**АО РТКомм.Ру**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**На разработку Автоматизированного рабочего места**

**по контролю за SIM картами (АРМ MultiSimBox)**

**Глоссарий**

|  |  |
| --- | --- |
| Понятие | Определение |
| АРМ MultiSimBox | Автоматизированное рабочее место по контролю за SIM картами – предмет договора |
| Заказчик | АО РТКомм.Ру (РТКОММ) |
| Исполнитель | Победитель конкурса на разработку АРМ MultiSimBox |
| Клиент | Клиент АО РТКомм.Ру, которому предоставляется услуга связи, у которого установлено оборудование, использующее SIM карту(ы) для организации канала связи |
| Объект | Территориально отделенный объект Клиента, на котором Заказчик устанавливает оборудование для предоставления услуг связи |
| Канал связи | Неотъемлемая часть предоставляемых услуг связи Клиентам на Объектах |
| Сим-карта (SIM) | идентификационный электронный модуль абонента, применяемый в мобильной связи |
| API | Application Programming Interface (набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) для использования во внешних программных продуктах) |
| ЛК | Личный кабинет |
| ЗО | Зона ответственности |
| ICCID | (integrated circuit card identifier) — уникальный серийный номер SIM-карты |
| DEF номер | телефонный код, присвоенный по негеографическому признаку, например, по признаку оператора связи. Чаще всего употребляется для обозначения телефонных номеров сотовой связи. |
| IMEI | International Mobile Equipment Identity — международный идентификатор мобильного оборудования |
| DaData | Сервис нормализации адресов |
| DHS | (data house system) – сервер для промежуточного хранения информации |
| UI | (user interface) — пользовательский интерфейс: все кнопки, таблички, поля ввода текста и другие способы взаимодействия пользователя с сайтом. приложением или иным IT-сервисом |
| Мобильные операторы | Операторы сотовой связи куда входят бренды Мегафон, МТС, Билайн, Ростелеком Теле2. |
| BDO | База данных MS-SQL, расположенная во внутренней сети РТКомм.Ру. на сервере DHS |
| Внутренний API клиент | Приложение, сервис, который получает данные от АРМ MultiSimBox посредством API. |

## Цель создания АРМ MultiSimBox:

* 1. Организация рабочего места, позволяющего в едином месте получать информацию и отдавать команды по SIM картах Заказчика в режиме on-line.
  2. Создание Аналитического блока, который позволит пользователям формировать правила по автоматическому изменению статуса SIM исходя полученных данных из различных источников.
  3. Создания конструктора отчетов, который позволит сотрудникам Заказчика самостоятельно создавать Типы отчетов.
  4. Коммуницировать с иными программами посредством API.

## Исполнитель должен выполнить следующие работы:

## Разработка АРМ MultiSimBox в соответствии с требованиями данного Технического задания.

## Тестирование и ввод в эксплуатацию.

## Обучение сотрудников и администратора Заказчика.

## Подготовка документации по АРМ MultiSimBox.

## Поддержка АРМ MultiSimBox в период действия гарантийного срока.

## Общее назначение платформы

## Обеспечить аутентификацию пользователя, для доступа к платформе.

## Обеспечить предоставление контента аутентифицированному пользователю в соответствии с группой, в которую он включен.

* 1. Обеспечить работу аналитического блока на постоянной основе без участия пользователя, согласно правилам, которые были в него заложены.
  2. Обеспечить оперативное информирование пользователей, посредством e-mail.

## Обеспечить возможность создания пользовательского контента без использования программирования, путем визуального конструирования.

## Предоставить административный интерфейс для управления платформой.

## Предоставить API для взаимодействия с платформой.

## Базовые требования

Платформа должна строиться с использованием Стека:

* Операционная система – Linux;
* База данных – PostgressPro;
* Back-end – технологии на основе решений, распространяемых с открытым исходным кодом, используя технологию интерпретации. Также допускается программное обеспечение, входящее в «Единый реестр российских программ для электронных вычислительных машин и баз данных» (https://reestr.digital.gov.ru/reestr/)
* Font-end - технологии на основе решений, распространяемых с открытым исходным кодом, используя технологию интерпретации. Также допускается программное обеспечение, входящие в «Единый реестр российских программ для электронных вычислительных машин и баз данных» (https://reestr.digital.gov.ru/reestr/)

Платформа должна поддерживать интерфейсы удаленного управления и конфигурирования. При организации удаленного доступа должны использоваться протоколы с применением алгоритмов шифрования (https, ssh и т.д.).

Необходимо использовать подход кроссбраузерности и адаптивности интерфейсов.

Исполнитель предлагает дизайн, архитектуру, платформу АРМ MultiSimBox в рамках настоящего технического задания и согласовывает их с Заказчиком. Платформа функционирует на мощностях Заказчика.

## Требования к масштабируемости

* 1. Платформа должна позволять обрабатывать до 1000000 SIM-карт.
  2. Платформа должна позволять Администраторам Заказчика подключать API иных мобильных операторов.

## Бизнес-требования

* 1. **Перечень базовых функций «АРМ MultiSimBox»**

|  |  |  |
| --- | --- | --- |
| **#** | **Функция** | **Описание** |
| 1. | Регистрация пользователя | Регистрация на платформе для получения логина и пароля от АРМ MultiSimBox. |
| 2. | Аутентификация пользователя | Аутентификация должна поддерживать как локальные учетные записи, так и записи в AD. |
| 3. | Авторизация пользователя | Выдача прав должна выдаваться на основе ролевой политики. |
| 4. | Логирование техническое | Сбор технической статистики по использованию АРМ MultiSimBox (время отклика, доступность, размер БД и т.д.) с иcпользованием протокола и службы syslog. |
| 5. | Логирование пользовательское | Сбор информации по деятельности пользователей в АРМ MultiSimBox. |
| 6. | Получение информации по SIM | Получение информации по SIM картам согласно выданных прав. |
| 7. | Изменение информации по SIM | Изменение информации по SIM картам согласно выданных прав, с последующей отправкой данных в ЛК Мобильного оператора. |
| 8. | Внесение дополнительной информации | Возможность внесение дополнительной информации в структурированные поля в разрезе каждой SIM. |
| 9. | Создание правил автоматических действий | Возможность создание правил по автоматическим действиям, при наступлении условий, которых Аналитический блок производит заложенные действия. |
| 10. | Формирование отчетов | Формирование отчетов как заранее сконфигурированных, так и созданных при помощи конструктора. |
| 11. | Уведомления | Процесс сообщения пользователям о событиях |

* 1. **Функциональные требования (сопровождение АРМ MultiSimBox):**
     1. Блок управления пользователями, группами, правами:
        1. **Группы пользователей:** Пользователи делятся на группы.
           + Первая группа – «Администраторы» – имеет неограниченные права, доступ в панель настроек, отправку уведомлений.
           + Вторая группа - «Старший оператор SIM» -имеет полный доступ ко всем SIM картам как на чтение, так и на внесение изменение. Может осуществлять выгрузку отчетов, читать и редактировать правила в блоке аналитики.
           + Третья группа – «Оператор SIM» имеет полный доступ ко всем SIM картам как на чтение, так и на внесение изменение. Может осуществлять выгрузку отчетов, читать правила в блоке аналитики.
           + Четвертая группа – «Пользователи». имеет доступ на чтение ко всем SIM. Может осуществлять выгрузку отчетов.
           + Четвертая группа – «Гости» (по умолчанию деактивирована).

Группы применяются – при заведении пользователей, при распределении выездов и отправке почтовых уведомлений.

Должна быть возможность добавлять/удалять группы.

В свойствах групп должны быть следующие возможности:

* Активировать/деактивировать группу;
* Добавлять/убирать отдельные права;
* Добавлять/удалять отдельных пользователей;

* + - 1. **Распределение прав по ролям:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Администратор АРМ MultiSimBox | Старший оператор SIM | Оператор SIM | Пользователь | Гость |
| Регистрация пользователей | + | - | - | - | - |
| Прикрепление пользователя к группе | + | - | - | - | - |
| Редактирование групп | + | - | - | - | - |
| Доступ к SIM на изменение (API) | + | + | + | - | - |
| Доступ к Заявкам | + | + | + | - | - |
| Доступ к SIM на чтение | + | + | + | + | - |
| Доступ к Аналитическому блоку на изменение | + | + | - | - | - |
| Доступ к Аналитическому блоку на чтение | + | + | + | - | - |
| Доступ к отчетам на изменение | + | + | - | - | - |
| Доступ к отчетам на чтение | + | + | + | + | - |

* + - 1. **Регистрация пользователей этапы:**

Регистрация производится через ручное заведение Администратором учетной записи пользователя с заполнение обязательных полей:

* + - * + Типа аутентификации локальное/LDAP.
        + Логин.
        + Пароль (если выбран тип LDAP поле неактивно).
        + E-mail.
        + Группа пользователей.
    1. **Логирование:** в системе ведется запись событий, позволяющее оперативно ответить на вопросы состояния системы и процессы, происходящие в ней. Логирование содержит следующие виды:
       1. Техническое – используя внутренние ресурсы ОС Linux логирование организованно с использованием протокола и демона syslog, где фиксируются данные, которые используются АРМ MultiSimBox.
       2. Пользовательское – в платформе организована возможность видеть какие действия производит сотрудник с обязательными полями:
* - дата время события;
* - под какой учетной записью производились действия;
* - тип действия (создание, удаление, изменение);
* - объект над которым производились действия;
  + 1. **Получение/ передача информации по SIM:** основывается на получении информации АРМ MultiSimBox от следующих источников информации:
       1. Личные кабинетов Мобильных операторов (API):
          - ICCID;
          - Статус SIM
          - Дата активации/деактивации;
          - Def номер;
          - IMEI модема через который передает SIM;
          - Геопозиция последнего расположения SIM;
          - Тариф SIM карты;
          - Израсходованный траффик за прошедшие сутки;
       2. ZABBIX(API):
          - Нostname;
          - Модель оборудования;
          - Серийный номер оборудования;
          - IMEI модема(ов) в оборудовании;
          - ICCID работающих SIM
       3. BDO (T-SQL)
          - Id клиента;
          - Наименование клиента;
          - Номер объекта;
          - Статус объекта;
          - Адрес предоставления услуги (DaData);
          - Геопозиция адреса предоставления услуги;
          - Модель оборудования, установленного на объекте;
          - ICCID SIM карт установленных на объекте;
          - Статус SIM;
          - Дата активации/деактивации;
       4. Периодичность опроса (синхронизации) каждого источника информации настраивается в административной панели приложения и имеет диапазон от 1 до 24 часов.
       5. Описание API каждого мобильного оператора находится в прилагаемых файлах:
          - Описание API Мегафон
          - Описание API Ростелеком
          - Описание API MTC
          - Описание API Билайн (находится в ЛК Билайна)

После получения информации АРМ MultiSimBox складирует все в свою БД, для дальнейшего использования. В результате у пользователей АРМ появляется информация в разрезе отдельной сим карты:

* + - * + Мобильный оператор;
        + DEF номер;
        + ICCID;
        + Статус SIM
        + Объект, где установлено;
        + Статус объекта;
        + Модель оборудования;
        + Доступность оборудования;

Где в разрезе каждой SIM имеется возможность активировать/деактивировать (при наличии прав на операцию). Также вносить комментарии, информацию в дополнительные поля.

* + 1. **Управление SIM пользователями:** 
       1. Целевой метод управления (API): пользователь, обладающий надлежащими правами, может самостоятельно активировать/деактивировать SIM карту на панели описанной в п.7.4-2., данная кнопка присутствует если настроено взаимодействие по API между АРМ SIM и ЛК Мобильного оператора.
       2. Альтернативный метод управления (e-mail): альтернативный метод управления основан на переписке посредством электронной почты между диспетчером Мобильного оператора и пользователем АРМ SIM.
          - Процедура переписки: пользователь в АРМ SIM создает заявку на активацию/деактивацию/получение информации по сим-карте(ам) путем выбора:

Мобильного оператора куда уйдет запрос (АРМ SMR подставляет e-mail получателя);

типа запроса (АРМ SMR подставляет текст запроса);

создания корректировке темы и текста заявки;

множественного выбора обрабатываемых в заявке SIM;

возможность прикрепления файла(ов).

* + - * + Заявка формируется в электронное письмо с выбранными данными, а при необходимости файлы как вложение. К теме письма прикрепляется номер заявки для дальнейшей идентификации переписки.
        + Представитель Мобильного оператора отвечает на письмо куда вносит информацию по проделанным действиям.
        + Ответное письмо, содержащее в теме письма номер заявки, сортируется, и информация из ответа отображается в АРМ SIM в блоке (таким образом вся переписка по конкретной заявке собирается в едином месте).
        + Заявка имеет следующие статусы:

«Создана» - заявка создана, но не отправлена, имеется возможность редактировать заявку;

«Отправлена» - e-mail с заявкой отправлен Мобильному оператору, отсутствует возможность редактировать заявку;

«Закрыта» - работа над заявкой закончена, все необходимые данные получены, манипуляции проведены. В статус «Закрыта» заявка переводится в ручном режиме пользователем, обладающим нужными правами.

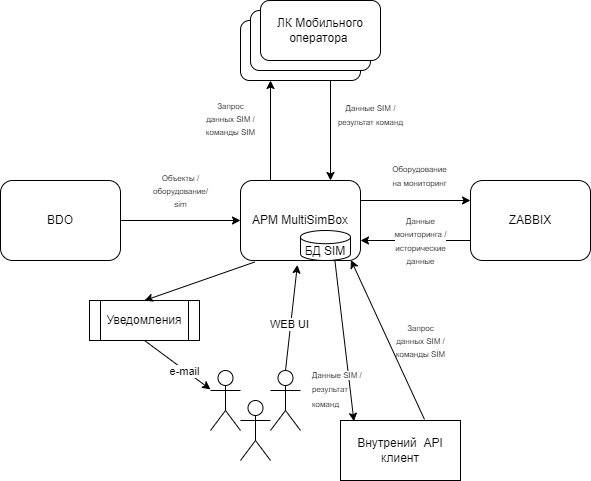
* + - * + В заявке должен быть блок «Комментарии», внесение информации в который также позволяет вести переписку с представителем Мобильного оператора посредством e-mail.
        + Информация о всех изменениях в заявке должна уходить через систему уведомлений пользователю, который эту заявку создал.
    1. **Аналитический блок:** блок, отвечающий за автоматическоевыполнение задач по заданным условиям.
       1. Поля у задачи:
          - Номер задачи;
          - Статус (активна/деактивирована);
          - Дата время начала действия задачи;
          - Периодичность выполнения задачи;
          - Дата время окончания действия задачи (если не заполнена, то бессрочно);
          - Наименование задачи;
          - Описание задачи;
          - Условие срабатывания триггера;
          - Действия при срабатывании триггера;
          - Отправка и получатели уведомлений;
          - Результат отработки отчёта (ОК/Error)

Если на шаге отбора и фильтрации информации происходит ошибка - блок активных действий не запускается.

* + - 1. Предустановленные задачи, периодичность каждые 24 часа, предварительно деактивированы:
         * Деактивация Активных SIM установленных на не рабочих объектах.
         * Деактивация Активных SIM у которых дата активации больше 25 дней с текущего момента и не прикреплены ни к какому объекту.
         * Деактивация Активных SIM ICCID IMIE модема которых отличается IMIE модема проданного оборудования.
         * Деактивация Активных SIM у которых геопозиция расположения SIM изменилась более чем на 1 км. (при работе от двух сотовых операторов правило срабатывает при логическом “И”) И статус объекта «Подключен».
    1. **Формирование отчетов**. В АРМ MultiSimBox должны быть ряд предустановленных отчетов. Формирование отчетов не должно ощутимо влиять на работоспособность системы, если выборка данных слишком большая, данное задание должно формироваться как «отсроченное» задание. Администратор может создавать новые отчеты используя SQL запросы.
       1. Предустановленные отчеты:
          - Агрегированные данные по израсходованному траффику за определённый период по определенному оператору, определенному тарифу.
          - Данные по израсходованному траффику за определённый период по определенному оператору, определенному тарифу в разрезе каждой sim.
    2. **Уведомления**: механизм дополнительно уведомления пользователей о событиях, происходящих в системе. Уведомления производятся через e-mail.
       1. Список событий для фиксации уведомлений:

Результат отработки правила в Аналитическом блоке.

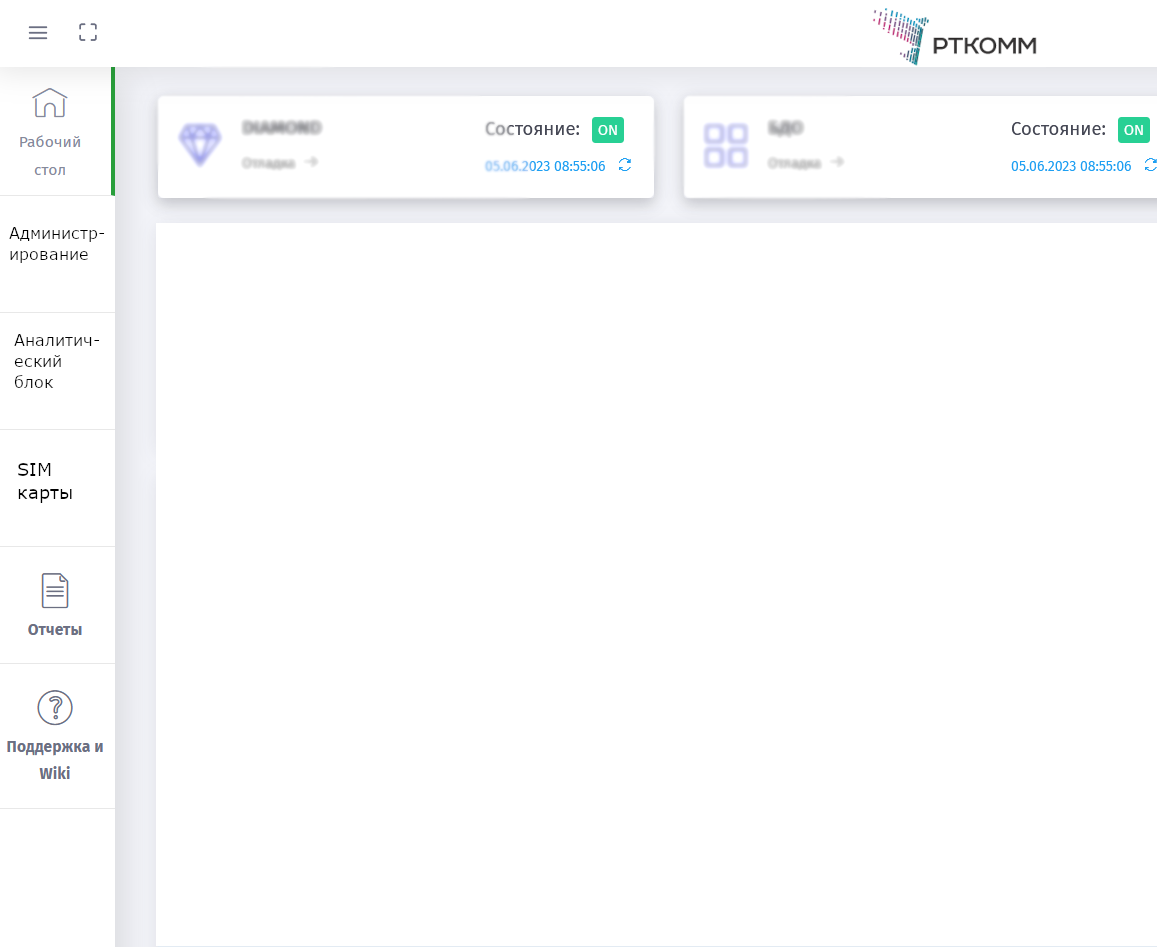
Новая информация в разрезе созданной заявки.

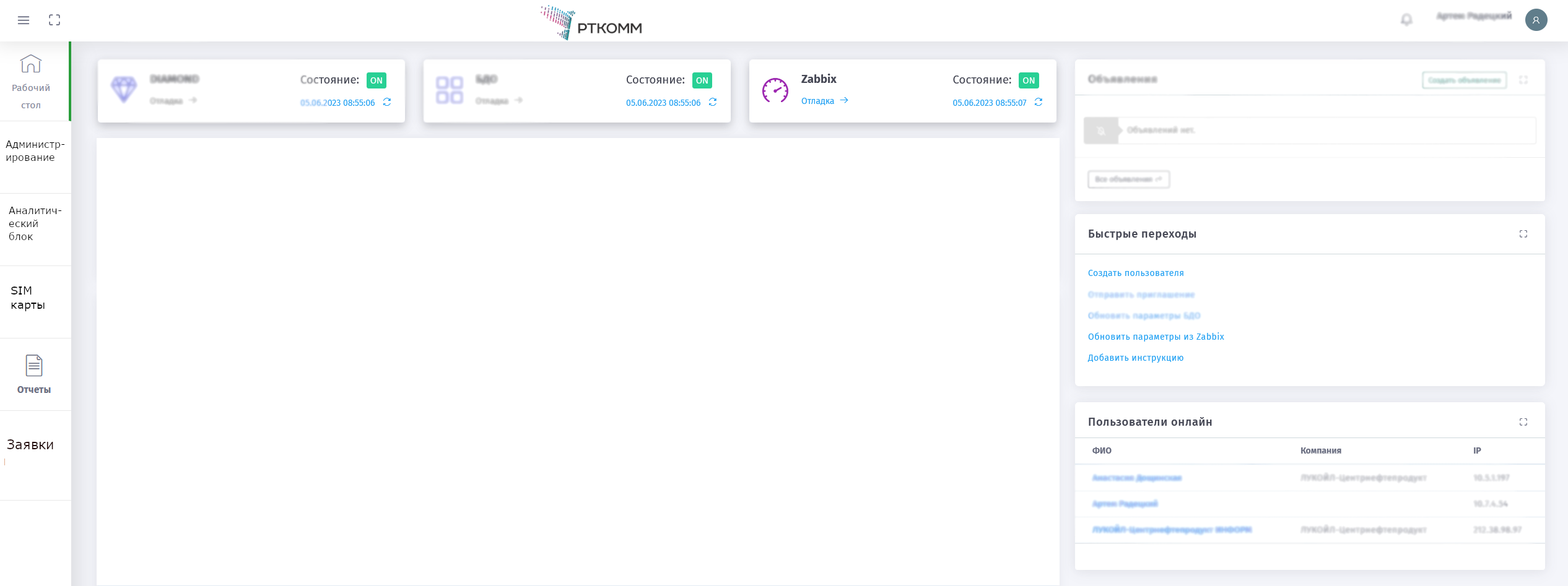
* + 1. **Входящие API запросы:** механизм с помощью которого иные программы могут получать данные в режиме on-line. Данный механизм должен отвечать следующим требованиям:
       1. Использовать интерфейс RESTful API с выдачей данных в формате json.
       2. Интерфейс RESTful API располагается на выделенным порту отличным от порта web интерфейса.
       3. Обеспечить аутентификацию методом «API ключ», позволяющей идентифицировать учетные данные, отправившие запрос.
       4. При получении входящего API запроса выдается ответ о результате обработке запроса.
       5. Использовать методы, позволяющие:
          - Получить текущий статус SIM;
          - Подать команду на активацию/деактивацию SIM;
  1. **Схема ИТ ресурсов**
  2. **Требования по настройке:** все конфигурационные и настроечные параметры должны быть вынесены в единый файл, для возможности тонкой настройки АРМ SIM без необходимости редактировать исходный код.

## Визуализация:

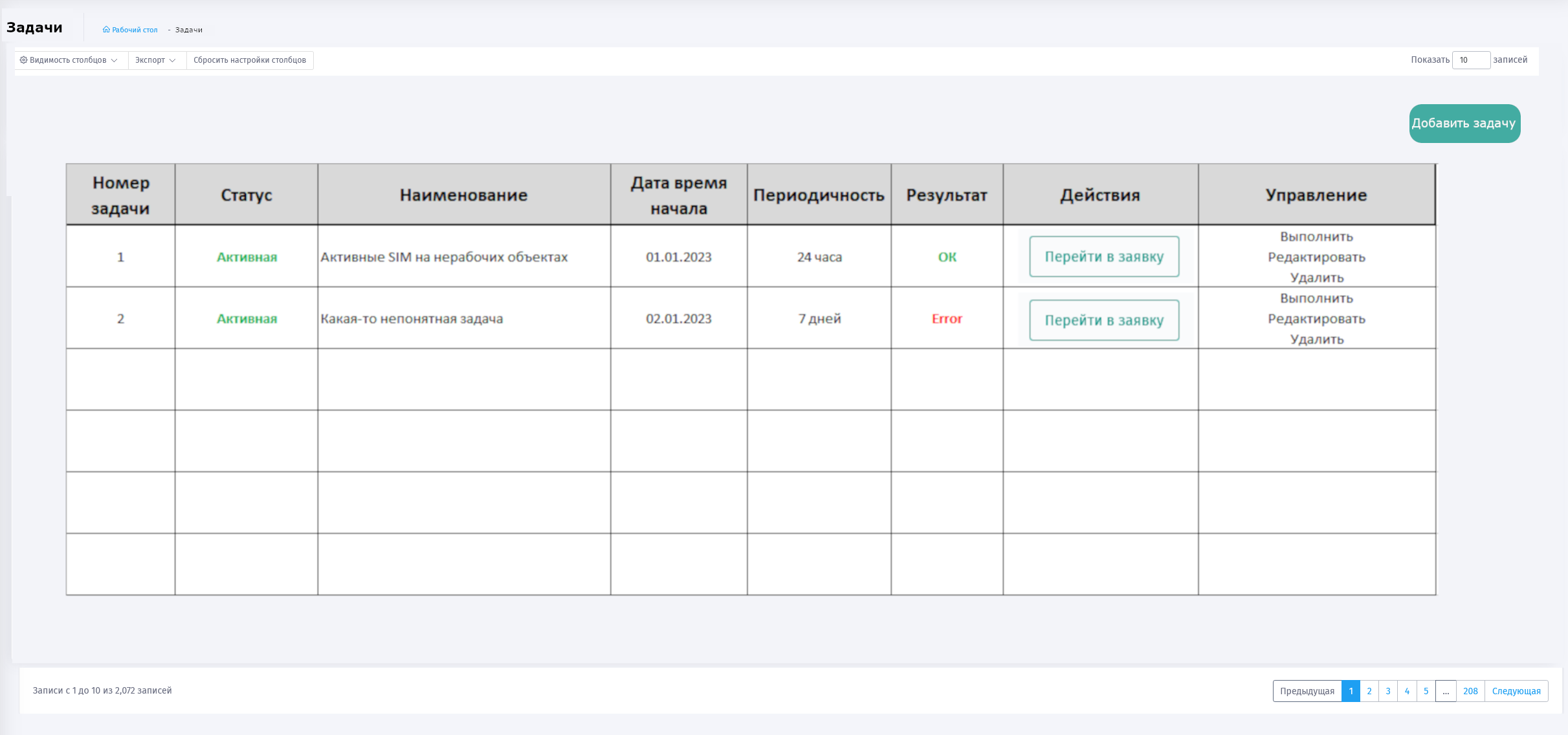
## Общий вид:

* + 1. Верхняя панель в АРМ MultiSimBox единая для всех и содержит в левой части кнопку скрывания меню и разворачивания во весь экран, в центре эмблему и слоган, в правой части наименование профиля пользователя.
    2. Левая часть содержит скрывающую панель, в которой отображаются пункты меню при наличии прав их использования у пользователя:
       1. Администрирование;
       2. Аналитический блок;
       3. Заявки
       4. SIM-карты;
       5. Отчеты;

*Визуальный пример:*

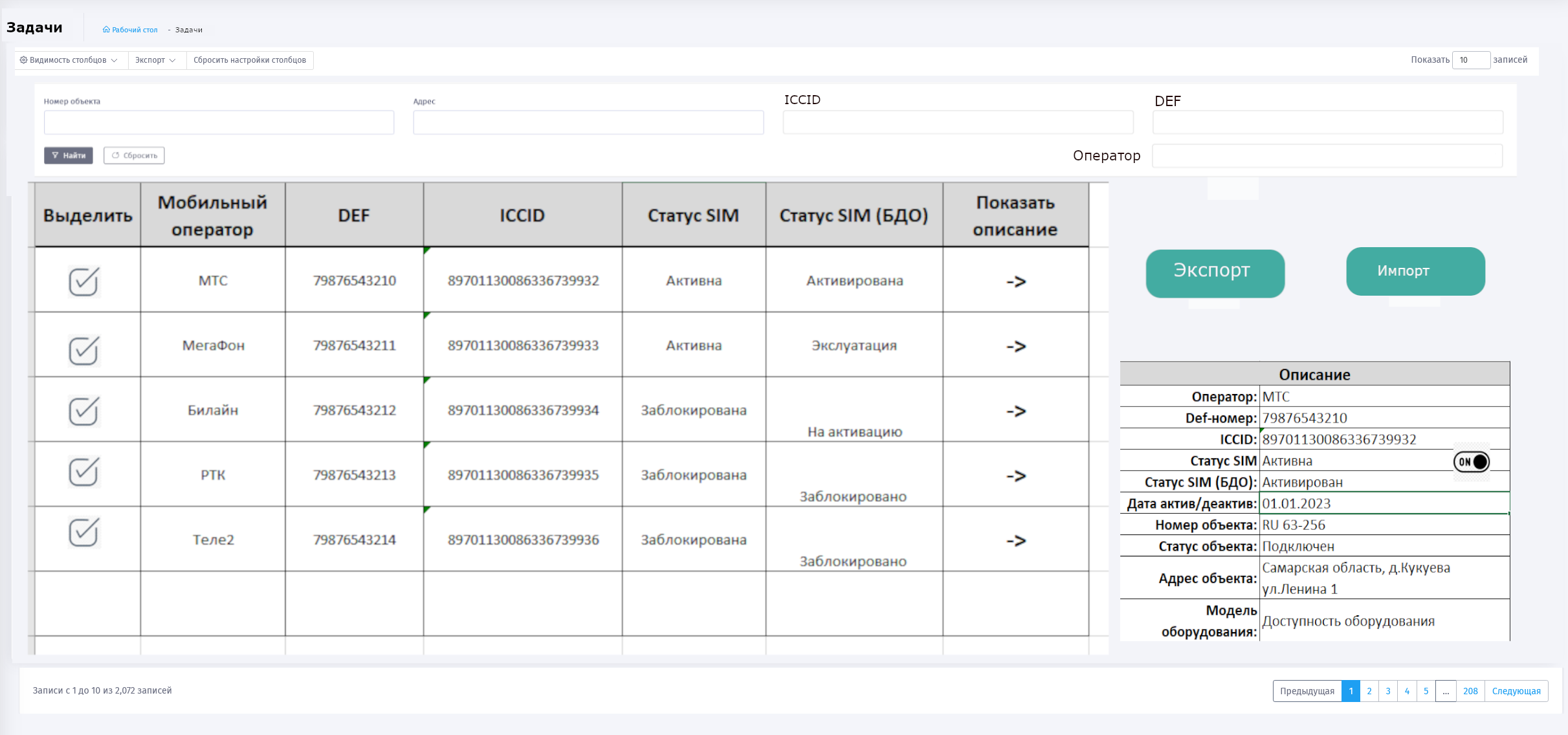
* 1. **Первоначальной страницей является** **Рабочий Стол (Dashboard)** который содержит определенную сжатую информацию.
     + 1. Рабочий Стол Администратора должен содержать блоки информации:
          - Состояние синхронизации с внешними системами;
          - Гиперссылки на часто используемые действия;
          - Лог действий пользователей (on-line);
          - Лог отработки задач Аналитического блока;
          - Панели настроек блоков, которые согласуют Исполнитель и Заказчик;
          - Иная информация, которую согласуют Исполнитель и Заказчик;
          - *******Визуальный пример:*
       2. Рабочий стол Пользователя должен содержать информацию в графическом виде:
          - Количество SIM-карт по мобильным операторам
          - Количество SIM-карт по статусам
          - Иная информация, которую согласуют Исполнитель и Заказчик;
  2. **Аналитический блок табличная форма:** способ отображения задач списком. Имеется кнопка «Создать задачу». Список полей настраиваемый-каждый пользователь может менять настройки отображения, сортировки, порядка и фильтрации столбцов.
     + 1. Список полей:
          - Номер задачи – по умолчанию;
          - Статус (активна/деактивирована) – по умолчанию;
          - Дата время начала действия задачи – по умолчанию;
          - Периодичность выполнения задачи – периодичность;
          - Дата время окончания действия задачи (если не заполнена, то бессрочно);
          - Наименование задачи – по умолчанию;
          - Результат отработки отчёта (OК/Error) – по умолчанию
          - Переход в задачу – по умолчанию;
          - Управление задачей – по умолчанию;
          - Описание задачи;
          - Условие срабатывания триггера;
          - Действия при срабатывании триггера;
          - Отправка и получатели уведомлений;

Имеется возможность «проваливаться» в каждую задачу. В настройках формы имеется возможность настройки отображения количества задач на одном листе. Также должна быть возможность экспорта списка в файлы формата csv, pdf, xls.

*Визуальный пример:*

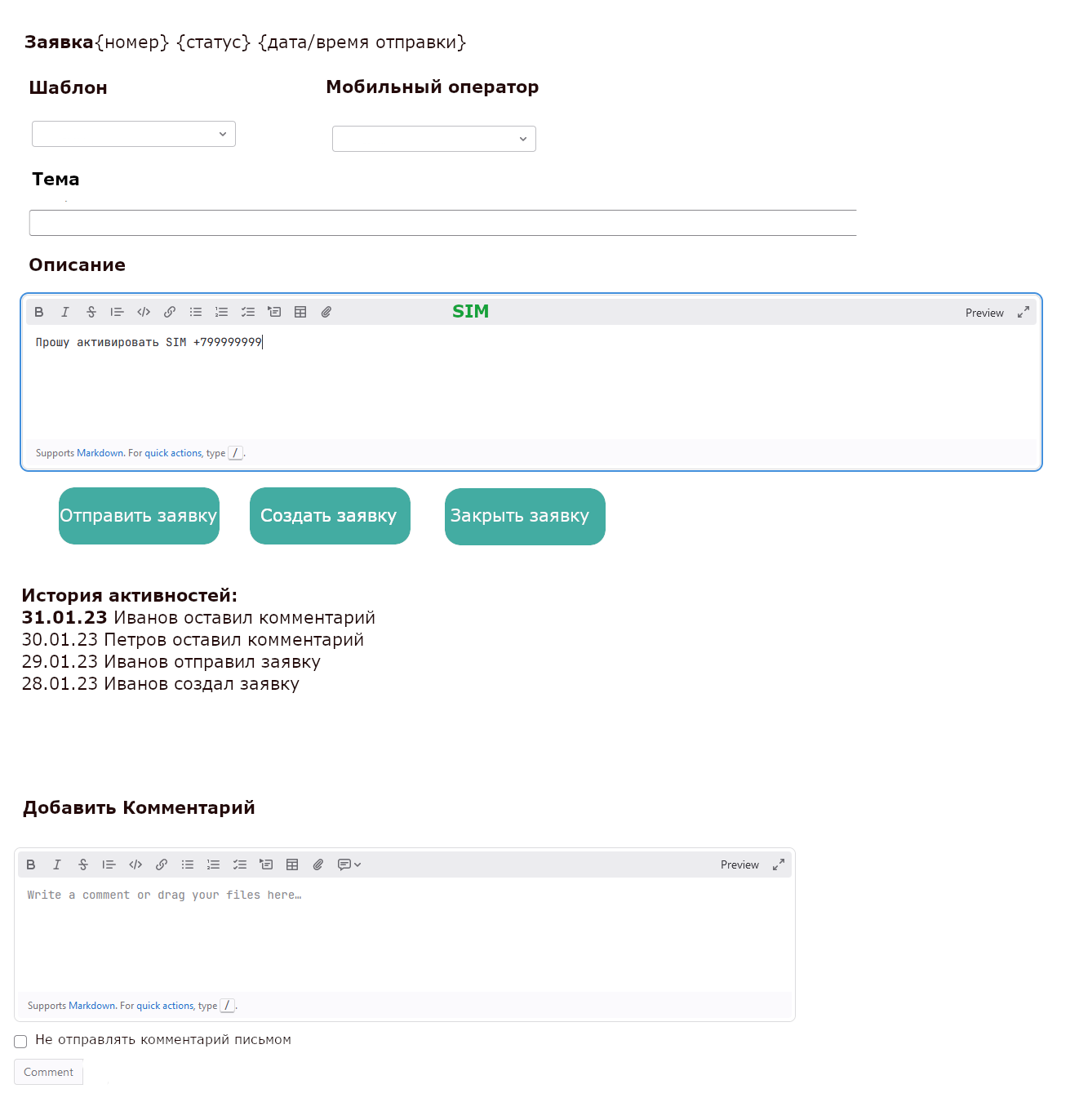
* + - 1. **Аналитический блок индивидуальная форма задачи:** индивидуальная форма задачи должна содержать все перечисленные в п.1 поля с учетом:
         * поле «Условие срабатывания триггера» имеет конструкторский тип, который позволяет отбирать определенные поля, а также фильтровать их;
         * поле «Действия при срабатывании триггера» должно иметь два поля активировать и деактивировать SIM-карту или ничего не делать;
         * поле «отправить отчет» - позволяет отправить отчет по выборке срабатывания триггера
  1. **SIM-карты табличная форма:** способ отображения SIM-карт списком с возможностью в правой части видеть более подробное описание. Список полей настраиваемый-каждый пользователь может менять настройки отображения, сортировки, порядка и фильтрации столбцов. В настройках формы имеется возможность настройки отображения количества SIM-карт на одном листе. Должна быть возможность экспорта списка в файлы формата csv, pdf, xls.
     + 1. Список полей:
          - Выделить(check-box) – по умолчанию;
          - Мобильный оператор – по умолчанию;
          - DEF номер– по умолчанию;
          - ICCID – по умолчанию;
          - Статус SIM – по умолчанию;
          - Статус SIM (БДО) – по умолчанию;
          - Дата активации/деактивации;
          - Номер объекта, где установлено;
          - Адрес объекта, где установлено;
          - Статус объекта – по умолчанию;
          - Модель оборудования;
          - Доступность оборудования;
          - Показать описание – по умолчанию;

Имеется возможность фильтровать список по полям:

* + - * + DEF номер (частичное совпадение);
        + ICCID (частичное совпадение);
        + Мобильный оператор (выбор из списка);
        + Номер объекта (частичное совпадение);
        + Адрес объекта (частичное совпадение);
      1. Визуальный пример
      2. Возможности групповой работы с SIM – должна иметься возможность групповой работы с SIM картами (активация/деактивация) как на UI через фиксирование поля «выделить» и кнопок «Активация», «Деактивация». Также должна быть возможность изменений через импорт файла, где связующими данными являются ICCID или DEF номер.
  1. **Отчеты:**
     1. **Отчеты табличная форма –** идентична табличной форме «Аналитического блока» п.7.3 1
     2. **Отчеты индивидуальная форма -** Идентична индивидуальной форме «Аналитического блока» п.7.3 2.
     3. **Предустановленные Отчеты:**
        + - SIM присутствуют в БДО но отсутствуют у мобильных операторов
          - Статус SIM = «Активна» И Статус SIM БДО <> «Активирован».
          - Активная SIM установлена на не рабочем объекте.
          - Активная SIM у которой дата активации больше 20 дней с текущего момента и не прикреплена ни к какому объекту.
  2. **Заявки:**
     1. **Заявки табличная форма:** способ отображения задач списком. Имеется кнопка «Создать заявку». Список полей настраиваемый-каждый пользователь может менять настройки отображения, сортировки, порядка и фильтрации столбцов.
     2. Список полей:
        + - Номер заявки;
          - Дата отправки заявки (дата/время, когда заявка перешла в статус «Отправлена»);
          - Мобильный оператор – получатель заявки;
          - Статус заявки;
          - Тема заявки;
          - Текст заявки;
          - Действие (Имеется возможность «проваливаться» в каждую задачу);

В настройках формы имеется возможность настройки отображения количества задач на одном листе. Также должна быть возможность экспорта списка в файлы формата csv, pdf, xls. Визуальный пример аналогичен визуальному примеру «Табличная форма Аналитический блок» п.7.3.

* + 1. **Заявки индивидуальная форма**: должна содержать следующие поля:
       - * Номер заявки (формируется автоматически);
         * Мобильный оператор заявки (выбор из списка);
         * Статус заявки;
         * Выбор шаблона заявки (выбор из списка);
         * Тема заявки (заполняется из шаблона, редактируемое пользователем);
         * Текст заявки (заполняется из шаблона, редактируемое пользователем) должно поддерживать форматирование «Markdown»;
         * Поле/кнопка прикрепления файлов;
         * Поле для комментария (заполняется пользователем и имеется возможность не отправлять комментарий Мобильному оператору);
         * Поле с историей по активности в заявке;
         * Кнопка «Сохранить заявку» при нажатии формируется номер заявки;
         * Кнопка «Отправить заявку»
         * Кнопка «Закрыть заявку»

*Визуальный пример:*

**8.** **Требования к конфиденциальности и безопасности**

## Общие требования:

При выполнении работ должны выполняться требования федерального законодательства, нормативно-правовых актов регуляторов в области защиты информации и персональных данных.

Все компоненты Системы должны быть размещены в пределах ИТ-инфраструктуры Общества (КСПД). Использование внешних “облачных”, сервисных, технологических решений и компонентов запрещено.

Все интеграционные взаимодействия со смежными ИС Общества должны быть реализованы в пределах КСПД.

Все компоненты и прикладное ПО 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).

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

В АРМ MultiSimBox Должна осуществляться проверка/валидация любых входных данных на длину, тип и допустимые символы. Проверка должна осуществляться до сохранения или отображения информации.

В АРМ MultiSimBox должен поддерживаться режим обработки ошибок, при котором пользователю не сообщается детальная информация об ошибке (версии подсистем, таблицы БД, сетевые адреса компонент и т.д.) в случае сбоя приложения. Детальная информация может предоставляться только администраторам АРМ MultiSimBox.

В АРМ MultiSimBox должны быть предусмотрены механизмы резервного копирования и восстановления данных. Процедура резервного копирования не должна работать с резервируемыми данными в монопольном режиме. В случае резервирования данных, содержащих конфиденциальную информацию, средства резервного копирования должны обеспечивать защиту резервируемых данных с применением криптографических алгоритмов.

АРМ MultiSimBox должен работать с имеющимися в Обществе средствами защиты информации, такими как Антивирус, FireWall.

## Требования к аутентификации и авторизации:

Запрещено использование личных учетных записей в качестве технологических. Все служебные и технологические учетные записи, должны иметь определенного из числа сотрудников Исполнителя ответственного, либо должны быть заблокированы.

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

АРМ MultiSimBox не должна выдавать информацию о типе и версии системы или ее компонент до успешного завершения процедур аутентификации и авторизации.

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.

АРМ MultiSimBox и ее компоненты не должны содержать жестко запрограммированных учетных записей, либо данные этих УЗ должны быть заменены

Компоненты АРМ MultiSimBox, критичные для функционирования АРМ MultiSimBox, в случае сетевого взаимодействия должны проходить процедуру взаимной аутентификации.

АРМ MultiSimBox должна:

* Предоставлять пользователям возможность самостоятельно устанавливать свой пароль и менять его в любое время;
* Позволять администраторам отключать возможность смены пароля у отдельных пользователей;
* Предоставлять возможность обязательной смены заданного администратором пароля при первом входе в систему;
* Проверять качество вводимого пароля в соответствии с требованиями политики использования паролей;
* Обеспечивать принудительную смену пароля через установленный в политике использования паролей промежуток времени;
* Иметь возможность автоматической блокировки учётной записи, в случае если ее пароль до установленной даты не был изменён;
* 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;
* Иметь возможность задавать параметры парольной политики для группы пользователей, а также возможность назначать их отдельно для каждой отдельной учетной записи;
* 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

Все пароли АРМ MultiSimBox должны храниться и передаваться только в зашифрованном виде (в т.ч. и пароли от технологических учетных записей на серверах в конфигурационных файлах, в базах данных). При хранении и передаче должны использоваться стойкие криптографические алгоритмы или алгоритмы хеширования

Подключение АРМ MultiSimBox к базам данных или другим внешним системам должно происходить под технологическими учетными записями с минимально необходимыми наборами привилегий.

Все неиспользуемые для штатной работы АРМ MultiSimBox учетные записи (установленные по умолчанию, тестовые, сервисные) должны быть удалены или заблокированы. Пароли от предустановленных учетных записей и сервисов должны быть изменены сразу после установки компонентов АРМ MultiSimBox.

## Список стойких криптографический алгоритмов:

**Симметричные алгоритмы шифрования:**

* ГОСТ 28147-89 (с утвержденными ЦБС ФСБ блоками замен)
* AES (согласно FIPS 197)
* CAST5
* IDEA
* Blowfish
* Twofish
* Serpent.

**Асимметричные алгоритмы шифрования и ЭЦП:**

* согласно ГОСТ Р 34.10-2001 (с утвержденными ЦБС ФСБ параметрами алгоритма)
* RSA (с размерностью составного модуля не менее 2048 бит и открытой степенью, согласно ISO/IEC 14888-2:2008 и IEEE P1363)
* ECDSA (с размерностью порядка базисной точки P не менее 256 бит согласно ISO/IEC 14888-3, IEEE P1363, FIPS 186-3 и ANSI X9.62-2005)
* DSA
* ElGamal

**Алгоритмы обмена ключевым материалом:**

* Diffie-Hellman.

**Алгоритмы хеширования и выработки MAC:**

* согласно ГОСТ Р 34.11-94 (с утвержденными ЦБС ФСБ параметрами алгоритма)
* SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384 и SHA-512), SHA-3 согласно FIPS 180-3
* HMAC согласно FIPS 198-1
* RIPEMD-160
* Whirlpool
* Tiger-192.

Для защиты ПДн и защиты конфиденциальных данных в государственных ИС допускается использование только отечественных криптографических алгоритмов: ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94.

## Механизм протоколирования событий:

Журналы аудита должны храниться как минимум три месяца в оперативном доступе в АРМ MultiSimBox. Также в АРМ MultiSimBox должна предоставляться возможность сохранять журналы аудита во внешних системах.

В АРМ MultiSimBox должно осуществляться логирование как минимум следующих действий:

* Успешные и неуспешные попытки аутентификации пользователя;
* Действия привилегированных пользователей по настройке и изменению конфигурации (в том числе изменение настроек аудита);
* Любой доступ пользователей к данным, содержащим конфиденциальную информацию;
* Успешные и неуспешные попытки доступа пользователя к данным системы;
* Доступ к записям журнала протоколирования событий;
* Запуск и остановка компонентов ИС;
* Создание и удаление объектов системного уровня.

Лог файлы должны содержать, как минимум, следующую информацию:

* Идентификатор пользователя, выполнившего операцию;
* Источник события (IP-адрес, идентификатор рабочей станции, процесс/приложение и т.д.);
* Название или тип выполненного события;
* Дату и время события;
* Результат события;
* Объект, над которым была выполнена операция;
* Используемый протокол доступа;
* Используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к объекту.

Журналы аудита ИС не должны содержать данных, содержащих конфиденциальную информацию.

Журналы аудита ИС должны быть защищены от изменений.

## Требования к сетевому взаимодействию:

Любой процесс обмена конфиденциальной информацией через сети внешнего пользования (по каналам связи, имеющим выход за пределы контролируемой зоны) должен осуществляться по зашифрованному каналу передачи данных. При этом допустимо использование следующих протоколов, выбор которых зависит от требований законодательства в части обработки защищаемой информации:

* TLS/SSL (последних версий);
* SFTP;
* FTPS;
* SSH-2;
* SCP;
* S/MIME с использованием сертификатов x.509 v3;
* VPN (IPSEC, L2TP, PPTP и т.д.);
* ГОСТ Р, при этом, при выборе конкретного протокола следует отдавать предпочтение последним версиям, а также рекомендациям по безопасности их использования.

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

## Требования к web-сервису:

АРМ MultiSimBox должна обеспечивать возможность завершения сессии пользователя из любой страницы\раздела системы, а также при закрытии браузера пользователя.

При обращении к базам данных АРМ MultiSimBox должны использоваться хранимые процедуры, вместо SQL запросов, содержащих параметры.

При обращении к базам данных не допускается прямое использование данных или их частей, полученных web-сервером от клиентской системы, в коде динамически формируемых SQL-запросов. Такие данные или их части могут быть напрямую использованы только в параметрах SQL-запросов или хранимых процедур.

## Требования к обновлениям и изменениям

Обновления безопасности для любых компонентов АРМ MultiSimBox должны устанавливаться не позднее 30 календарных дней с момента их выпуска производителем. Перед установкой обновления должны тестироваться на тестовых экземплярах АРМ MultiSimBox. Обновления безопасности для сертифицированных средств защиты информации должны устанавливаться в соответствии с требованиями Приказа ФСТЭК России от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

В случае возникновения нестабильной работы ИС в результате установки обновлений безопасности, Исполнитель, либо компания, осуществляющая поддержку АРМ MultiSimBox, должна в сроки, определенные в договоре технической поддержки предложить и внедрить альтернативное решение возникшей проблемы. В случае возникновения нестабильной работы АРМ MultiSimBox в результате установки обновлений сертифицированных средств защиты информации следует руководствоваться требованиями Приказа ФСТЭК России от 03.04.2018 № 55 «Об утверждении Положения о системе сертификации средств защиты информации».

Установка средств разработки (компиляторы, отладчики, шестнадцатеричные редакторы и д.р.) и тестирования на продуктивный экземпляр АРМ MultiSimBox запрещена за исключением случаев, когда необходимость в таких средствах для развертывания и последующей эксплуатации явно указана производителями общесистемного ПО, СУБД.

1. **Требования к документированию**

Должна быть разработана техническая и эксплуатационная документация на русском языке в составе следующих документов:

* Структурная схема;
* Спецификация технических средств функциональная схема;
* Описание системы;
* Описание массива информации;
* Описание протокола взаимодействия с внешними системами и внутренними клиентами (API);
* Программа и методика испытаний;
* Протокол проведения испытаний;
* Руководство пользователя;
* Руководство администратора;

В рамках документа Описание массива информации должно приводиться описание структуры БД с информацией о событиях, описание таблиц, полей таблиц, взаимосвязей и индексов.

Полнота предоставленной технической документации должна быть достаточной для разработки модулей, размещаемых на данной платформе, без привлечения Исполнителя.