ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«ЛАБОРАТОРИЯ ИНЖЕНЕРНЫХ СИСТЕМ»

УТВЕРЖДАЮ
Генеральный директор ООО «ЛиС»

И.С. Соколов
«31» октября 2021 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

ПО РАЗРАБОТКЕ ПРОГРАММНОГО ОБНСПЕЧЕНИЯ «АВТОМАТИЗИРОВАНАЯ ИНФОРМАЦИОННАЯ СИСТЕМА HARVEST»

ИСПОЛНИТЕЛЬ
Заместитель директора по науке ООО «ЛиС»

М.Е. Литвинов
«31» октября 2021 г.

Содержание

1 Общие сведения о программе.

Автоматизированная информационная система Harvest — это платформа с открытым исходным кодом для визуализации, мониторинга и анализа данных в тепличных комплексах. Harvest позволяет пользователям создавать дашборды с панелями, каждая из которых отображает определенные показатели в течение установленного периода времени. Каждый дашборд универсален, поэтому его можно настроить для конкретного проекта или с учетом любых потребностей разработки и/или бизнеса.

Терминология

В настоящем документе используются следующие определения и сокращения:

АИС	Автоматизированная информационная система
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
Продукт	Продукт с рабочим названием «Умный дом»
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.
ТОА	Технологическое оборудование агрономическое.

1.1 Основание для выполнения работ.

План развития ООО «ЛиС», Приказ №1В от 01 октября 2021 г.

1.2 Сведения об источниках и порядке финансирования.

Источник финансирования определяется Заказчиком.

2 Назначение, цели и задачи ПО «Harvest».

Пользователь АСП должен иметь доступ к информации о работе технологического оборудования, установленного у заказчика, иметь возможность просмотра данных и управления в режиме реального времени посредством веб-интерфейса и в браузерах для мобильных устройств.

2.1 Цель выполнения работ.

Работы по Приказу №1В от 01 октября 2021 г. выполняются с целью пилотного запуска автоматизированной информационной системы «Harvest».

2.2 Место выполнения работ.

Работы выполняются на территории Российской федерации.

2.2 Состав работ.

Исполнитель выполняет перечисленные ниже работы:

- Разработка ПО.

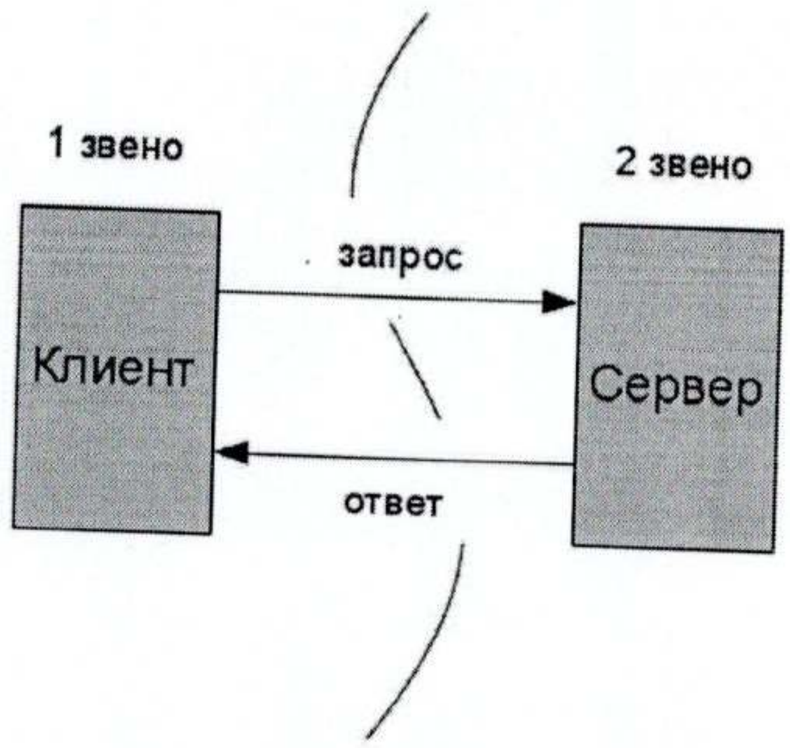
В таблице 1 представлены этапы выполнения работ согласно Приказу №1В от 01 октября 2021 г.

Таблица 1 - Этапы выполнения работ

№ Этап	Наименование этапа	Срок сдачи работ	Результат работ
1	Разработка АИС «Harvest»		– Описание API Контроллера; – Комплект документов технического проекта – Комплект документов эксплуатационной документации – Программа и методика испытаний – Протокол проведения предварительных испытаний – Исходные коды комплекса программных средств
2	Проведение опытной эксплуатации АИС	В течение всего срока опытной эксплуатации, но не более 4 месяцев	– Отчет о проведении опытной эксплуатации – Протокол проведения приемо-сдаточных испытаний

3 Описание услуги «Harvest».

3.1 Схема работы.



У заказчика устанавливается сервер АИС «Harvest». Заказчик настраивает необходимое количество абонент с использованием web-браузера и подключается к АИС. Также возможно с использованием мобильного web-браузера платформ iOS или Android.

3.2 Архитектура ПО.

Пользовательские интерфейсы должны быть размещены на отдельном сервере. Доступ к АИС осуществляется через сеть Internet по защищённому каналу.

В результате внедрения АИС должна быть обеспечена поддержка бизнес-процессов подключения, эксплуатации и абонентского обслуживания на всех этапах жизненного цикла продукта.

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

4 Требования к системе.

4.1 Функциональные требования.

АИС должна предоставлять Пользователям следующие возможности:

- просмотр статусов и событий;
- отображение состояния датчиков, механизмов;
- управление подключенными устройствами;
- управления с мобильных устройств;
- рассылка уведомлений.

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

1) Подсистема авторизации и аутентификации пользователей;
2) Подсистема регистрации и хранения событий;
3) Подсистема взаимодействия с управляющим контроллером;

4) Подсистема уведомлений;
5) Веб-интерфейс пользователя;
6) Веб-интерфейс администратора;

4.1.1 Авторизация и аутентификация пользователей.

Процесс авторизации пользователей выполняется по логину и паролю в АИС. Смена пароля и иные действия с учётной записью проводятся средствами платформы.

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

- E-mail;
- номер телефона.

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

4.1.2 Регистрация и хранение событий.

В АИС реализованы функции регистрации событий (логирования). Просмотр событий доступен для администраторов АИС. События сортируются по времени появления. Должен быть предусмотрен механизм выделения важных и критических событий.

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.

Возможность отправки событий по средствам популярных мессенджеров или электронной почты.

Список конкретных мессенджеров согласуется с заказчиком индивидуально.

4.1.4 Взаимодействие с управляющим контроллером

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

- регистрация управляющего контроллера;
- взаимодействие с управляющим контроллером посредством прямого постоянно открытого соединения;
- оповещение пользователя о потере связи с управляющим контроллером;
- регистрация датчиков, механизмов;
- доступ к функциям механизмов;
- доступ к архивам записей с помощью панели Web приложения;

- вывод информации о работе контроллера, исполнительных механизмов, измерений по произвольному контроллеру либо по совокупности контроллеров;
- ввод настроек контроллера с возможностью прослеживания времени и даты внесения изменений;
- анализ разработка специальных компонентов для визуализации специализированных данных о работе контроллера исполнительных механизмов.

4.1.9 Веб-интерфейс пользователя.

Веб-сервис пользователя должен состоять из следующих информационных блоков, предоставляющих доступ к функциям АИС:

- Блок «Рабочий стол» (дашборд) может содержать следующие компоненты:
  - графики работы механизмов, измерений;
  - просмотр последних событий с фильтром по времени;
  - блок с отображением состояния датчиков и сигналов, содержащий управляющие элементы в виде специализированных визуальных компонентов;
  - 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 список управляющих контроллеров 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;

- Блок «Настройки» должен содержать:
  - Управление рассылкой уведомлений;
  - Управление мобильными устройствами для рассылки push-уведомлений;

4.1.10 Веб-интерфейс администратора.

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

- Просмотр верхнеуровнего состояния системы;
- Просмотр параметров подключенных контроллеров;
- Просмотр системных событий;
- Просмотр состояния подключенного оборудования;
- Обновление прошивки контроллеров.

Веб-интерфейс администраторов должен состоять из следующих разделов:

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

4.1.11 Интерфейс для мобильных приложений.

Основные функции АИС должны быть доступны пользователям на устройствах под управлением ОС Android и iOS.

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

- авторизация в АИС;
- добавление контроллера;
- управление контроллером;
- добавление и удаление пользовательских устройств; ▪ управление подключенными устройствами;
- получение событий;
- получение справочников;
- возможность активации и деактивации режимов работы сервиса;

4.1.12 Интерфейс для взаимодействия с контроллером.

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

- авторизация в АИС;
- управление контроллером;
  - получение информации о контроллере; ○ текущее состояние;
  - версия прошивки;
  - восстановление конфигурации контроллера. ▪ добавление/удаление устройств;
- управление устройствами;
- получение информации о изменении состояния устройств;

4.2 Нефункциональные требования.

4.2.1 Требования к надежности.

Разработка должна выполняться с учетом необслуживаемого функционирования АИС 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.

АИС 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.

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

На этапе пилота должно быть обеспечено резервное копирование для всех компонентов АИС. В промышленной эксплуатации резервирование всех компонентов АИС 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.

АИС должен разрабатываться с учетом Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования.

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.

АИС относится к информационным системам общего пользования, 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;
- 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 АИС на этапе передачи в промышленную эксплуатацию, должны быть стабильных последних версий, либо должны быть установлены обновления до тех версий, которые обеспечивают максимальную защищенность системы (отсутствие известных уязвимостей).

4.2.4.2 Требования к аутентификации и авторизации

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

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

- Логин/Пароль;

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

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

АИС 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 АИС должна создаваться в процессе подключения. После аутентификации в АИС пользователь может выполнить первый вход в систему с новой учетной записью.

На этапе пилотного проекта к процессу аутентификации предъявляются следующие требования.

АИС 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 учетной записи, в случае если ее пароль до установленной даты не был изменен;
- Иметь возможность блокировки учетной 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 АИС в промышленную эксплуатацию дополнительно предъявляются следующие требования. АИС 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 АИС не должны выдавать информации о типе и версии системы или ее компонент до успешного завершения процедур аутентификации и авторизации. Для ввода АИС в промышленную эксплуатацию данное требование должно выполняться для всех интерфейсов АИС.

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.

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

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

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

Все неиспользуемые для штатной работы АИС 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 АИС в продуктивную среду.

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

4.2.4.3 Требования к аудиту.

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

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

Для ввода АИС 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 АИС необходим доступ к системам или базам данных, расположенным во внутренней сети Заказчика, то обмен данными между ними должен осуществляться с использованием защищенных протоколов.

Сетевое взаимодействие между компонентами АИС, 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 АИС должны носить характер транзакционно-ориентированных, т.е. выполняющихся в целом от начала до конца либо, в случае сбоя транзакции, не выполняющихся совсем.

АИС 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 АИС, должны быть защищены с использованием стойких алгоритмов шифрования.

В пользовательских интерфейсах АИС 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.).

АИС 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 АИС 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 АИС не должен постоянно работать с данными в монопольном режиме. Должны быть предусмотрены временные интервалы, в которые АИС будет снимать блокировки с данных.

4.2.4.6 Дополнительные требования к web-компонентам.

АИС 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.

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

На web-серверах АИС 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, АИС 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 АИС 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.

АИС должен обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях АИС 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:

- 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 АИС, 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 АИС, должны соблюдаться условия лицензионных соглашений и обеспечиваться патентная чистота.

4.2.8 Требования по стандартизации и унификации.

Разработка прикладного программного обеспечения АИС 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 АИС 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.

АИС 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.

АИС 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 АИС, 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, 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 АИС 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;

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

Требования к техническим характеристикам серверной группы:

Компонент	**Конфигурация**
Тип сервера	Физический/Виртуальный сервер
Процессор	не менее 4 ядер
Оперативная память	веб-сервер – не менее 16 Гб сервер приложений – не менее 16 Гб
	веб-сервер – не менее 300 Гб SAS сервер приложений – не менее 300 Гб 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	Не менее 2 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.

5 Состав и содержание работ по развертыванию.

5.1 Требования к выполнению развертывания на инфраструктуре Заказчика.

АИС 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.

6 Порядок контроля и приемки.

6.1 Предварительные испытания.

Предварительные испытания проводятся согласно разработанной Программе и методике испытаний. По результатам предварительных испытаний составляется протокол проведения предварительных испытаний.

6.2 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.

6.3 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.

7 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). 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

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

Приоритет - критерий важности и срочности решения инцидента, с учетом 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).

8 Требования к программной документации.

8.1 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;
- Программа и методика испытаний;
- Протокол проведения предварительных испытаний;
- Отчет о проведении опытной эксплуатации;
- Протокол проведения приемо-сдаточных испытаний;
- Исходные коды АИС, исключительные права на использование, доработку, продажу доработанной системы должны быть переданы Заказчику,
- Исходные коды НОП.

8.2 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.