КПС при увеличении нагрузки свыше до 72 000 пользователей;
- Программа и методика испытаний;
- Протокол проведения предварительных испытаний;
- Отчет о проведении опытной эксплуатации;
- Протокол проведения приемо-сдаточных испытаний;
- Исходные коды КПС, исключительные права на использование, доработку, продажу доработанной системы должны быть переданы Заказчику,
- Исходные коды НОП.

9.2 Требования к оформлению

Вся разрабатываемая документация должна быть на русском языке. Исключения допускаются для общепринятых терминов и аббревиатур.

Проектная и рабочая документация должна разрабатываться с учетом требований комплекса государственных стандартов «Информационная технология. Комплекс стандартов на автоматизированные системы»:

- ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»;
- ГОСТ 34.003-90 «Автоматизированные системы. Термины и определения»;
- ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.603-92 «Виды испытаний автоматизированных систем»;
- РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»;
- ГОСТ 19.301-79 «Программа и методика испытаний. Требования к содержанию и оформлению»;
- ГОСТ 2.601-2006 «ЕСКД. Эксплуатационные документы»;
- ГОСТ 2.106-96 «ЕСКД. Текстовые документы» (с изменениями от 22 июня 2006 года);
- ГОСТ 2.120-73 «ЕСКД. Технический проект» (с изменениями от 22 июня 2006 года).

Разрабатываемая документация должна соответствовать следующим требованиям:

- язык отчетных материалов – русский;

– отчетные материалы должны быть представлены на бумажном носителе и в электронной форме;

– отчетные материалы на бумажном носителе должны быть оформлены на листах формата А4 и А3;

– номера листов (страниц) должны быть проставлены, начиная с первого листа, следующего за титульным листом, в верхней части листа (над текстом, посередине);

– на титульном листе должно быть помещено наименование отчетного материала, учетные реквизиты, подписи Исполнителя и Соисполнителей, скрепленные печатями;

– отчетные материалы в электронном виде должны быть представлены на оптическом диске, исключающем возможность изменения информации (CD-R, DVD-R, DVD+R);

– форматы представления информации в электронном виде – doc, rtf, vsd, ppt, xml.

Представляемые в составе отчетных материалов оптические диски должны быть помещены в защитные коробки или бумажные конверты. Защитные коробки или бумажные конверты должны быть промаркированы несмываемыми водой фломастерами или наклейками.

Отчетная документация должна прилагаться в бумажном и электронном виде (на оптическом CD или DVD носителе) на русском языке. Вспомогательная документация (не указанная в качестве непосредственного результата работ) должна передаваться только в электронном виде.

10 Требования к Исполнителю

10.1 Требования к квалификации Исполнителя

10.1.1 Квалификация в области разработки средств защиты информации

В процессе разработки Исполнитель должен обеспечить защиту персональных данных пользователей Услуги. На основании постановления Правительства Российской Федерации от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" Исполнитель должен обладать лицензией ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации.

10.1.2 Квалификация в области технической защиты информации

В процессе развертывания КПС Исполнитель должен обеспечить защиту персональных данных пользователей Услуги. На основании постановления Правительства Российской Федерации от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" Исполнитель должен обладать лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации.

10.1.3 Квалификация в области разработки криптографических средств

В процессе разработки Исполнитель должен выполнить работы по оценке необходимости и возможности применения в системе средств криптографической защиты данных по ГОСТ. На основании постановления Правительства Российской Федерации от 16 апреля 2012 г. N 313 Исполнитель должен обладать лицензией ФСБ России:

- лицензия ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

Приложение А

к Техническому заданию

Формат CDR

Описание формата CDR:

– файлы CDR должны записываться в формате CSV («comma separated values») с сепаратором полей «,» и записей (строк) hex («0D0A») (стандарт windows);

– каждая запись должна соответствовать формату BIZ+(L5);

– в каждой записи должны присутствовать все 48 полей (полное описание формата приведено в таблице «Описание полей CDR»).

Таблица 1 - Описание полей CDR

№ поля	Название поля	Описание поля	Тип содержимого
1	**2**	**4**	**5**
1	REC_TYPE	Тип записи Условный код типа УЗ. 15- разовые; 16- периодические; 17- трафиковые; 18 – прочие	Integer, not null
2	REC_NUMBER	Номер УЗ, позволяющий идентифицировать УЗ с коммутатора. Уникальный, инкрементируемый для всех CDR НОП	integer, not null
3	REC_STATUS	Статус частичной УЗ	Не заполняется
4	REC_SUB_NUMBER	Номер ЧУЗ	Не заполняется
5	IMSI	ID Клиента в АСР МРФ	string, not null
6	MSISDN	Идентификатор клиента. Номер лицевого счета	string, not null
7	DIALED	Логический B - номер вызываемого абонента, преобразованный к международному формату, за исключением услуг ИСС. B-номера на услуги ИСС представлены в виде 80 %. Пустое значение - недопустимо	Не заполняется

№ поля	Название поля	Описание поля	Тип содержимого
1	**2**	**4**	**5**
8	START_TIME	Дата и время начала периода оказания услуги, описываемого CDR в формате YYYYMMDDHH24MISS. Дата и время по г. Москве	string, not null. YYYYMMDDHH24MISS, utc + 3
9	DURATION	Продолжительность соединения (в секундах) или объем услуги. Целое, Integer (max 2E32). Нулевое значение недопустимо. Количество потребленной услуги	integer, not null
10	SUCCESS	Код причины завершения вызова	Не заполняется
11	DD_TYPE	Количество дней предоставления услуги	Не заполняется
12	CALL_TYPE	Размер объема услуги, представленной в поле 9 «DURATION» (штуки, Гигабайты, потоки и т.д.). Единицы измерения	string, not null
13	CALLING_NUMBER	Физический С-номер абонента, преобразованный к международному формату либо непреобразованный А-номер	Не заполняется
14	IMEI	ID Абонента в АСР МРФ	Не заполняется
15	MS_CLASS	ID профиля	Не заполняется
16	TYPE_1_SER	Тип основной услуги. ID основной услуги	integer, not null
17	CODE_1_SER	Код основной услуги. ID детализированной услуги	Не заполняется
18	TYPE_2_SER	Тип дополнительной услуги	Не заполняется
19	CODE_2_SER	Код дополнительной услуги	Не заполняется
20	A_AREA	Идентификатор Location Area абонента А. Идентификатор АСР МРФ	ID АСР МРФ, string, not null
21	A_CELL	Идентификатор ячейки абонента А	Не заполняется
22	B_AREA	Идентификатор Location Area абонента В	Не заполняется
23	B_CELL	Идентификатор ячейки абонента В	Не заполняется
24	ACTION	Поле кода управления услугой (Subscriber-controlled input)	Не заполняется

№ поля	Название поля	Описание поля	Тип содержимого
1	**2**	**4**	**5**
25	SERV_CODE	Действия со вспомогательной услугой	Не заполняется
26	REASON	Код причины переадресации	Не заполняется
27	CALLED_NUMBER	Реальный номер, с которым установлено соединение (в случае переадресации – номер, на который переадресован вызов). Непреобразованный номер B. Значение null- недопустимо	Не заполняется
28	SUBS_CODE	Код коллективного пользователя	Не заполняется
29	PASSWORD	Признак предоставления связи через пароль	Не заполняется
30	INST_ID	Условный номер МРФ, в котором производятся расчеты с Клиентом	Значение INST_ID, представленное в Таблице 1. String, not null
31	CIRCUIT_IN	Номер (мнемоника) входящего транка	Не заполняется
32	CIRCUIT_OUT	Номер (мнемоника) исходящего транка	Не заполняется
33	MSC_ID_LONG	Номер (ID) первого коммутатора	Не заполняется
34	GLUING_STATUS	Поле характеризует режим склейки для длинной УЗ	Не заполняется
35	A_NUMBER_LONG	Физический номер абонента А из УЗ последнего коммутатора	Не заполняется
36	CIRCUIT_IN_LONG	Входящий транк из УЗ последнего коммутатора. Поле заполняется для склеенной УЗ	Не заполняется
37	CIRCUIT_OUT_LONG	Исходящий транк из УЗ первого коммутатора. Поле заполняется для склеенной УЗ	Не заполняется
38	MSC_ID	Номер (ID) коммутатора	150
39	Source IP	IP-адрес источника вызова	Не заполняется
40	Destination IP	IP-адрес точки терминации вызова	Не заполняется
41	UDF	Пользовательское поле. Название основной/детализированной услуги (текст)	String, not null
42	A_category	Категория абонента А	Не заполняется

№ поля	Название поля	Описание поля	Тип содержимого
1	**2**	**4**	**5**
43	B_subsc_type	Тип вызываемого абонента	Не заполняется
44	PPIMARY_ID	Уникальный идентификатор звонка.	Не заполняется
45	A_type	Тип поля 46	Не заполняется
46	T_klass	Идентификатор тарифного класса, применяемого для данной услуги	String, not null
47	Trial_period	Признак триального периода	0 – не триальный, 1 - триальный
48	Reserved		Не заполняется

Приложение Б

к Техническому заданию

Форма описания релиза

Релиз СУ НОП _____

Тип релиза: изменение / исправление ошибок.

Финализация релиза _____

Среда тестирования: _____

Список изменений

№	Номер задачи (СКУФ, при наличии)	Краткое описание функциональности/дефекта	Тип изменения (разработка/доработка/ исправление ошибок)

План установки релиза:

1) Прерывание сервиса: _____.
2) Выполнение SQL-скриптов: _____.
3) Обновление кода: _____.
4) Влияние на компоненты системы (смежные системы): _____.
5) Дистрибутив: <ссылка на репозиторий>.

Порядок действий:

1) Действие 1;
2) Действие 2 и т.д.;

Не стандартные изменения:

1) Изменение 1;
2) Изменение 2 и т.д.;

План отката:

1) Действие 1;
2) Действие 2 и т.д.;