Функциональные требования

Информационная система

Интеграции Приложений

Москва, 2024 г.

СОДЕРЖАНИЕ

[1 ОБЩИЕ СВЕДЕНИЯ 6](#_Toc175831083)

[1.1 Полное наименование системы и ее условное обозначение 6](#_Toc175831084)

[1.2 Номер договора 6](#_Toc175831085)

[1.3 Заказчик 6](#_Toc175831086)

[1.4 Исполнитель 6](#_Toc175831087)

[2 НАЗНАЧЕНИЕ И ЦЕЛИ ЗАКУПКИ ПЛАТФОРМЫ 7](#_Toc175831088)

[2.1 Назначение 7](#_Toc175831089)

[2.2 Номер договора 7](#_Toc175831090)

[2.3 Заказчик 7](#_Toc175831091)

[2.4 Исполнитель 7](#_Toc175831092)

[2.5 Плановые сроки начала и окончания работы по созданию системы 7](#_Toc175831093)

[2.6 Источники финансирования работ 7](#_Toc175831094)

[2.7 Порядок оформления и предъявления заказчику результатов работ по созданию системы (ее частей), по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы 7](#_Toc175831095)

[2.8 Цели создания 7](#_Toc175831096)

[3 ХАРАКТЕРИСТИКА ОБЪЕКТОВ АВТОМАТИЗАЦИИ 9](#_Toc175831097)

[3.1 Вид автоматизируемой деятельности 9](#_Toc175831098)

[3.2 Перечень объектов автоматизации 9](#_Toc175831099)

[3.2.1 Сбор данных: 9](#_Toc175831100)

[3.2.2 Обработка данных: 9](#_Toc175831101)

[3.2.3 Хранение данных: 9](#_Toc175831102)

[3.2.4 Доставка данных: 9](#_Toc175831103)

[3.2.5 Мониторинг и логирование: 9](#_Toc175831104)

[3.2.6 Управление доступом и безопасность: 9](#_Toc175831105)

[3.2.7 Резервное копирование и восстановление: 10](#_Toc175831106)

[3.2.8 Интеграция с внешними системами: 10](#_Toc175831107)

[3.3 Сведения об условиях эксплуатации объекта автоматизации 10](#_Toc175831108)

[4 ТРЕБОВАНИЯ К СИСТЕМЕ 11](#_Toc175831109)

[4.1 Требования к системе в целом 11](#_Toc175831110)

[4.2 Требования к численности и квалификации персонала Исполнителя 11](#_Toc175831111)

[4.3 Требования к численности и квалификации персонала Системы и режиму его работы 11](#_Toc175831112)

[4.3.1 В Системе должны быть предусмотрены следующие роли персонала: 11](#_Toc175831113)

[4.3.2 Требования к персоналу 11](#_Toc175831114)

[Детальные требования к численности и квалификации персонала Системы и режиму его работы должны быть определены на этапе технического проектирования ИСИП. 11](#_Toc175831115)

[4.4 Требования к патентной и лицензионной чистоте 11](#_Toc175831116)

[4.5 Требования к функциональным характеристикам. 12](#_Toc175831117)

[4.5.1 Функция публикации сообщений: 12](#_Toc175831118)

[4.5.2 Функция подписки на сообщения: 12](#_Toc175831120)

[4.5.3 Функция управления топиками: 12](#_Toc175831121)

[4.5.4 Функция мониторинга и логирования: 12](#_Toc175831122)

[4.5.5 Функция централизованного управления схемами данных: 13](#_Toc175831123)

[4.6 Требования к информационной и программной совместимости. 13](#_Toc175831124)

[4.6.1 Форматы данных: 13](#_Toc175831125)

[4.6.2 Протоколы взаимодействия: 13](#_Toc175831126)

[4.7 Требования к защите информации: 13](#_Toc175831127)

[4.7.1 Шифрование: 15](#_Toc175831128)

[4.7.2 Разграничение и контроль доступа 15](#_Toc175831129)

[4.7.3 Доступность 16](#_Toc175831130)

[4.7.4 Среды информационной системы 16](#_Toc175831137)

[4.8 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы 17](#_Toc175831138)

[4.9 Требования по сохранности информации при авариях 17](#_Toc175831139)

[4.10 Требования к надежности, производительности и показателям назначения 17](#_Toc175831140)

[4.10.1 Показатели назначения 17](#_Toc175831141)

[Обеспечение пропускной способности не менее 100 000 сообщений в секунду. 17](#_Toc175831142)

[4.10.2 Надежность 18](#_Toc175831143)

[4.11 Требования к видам обеспечения 19](#_Toc175831149)

[4.11.1 Требования к организационному обеспечению 19](#_Toc175831150)

[4.11.2 Требования к методическому обеспечению 19](#_Toc175831151)

[4.11.3 Требования к программному обеспечению 19](#_Toc175831152)

[4.11.4 Требования к техническому обеспечению 20](#_Toc175831153)

[5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ 21](#_Toc175831154)

[5.1 Требования к выполнению работ 21](#_Toc175831155)

[5.2 Требования к исполнителю работ 24](#_Toc175831156)

[5.3 Требования к взаимодействию Исполнителя и Заказчика 24](#_Toc175831157)

[5.4 Требования к работам по оказанию услуг технической и консультационной поддержки пользователей Системы 25](#_Toc175831158)

[6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ 26](#_Toc175831159)

[6.1 Виды, состав, объем и методы испытаний системы и ее составных частей (виды испытаний в соответствии с действующими нормами, распространяющимися на разрабатываемую систему) 26](#_Toc175831160)

[6.2 Общие требования к приемке работ по стадиям (перечень участвующих предприятий и организаций, место и сроки проведения), порядок согласования и утверждения приемочной документации 26](#_Toc175831161)

[7 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ 28](#_Toc175831162)

[7.1 Общие требования 28](#_Toc175831163)

[7.2 Перечень основных мероприятий и их исполнителей, которые следует выполнить при подготовке объекта автоматизации к вводу Системы в действие 28](#_Toc175831164)

[8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ 30](#_Toc175831165)

[9 ТРЕБОВАНИЯ К ГАРАНТИЙНОМУ ОБСЛУЖИВАНИЮ 31](#_Toc175831166)

[10 ИСТОЧНИКИ РАЗРАБОТКИ 32](#_Toc175831168)

[10.1 Документы и информационные материалы, на основе которых разрабатывались ФТ 32](#_Toc175831169)

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе применены следующие термины, определения и сокращения:

|  |  |
| --- | --- |
| API | Application Programming Interface. Программный интерфейс приложения – описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой |
| AD | Active Directory или LDAP совместимая служба каталогов |
| ОС | Операционная система |
| Исполнитель | Подрядная организация, выполняющая работы по Проекту в соответствии с настоящими функциональными требованиями |
| Компания | АО РНПК |
| ИСИП | Информационная система интеграции приложений |
| Apache Kafka | Распределённый программный брокер сообщений с открытым исходным кодом |
| Брокер сообщений | Архитектурный паттерн в распределённых системах; приложение, которое преобразует сообщение по одному протоколу от приложения-источника в сообщение протокола приложения-приёмника, тем самым выступая между ними посредником. |

# ОБЩИЕ СВЕДЕНИЯ

## Полное наименование системы и ее условное обозначение

Полное наименование платформы: ИНФОРМАЦИОННАЯ СИСТЕМА ИНТЕГРАЦИИ ПРИЛОЖЕНИЙ (корпоративная шина данных), построенная на базе Arenadata Streaming Platform (Kafka), запись в Реестре отечественного ПО №23927 от 06.09. 2024.

Условное обозначение Системы: Корпоративная шина данных.

## Номер договора

Определяется по результатам торгово-закупочных процедур Заказчика (далее – «Договор»).

## Заказчик

Полное наименование заказчика работ: Акционерное общество «Российская Национальная Перестраховочная Компания».

Краткое наименование заказчика: АО РНПК.

## Исполнитель

Исполнитель (поставщик, подрядчик) работ определяется по результатам закупочных процедур Заказчика.

# НАЗНАЧЕНИЕ И ЦЕЛИ ЗАКУПКИ ПЛАТФОРМЫ

## Назначение

Обеспечение надежной и эффективной передачи данных между различными компонентами информационных системы и самими информационными системами в распределенных средах.

## Номер договора

Определяется по результатам торгово-закупочных процедур Заказчика (далее – «Договор»).

## Заказчик

Полное наименование заказчика работ: Акционерное общество «Российская Национальная Перестраховочная Компания».

Краткое наименование заказчика работ: АО РНПК.

## Исполнитель

Исполнитель (подрядчик) работ определяется по результатам торгово-закупочных процедур Заказчика.

Возможность привлечения Исполнителем соисполнителей (субподрядчиков) работ, должна быть согласована с Заказчиком в письменном виде.

## Плановые сроки начала и окончания работы по созданию системы

Сроки начала и окончания работ описаны в разделе 5 настоящих ФТ.

## Источники финансирования работ

Финансирование работ осуществляется за счет собственных средств Заказчика.

## Порядок оформления и предъявления заказчику результатов работ по созданию системы (ее частей), по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы

Порядок оформления и предъявления Заказчику результатов работ по созданию Системы описан в разделах 5-8 настоящего документа.

## Цели создания

Цель - получение распределенной высокопроизводительной и масштабируемой платформы, предназначенной для обработки потоков данных в реальном времени.

Достижение данной цели достигается выполнением следующих задач

* Поставка и настройка платформы
* Документирование информационной системы

# ХАРАКТЕРИСТИКА ОБЪЕКТОВ АВТОМАТИЗАЦИИ

## Вид автоматизируемой деятельности

Видом автоматизируемой деятельности является автоматизация потоковой обработки данных в реальном времени.

## Перечень объектов автоматизации

### Сбор данных:

* Автоматизация процесса сбора данных от различных источников (приложений, микросервисов) и передача их в брокер сообщений.
* Обеспечение гарантированной доставки данных с возможностью настройки политик повторных попыток и временных окон.

### Обработка данных:

* Автоматизация процесса обработки данных, поступающих из брокера сообщений
* Обеспечение возможности параллельной обработки данных для повышения производительности.

### Хранение данных:

* Автоматизация процесса хранения данных в брокере сообщений с возможностью настройки политик хранения и ротации логов.
* Обеспечение надежности и доступности данных за счет механизмов репликации и отказоустойчивости.

### Доставка данных:

* Автоматизация процесса доставки данных из брокера сообщений в другие системы и приложения, включая поддержку различных протоколов и форматов данных.
* Обеспечение гарантированной доставки данных с возможностью настройки политик повторных попыток и временных окон.

### Мониторинг и логирование:

* Автоматизация процесса мониторинга состояния кластера брокера сообщений, производительности и ошибок.
* Обеспечение возможности анализа и диагностики проблем через логи и метрики.
* Обеспечение возможности просмотра очередей сообщений

### Управление доступом и безопасность:

* Автоматизация процесса управления доступом к данным в брокере сообщений, включая аутентификацию, авторизацию и шифрование данных.
* Обеспечение безопасности данных при передаче и хранении.

### Резервное копирование и восстановление:

* Автоматизация процесса резервного копирования данных в брокера сообщений и восстановление в случае сбоев с без потери данных.

### Интеграция с внешними системами:

* Автоматизация процесса интеграции брокера сообщений с внешними системами и приложениями, включая поддержку различных протоколов и форматов данных.
* Обеспечение надежной и безопасной передачи данных.

## Сведения об условиях эксплуатации объекта автоматизации

Объект автоматизации должен функционировать на виртуальных вычислительных ресурсах ИТ-инфраструктуры АО РНПК, развернутых на арендованных вычислительных мощностях в коммерческих ЦОД.

# ТРЕБОВАНИЯ К СИСТЕМЕ

## Требования к системе в целом

Платформа должна входить в реестр российского программного обеспечения, либо являться программным обеспечением с открытым исходным кодом, поставка, техническая поддержка и сопровождение которой осуществляется российскими организациями.

Все компоненты Платформы для организации взаимодействия с пользователем должны использовать русский язык или английский языки.

Платформа должна обеспечиваться гарантированной технической поддержкой, консультированием и сопровождением, направленными на обеспечение бесперебойного функционирования.

## Требования к численности и квалификации персонала Исполнителя

Требования к численности и квалификации персонала Исполнителя представлены в конкурсной документации (Документ Требования к участнику).

## Требования к численности и квалификации персонала Системы и режиму его работы

### В Системе должны быть предусмотрены следующие роли персонала:

* Администратор Системы;
* Пользователь Системы
* Пользователь СИБ (службы информационной безопасности)

### Требования к персоналу

### Детальные требования к численности и квалификации персонала Системы и режиму его работы должны быть определены на этапе технического проектирования ИСИП.

## Требования к патентной и лицензионной чистоте

Исполнитель гарантирует, что все компоненты, входящие в состав Платформы, отвечают требованиям к патентной чистоте, заключающиеся в том, что они могут свободно использоваться на территории Российской Федерации без опасности нарушения действующих на ее территории патентов.

Программные и технические средства, приобретаемые у сторонних фирм и предприятий и входящие в состав Платформы, должны сопровождаться документацией, подтверждающей правомочность этих организаций поставлять данную продукцию, а также должны сопровождаться лицензионным соглашением.

## Требования к функциональным характеристикам.

### Функция публикации сообщений:

* Возможность публикации сообщений в топики с указанием ключа и значения.
* Поддержка различных форматов данных (JSON, Avro, Protobuf и т.д.).
* Обеспечение гарантированной доставки сообщений с возможностью настройки политик повторных попыток и временных окон.
* Поддержка механизмов компрессии данных для оптимизации использования сети.

### Функция подписки на сообщения:

* Возможность подписки на топики с возможностью фильтрации сообщений по ключу или значению.
* Поддержка механизма подтверждения обработки сообщений с возможностью настройки стратегии подтверждения обработки сообщений (например, автоматическая или ручная).
* Обеспечение возможности репликации данных для повышения надежности и доступности.
* Поддержка механизмов балансировки нагрузки между потребителями.

### Функция управления топиками:

* Возможность создания, изменения и удаления топиков через административный интерфейс или API.
* Поддержка разделения топиков на партиции для масштабирования и обеспечения параллельной обработки данных.
* Обеспечение возможности настройки политик хранения данных, включая время хранения и максимальный объем данных.
* Поддержка механизмов ротации логов для оптимизации использования дискового пространства.

### Функция мониторинга и логирования:

* Возможность мониторинга состояния кластера, производительности и ошибок через интерактивный интерфейс или API.
* Поддержка логирования операций с возможностью настройки уровней логирования (например, DEBUG, INFO, ERROR).
* Интеграция с системами мониторинга и алертинга (например, Prometheus, Grafana, ELK Stack).
* Обеспечение возможности анализа и диагностики проблем через логи и метрики.
* Возможность просмотра логов топиков через административный интерфейс.

### Функция централизованного управления схемами данных:

* Управление версиями схем.

Обеспечение совместимости между различными версиями схем

## Требования к информационной и программной совместимости.

### Форматы данных:

* Поддержка стандартных форматов данных (JSON, xml, Avro, Protobuf и т.д.)

### Протоколы взаимодействия:

* возможность интеграции с другими системами через REST API на основе HTTP/HTTPS .
* Возможность интеграции с другими системами через бинарный протокол Apache Kafka на основе TCP

## Требования по обеспечению безопасности:

### Система должна соответствовать требованиям Приказа ФСТЭК России от 25.12.2017 N 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (категория значимости 3) и ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» (стандартный уровень защищенности).

4.7.2 Состав мер по обеспечению безопасности:

* Осуществление логического доступа пользователями и эксплуатационным персоналом под уникальными и персонифицированными учетными записями;
* Исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа;
* Исключение возможного бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации;
* Реализация возможности определения состава предоставленных прав логического доступа для конкретного ресурса доступа;
* Реализация возможности определения состава предоставленных прав логического доступа для конкретного субъекта логического доступа;
* Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего привилегированными правами логического доступа, позволяющими осуществить деструктивное воздействие, приводящее к нарушению выполнения бизнес-процессов или технологических процессов финансовой организации;
* Регистрация событий защиты информации, связанных с действиями, и контроль действий эксплуатационного персонала, обладающего правами по изменению параметров настроек средств и систем защиты информации, параметров настроек АС, связанных с защитой информации;
* Аутентификация программных сервисов, осуществляющих логический доступ с использованием технических учетных записей;
* Запрет на использование групповых, общих и стандартных учетных записей и паролей, а также прочих подобных методов идентификации и аутентификации, не позволяющих определить конкретного субъекта доступа;
* Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод) при разграничении логического доступа к ресурсам доступа;
* Реализация необходимых типов (чтение, запись, выполнение или иной тип) и правил разграничения логического доступа к ресурсам доступа;
* Запрет реализации пользователями-процессов и технологических процессов финансовой организации с использования учетных записей эксплуатационного персонала;
* Запрет выполнения пользователями бизнес-процессов с использованием привилегированных прав логического доступа, в том числе работы пользователей с правами локального администратора АРМ;
* Контроль состава разрешенных действий в Системе до выполнения идентификации и аутентификации;
* Организация мониторинга данных регистрации о событиях защиты информации, формируемых Системой и приложениями
* Регистрация нарушений и сбоев в формировании и сборе данных о событиях защиты информации

### Требования к аудиту

4.7.3.1 Механизм протоколирования событий должен быть способен сопоставить каждое подлежащие аудиту событие с источником события с возможным определением IP-адреса источника.

4.7.3.2 Должны протоколироваться следующие события:

* события аутентификации пользователя в системе, выход (окончание сессии) из системы;
* работа пользователя с данными системы, в том числе создание, чтение, изменение, или удаление данных;
* действия привилегированных пользователей по настройке и изменению конфигурации системы, в том числе изменение настроек системы, настроек аудита, создание/удаление пользователей/ролей/групп пользователей, изменение привилегий пользователей/ролей/групп пользователей, установка/удаление компонентов системы;
* доступ к записям журнала протоколирования событий;
* очистка логов;
* запуск и остановка компонентов системы.

4.7.3.3 По каждому событию должна протоколироваться следующая информация:

* результат операции (успешно/неуспешно);
* индикатор источника операции (индикатор пользователя, логин пользователя, имя процесс, IP-адрес, индикатор рабочей станции и т.д.);
* индикатор объекта, над которым было выполнена операция;
* название и тип выполненной операции (например, аутентификация, чтение, запись, удаление, установление соединения и др.);
* значения параметра до и после операции, если действие предполагает изменение данных или состояния компоненты системы;
* дата и время выполнения операции, включая указания часового пояса.

4.7.3.4 По возможности Система должна предоставлять средства фильтрации событий журнала аудита по протоколируемым событиям.

#### Журнал аудита системы должен быть защищен от изменений.

### 4.7.4 Регистрация доступа к хранимым данным о событиях защиты информации Шифрование:

* Поддержка шифрование данных при передаче и хранении с возможностью настройки алгоритмов шифрования и ключей.

### Разграничение и контроль доступа

* Поддержка изоляции данных между различными пользователями и приложениями.

Система должна быть доступна только авторизованным пользователем и клиентам.

* Компоненты Системы должны поддерживать аутентификацию учетных записей пользователей с помощью различных механизмов аутентификации, включая SASL (Simple Authentication and Security Layer) и SSL (Secure Sockets Layer)
* Компоненты Системы должны поддерживать авторизацию в соответствии со списками контроля доступа. Ролевая модель полномочий доступа к Системе должна быть разработана на этапе технического проектирования Системы.Система не должна накладывать ограничений на количество персонала, назначенные на определенные в ней роли.
* Доступ в Систему должен предоставляться только авторизованным пользователям и администраторам;
* Каждый пользователь и администратор Системы должен обладать уникальной учетной записью, запрещается наличие обезличенных/групповых учетных записей (за исключением встроенных в Систему технических учетных записей, отключение которых невозможно).
* В Системе должно быть реализовано разграничение доступа пользователей и администраторов как на уровне данных, так и на уровне функционала ИС (функционал администраторов должен быть недоступен пользователям; функционал по вводу/редактированию данных должен быть недоступен пользователям, имеющим права только на просмотр содержимого);
* Система должна обладать функционалом по разграничению прав доступа к элементам управления (администрирования ИС) и прикладному функционалу ИС;
* В ИС должны выполняться требования к паролям и парольным политикам, установленные Политикой информационной безопасности, Инструкцией по парольной защите АО РНПК.

### Доступность

* Пользователи должны получать доступ к приложениям ИС посредством web-интерфейса, с использованием web-браузера.
* Доступ к веб-интерфейсу должен быть организован по протоколу HTTPS (с применением криптографического протокола TLS не ниже версии 2.0).
* Пользователи должны получать доступ к ИС посредством web-браузера на базе Chromium, российского производства, в том числе: Uran; Атом; Яндекс браузер.

### Среды информационной системы

В ИС должна быть реализована среда промышленной эксплуатации, среда тестирования, среда разработки. Среды тестирования и разработки не должны иметь доступ к базам данных среды промышленной эксплуатации.

Представители подрядной организации, осуществляющие доработку ИС и/или доработку программного обеспечения ИС и/или техническую поддержку, не должны иметь доступ к среде промышленной эксплуатации.

4.7.8 Требования по отказоустойчивости:

* Система должна разрабатывается с учетом возможности балансировки нагрузки между отдельными модулями и компонентами. При этом выход из строя отдельных компонентов или модулей Системы не должно сказываться на общей функциональности остальной части Системы.
* В рамках разработки Системы должны быть встроены процессы резервного копирования и восстановления данных, обрабатываемых в Системе. Процесс резервного копирования не должен работать с резервируемыми данными в монопольном режиме.

### Требования к окружению:

* Разрабатываемая Система должна корректно функционировать с используемыми АО РНПК:
* средствами обеспечения безопасности рабочих станций и серверов, например, антивирусами, средствами обнаружения и предотвращения вторжений, средствами межсетевого экранирования, и т.д.;
* ОС, СУБД, прикладными программами;
* Компоненты системы, включая программное и аппаратное обеспечение, не должны содержать недокументированных возможностей, направленных на скрытый контроль пользователей или администраторов системы;
* На компонентах Системы должны быть запущены только те сервисы и приложения, которые необходимы для функционирования данной Системы или других систем (при совместном использовании компонента).

## Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

Инсталляционный пакет Системы должен храниться на внешних носителях в количестве не менее двух копий в защищенном от несанкционированного доступа и механических повреждений месте, под контролем администратора системы.

Регламент обслуживания Системы должен быть разработан Исполнителем на этапе подготовки эксплуатационной документации и включен в реестр сервисной документации.

## Требования по сохранности информации при авариях

Сохранность информации в Системы должна обеспечиваться резервным копированием.

Должна быть обеспечена возможность настройки резервного копирования данных, программного обеспечения и настроек Системы. Периодичность и глубина хранения резервных копий детально определяются на этапе технического проектирования.

Время восстановления после отказа, вызванного сбоем электропитания технических средств (иными внешними факторами), не фатальным сбоем (не крахом) операционной системы, не должно превышать 30-ти минут при условии соблюдения условий эксплуатации технических и программных средств.

Время восстановления после отказа, вызванного неисправностью технических средств, фатальным сбоем (крахом) операционной системы, не должно превышать времени, требуемого на устранение неисправностей технических средств и переустановки или восстановления программных средств из резервной копии.

## Требования к надежности, производительности и показателям назначения

### Показатели назначения

Обеспечение пропускной способности не менее 100 000 сообщений в секунду (в целевой реализации). На этапе внедрения требования по пропускной способности составляют до 1 000 сообщений в секунду.

### Надежность

При выполнении приложений должно обеспечиваться штатное функционирование Системы в части:

* устойчивости к некорректным действиям пользователей;
* контролю корректности вводимой информации;
* наличию возможностей предоставления точной и полной картины функционирования системы в любой момент времени.

Причинами возникновения сбоев Системы могут послужить:

* нарушение функционирования каналов передачи данных;
* сбои в работе системного программного обеспечения или аппаратного обеспечения;
* превышение выделенного дискового пространства;
* ошибки в собственном программном обеспечении Системы.

Действия администратора Системы в случае возникновения сбоев в работе системы по каждой из вышеуказанных причин должны быть регламентированы в руководстве администратора Системы.

Защита от возможных некорректных действий конечных пользователей должна быть предусмотрена в программном обеспечении интерфейса пользователя за счет:

* наличия процедур обработки не предусмотренных правилами работы с системой действий пользователя;
* наличия функций выдачи предупреждений пользователю о возможной потере информации в результате его действий, приводящих к удалению информации из базы данных.
* Защита от возможных некорректных сообщений, передаваемых в систему должна быть обеспечена за счет функции централизованного управления схемами данных

Система должна функционировать в отказоустойчивом режиме за счет реализации следующих функций:

* + Репликация для обеспечения отказоустойчивости. Каждый топик может быть разделен на несколько партиций, и каждая партиция может иметь несколько реплик, распределенных по разным серверам.
  + Фиксация записей: Запись всех сообщений в журнал фиксации, который является упорядоченным и неизменяемым списком записей.
  + Обработка ошибок: Механизмы для обработки ошибок и восстановления данных. Например, если лидер-реплика партиции становится недоступной, одна из следящих реплик может быть повышена до лидера, чтобы обеспечить непрерывную доставку сообщений.
  + Гарантии доставки: Различные уровни гарантий доставки сообщений, включая хотя бы один раз, не более одного раза, ровно один раз.
  + Проверка состояния: Контроля состояния для мониторинга состояния реплик и обеспечения их синхронизации.
  + Хранение данных: Настройка периода хранения данных

## Требования к видам обеспечения

### Требования к организационному обеспечению

В ходе разработки должно обеспечиваться постоянное взаимодействие между сторонами, для чего ими должны быть сформированы рабочие группы по данному этапу проекта, включающие, как минимум, лиц, ответственных за:

* решение административных вопросов (организация встреч, предоставление допусков, рассмотрение и согласование документации и т.п.);
* решение инженерно-технических вопросов (согласование технических аспектов реализации и администрирования системы, определение наличия и размещения технических средств, коммуникаций и т.п.);
* нормативно-методическое и информационное обеспечение проектных работ, включая необходимое консультирование, организацию интервьюирования экспертных групп с целью уточнения функциональных характеристик подсистем и т.п.;
* согласование.

Члены рабочих групп должны иметь необходимый уровень компетенции, в том числе, для принятия (организации принятия) оперативных решений по вопросам разработки.

### Требования к методическому обеспечению

При разработке Системы и создании документации на нее, следует руководствоваться следующими нормативными документами:

* ГОСТ 34.602-89 "Техническое задание на создание автоматизированной системы";
* ГОСТ 34.201-89. "Виды, комплектность и обозначение документов при создании автоматизированных систем";
* ГОСТ 34.601-90 "Автоматизированные системы. Стадии создания";
* РД 50-34.698-90 "Автоматизированные системы. Требования к содержанию документов".

Всё прикладное программное обеспечение, поставляемое и разрабатываемое в рамках проекта, должно поставляться в комплекте с «Руководством пользователя» и «Руководством администратора»

Так же требуется «Регламент добавления безопасных библиотек в Программное средство управления сборочными зависимостями», «Комплект документации на программную платформу»;

### Требования к программному обеспечению

Программное обеспечение должно быть основано на типовых промышленных компонентах, в том числе с открытым кодом.

Запрещается использование иностранного проприетарного ПО, а также ПО с открытым исходным кодом, техническая поддержка и сопровождение которого не осуществляется российскими компаниями, обладающими соответствующими компетенциями.

Система должна функционировать на базе серверной операционной системы Astra Linux SE.

Взаимодействие компонентов системы должно осуществляться по выделенным портам.

Правила настроек межсетевых экранов должны быть описаны на этапе детального технического проектирования.

### Требования к техническому обеспечению

Требования к архитектуре Системы должны быть определены на этапе технического проектирования.

Требования к КТС и спецификация серверов (ВМ) должны быть определены на этапе технического проектирования.

# СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

## Требования к выполнению работ

В рамках создания Системы должны быть выполнены следующие работы в соответствии с таблицей «План-график разработки Системы».

Исключительные права на результаты интеллектуальной деятельности, полученные в ходе выполнения работ, принадлежат Заказчику после подписания акта сдачи-приемки работ по соответствующем этапу работ.

Неисключительные права на все лицензируемые компоненты Системы должны быть переданы не позднее последнего этапа разработки Системы по лицензионному (сублицензионному) соглашению между Заказчиком и вендором продукта.

Разработка Системы осуществляется поочередно и поэтапно.

**Рекомендательный срок выполнения этапов Технического проектирования и Разработки системы (к Опытно-промышленной эксплуатации системы) - 25.12.2024.**

Таблица «План-график разработки Системы»

(сроки работ представлены для примера заполнения):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование группы работ | Выполняемые работы | Сроки исполнения | Отчётная документация  (результат работ) |
| 1 | Этап: Подготовительный | | | |
| 1.1. | Подготовительные работы | Формирование рабочей группы проекта из числа сотрудников Исполнителя и Заказчика из постоянных участников и представителей АО РНПК, привлекаемых к работе.  В течение 5 рабочих дней с даты подписания Договора Исполнителем должен быть разработан и передан на утверждение Заказчику детализированный план-график работ с детализацией задач до 1-й календарной недели по всем этапам работ по Договору.  Запрос доступов к информационным ресурсам Заказчика, необходимым для выполнения работ по договору. | Начало работ:  С даты подписания договора между Заказчиком и Исполнителем.    Окончание работ:  Не позднее 2 (двух) календарных недель с даты начала работ по первому этапу Договора. | * Исходящее письмо от Исполнителя в адрес Заказчика с указанием состава сотрудников проектной (рабочей) группы Исполнителя. * Электронный план-график работ. * Обеспечен доступ сотрудников Исполнителя к информационным ресурсам Заказчика. |
| 1.2. | Обследование объекта автоматизации и уточнение требований настоящих ФТ | проводится анализ следующих объектов:  - организационная структура, обязанности и квалификация персонала Администраторов системы и работников СИБ РНПК;  - имеющиеся средства и механизмы информационной безопасности, предоставляемые СИБ РНПК;  - функциональные возможности ПО ИСИП, в том числе по информационной безопасности;  - процессы сопровождения и обеспечения функционирования ИСИП;  - данные о функционировании компонентов и приложений ИСИП;  - решения по интеграции ИСИП со смежными ИС;  - документация на смежные ИС;  - информационные потоки, виды входящей и исходящей информации ИСИП.  В рамках обследования Заказчик предоставляет Исполнителю всю необходимую документацию для работ по проекту,  Исполнитель выполняет интервьюирование сотрудников Заказчика.  Исполнитель выполняет анализ и детализацию требований к Системе. | * Общее описание системы * Акт сдачи-приемки работ * Отчет об обследовании |
| 2. | Этап: Техническое проектирование и разработка Системы | | | |
| 2.1. | Разработка требований к программному обеспечению, входящему в состав ИСИП и его интеграции с СИБ РНПК | В рамках данного этапа Исполнитель формирует требования по разработке ПО, входящего в состав Системы, с учетом требований настоящих ФТ и решений по и обеспечению информационной безопасности Системы. | Начало работ:  С даты завершения работ по Этапу 1.    Окончание работ:  Не позднее 4 (четырех) недель с даты начала работ по второму этапу Договора. | * Частное техническое задание * Чек лист доработок |
| 2.2. | Настройка/доработка поставляемого программного обеспечение под требования ИСИП | Настройка/доработка в соответствии с ЧТЗ компонентов входящих в состав ИСИП | * Акт сдачи-приемки работ * Погашенный чек лист |
| 2.3. | Разработка эксплуатационной документации | Исполнитель выполняет проектирование и разработку решений по созданию Системы в соответствии с требованиями ГОСТ 34.201-89 «Виды, комплектность и обозначения документов при создании автоматизированных систем» и РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»  Вся отчетная документация, разработанная Исполнителем перед завершением всех работ, должна отражать состояние проектируемых решений, соответствующие состоянию ИТ-инфраструктуры, при котором были пройдены последние успешные приемо-сдаточные испытания, в том числе, если по итогам приемо-сдаточных испытаний требуется внесение изменений в проектное решение. | * Ведомость технического проекта; * Пояснительная записка к техническому проекту; * Описание автоматизируемых функций; * Описание информационного обеспечения системы; * Описание комплекса технических средств; * Описание программного обеспечения. |
| 2.4 | Пусконаладочные работы |  | * Программное обеспечение Системы, установленное на КТС Заказчика в тестовом контуре; * Акт сдачи-приемки работ. |
| 3. | Этап: Опытно-промышленная эксплуатация | | | |
| 3.1 | Проведение предварительных испытаний |  | Начало работ:  С даты завершения работ по Этапу 2.    Окончание работ:  Не позднее 2 (двух) недель с даты начала работ по второму этапу Договора. | * Протокол предварительных испытаний * Акт о приемке системы в опытную эксплуатацию |
| 3.2 | Инструктаж пользователей |  | * Протокол инструктажа пользователей |
| 3.3 | Опытная эксплуатация |  | * Журнал опытной эксплуатации * Акт о завершении опытной эксплуатации |
| 3.4 | Проведение приемочных испытаний |  | * Протокол приёмочных испытаний * Акт сдачи-приемки работ |
| 4. | Этап: Сопровождение | | | |
| 4.1 | Гарантийная техническая поддержка |  | Начало работ:  С даты подписания Акта о приемке системы    Окончание работ:  Не позднее 1 (одного) года с даты начала работ по четвертому этапу Договора. |  |

## Требования к исполнителю работ

Наличие у подрядной организации информационной системы лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Поскольку в рамках данного проекта предусмотрена интеграция с платформой JMIX, то подрядчик должен являться партнером вендора JMIX.

Система должна функционировать без обращений к внешним по отношению к Заказчику, в том числе облачным, сервисам.

Разрабатываемые и внедряемые ИТ-решения должны быть задокументированы, соответствовать требованиям действующего законодательства РФ. Данные услуги входят в состав работ Исполнителя, при необходимости допускается привлечение субподрядной организации (обязательно согласование с Заказчиком).

Разработанные процессы, документы и технические решения должны соответствовать Политики информационной безопасности акционерного общества «Российская Национальная Перестраховочная Компания» Протокол от «22» июня 2017 г. № 17-2017г., Приказу «О введении режима коммерческой тайны в АО РНПК» № 0068 от 27 декабря 2017г., Приказу Об утверждении Положения о комиссии по организации обработки и обеспечению безопасности персональных данных в Акционерном обществе «Российская Национальная Перестраховочная Компания» и Положения об обработке персональных данных в Акционерном обществе «Российская Национальная Перестраховочная Компания» № 078 от 24 декабря 2018г., Инструкции по парольной защите АО РНПК № 01 от 14 января 2018г., в том числе (но не ограничиваясь), Заказчик обязуется ознакомить Исполнителя с необходимыми документами, после заключения Соглашения о неразглашении конфиденциальной информации.

К работе по развертыванию и внедрению информационной системы допускаются только граждане Российской Федерации, прошедшие проверку Отделом экономической безопасности РНПК.

## Требования к взаимодействию Исполнителя и Заказчика

При рабочем взаимодействия между Заказчиком и Исполнителем допускается использовать следующие виды каналов коммуникаций:

* электронная почта;
* телефон;
* система онлайн-конференций Толк (https://rnrc.ktalk.ru/);
* другие технические средства связи доступные как Заказчику, так и Исполнителю;
* переписка с использованием почтовой корреспонденции (услуги Почты РФ, курьерская доставка).

Не реже одного раза в неделю Исполнитель должен обеспечить присутствие рабочей группы Исполнителя на рабочих (оперативных) совещаниях с представителями рабочей группы Заказчика посредством видеоконференцсвязи, либо очно по требованию Заказчика.

В случае возникновения инцидентов (нештатного функционирования Системы, аварийных сбоях), срочных задач, по запросу Заказчика, Исполнитель обеспечивает присутствие членов рабочей группы на оперативных совещаниях Заказчика. Инициировать подобные совещания может как Заказчик, так и Исполнитель.

Рекомендуемые способы фиксации результатов совещаний:

* электронное письмо участникам совещания с оформлением резюме (протокола) в тексте письма;
* электронное письмо участникам совещания с оформлением резюме в формате ODT (формат согласуется предварительно с Заказчиком);
* проектное или техническое решение, оформленное в виде отчетного документа и направленное на утверждение Заказчику;
* в виде протокола производственного совещания, направленного на согласование в СЭД Заказчика.

Формализацию результатов и предоставление на согласование итогового протокола совещания рабочей группы руководителю проекта от Заказчика осуществляет Исполнитель, если не оговорено иное в начале совещания.

Исполнитель обеспечивает ведение и поддержание в актуальном состоянии следующих рабочих документов (формат согласовывается с Заказчиком):

* детальный календарный план-график работ по проекту;
* еженедельный статус - отчет о выполненных и планируемых работах. Формат согласовывается с Заказчиком в течении 10 рабочих дней с даты подписания Договора;
* протоколы рабочих совещаний участников проекта;
* реестр рисков проекта.

## Требования к работам по оказанию услуг технической и консультационной поддержки пользователей Системы

С даты ввода Системы в опытную эксплуатацию Исполнитель предоставляет Заказчику услуги по технической и консультационной поддержке пользователей Заказчика, подключенных к Системе.

Силами Исполнителя должны быть организована горячая линии консультационной и технической поддержки. Контактные данные горячей линии поддержки должны быть переданы специалистам Заказчика перед началом опытной эксплуатации Системы.

# ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

## Виды, состав, объем и методы испытаний системы и ее составных частей (виды испытаний в соответствии с действующими нормами, распространяющимися на разрабатываемую систему)

Тестирование прототипа Системы должно быть выполнено на инфраструктуре Исполнителя в соответствии с программой тестирования, представленной Заказчиком. Результаты тестирования фиксируются в Журнале опытной эксплуатации, подписываемом Заказчиком и Исполнителем.

Приемо-сдаточные испытания (ПСИ) Системы должны быть выполнены на технической инфраструктуре Заказчика представителями Заказчика и Исполнителя согласно Программе приёмо-сдаточных испытаний Системы. Результаты выполнения ПСИ фиксируются в Протоколе (Акте) проведения ПСИ, подписываемом Заказчиком и Исполнителем. ПСИ Системы проводятся на предмет соответствия требованиям настоящих ФТ.

Программа и методика проведения приемо-сдаточных испытаний должна включать следующие проверки:

- оценку и установление факта достижения требований к успешности выполнения работ;

- соответствие функционирования внедряемых решений параметрам штатного функционирования программного обеспечения на площадках Заказчика;

- соответствие внедряемых решений требованиям проектного решения;

- соответствие внедряемых решений требованиям частного технического задания;

- комплектность и качество документации.

Программа и методика приемо-сдаточных испытаний предоставляется Исполнителем на согласование и утверждение Заказчику не позднее, чем за 10 рабочих дней до планируемой даты начала проведения приемо-сдаточных испытаний. В рамках проведения приемо-сдаточных испытаний Исполнитель должен проводить работы по устранению выявленных недостатков, по решению задач эксплуатации и технической поддержки поставляемого ПО в составе ИСИП.

## Общие требования к приемке работ по стадиям (перечень участвующих предприятий и организаций, место и сроки проведения), порядок согласования и утверждения приемочной документации

В случае выявления недостатков в работе Системы и несоответствия требованиям Технического проекта в ходе ПСИ, они фиксируются в Протоколе (Акте) ПСИ и устраняются в сроки, согласованные с Заказчиком. После устранения выявленных недостатков, должны быть проведены повторные испытания, касающиеся зафиксированных недостатков, и подписан Протокол (Акт) соответствия Системы заявленным требованиям.

В рамках ОПЭ к Системы могут быть определены новые дополнительные требования. Управление этими требованиями осуществляется в рамках процедур управления изменениями. Новые требования не являются предметом настоящих ФТ.

Сдача-приёмка результатов работ осуществляется комиссией, в состав которой входят представители Заказчика и Исполнителя. После выполнения работ по каждому из указанных этапов Исполнитель предоставляет Заказчику отчётные документы на электронных носителях не менее, чем за 5 рабочих дней до даты окончания этапа. По результатам приёмки подписывается акт о приёмке услуг.

# ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

## Общие требования

С даты начала работ по соответствующему этапу работ по Договору Исполнитель разрабатывает и согласовывает в рабочем порядке с Заказчиком шаблоны технической и рабочей документации, которые должны быть использованы при разработке технической документации на Систему.

Техническая и эксплуатационная документация, разрабатываемая в рамках выполнения данных работ, должна быть разработана согласно рекомендациям ГОСТ 34.201-89 «Информационная технология. Виды, комплектность и обозначение документов при создании Автоматизированных систем» и РД 50-34.698-90 «Информационная технология. Автоматизированные системы. Требования к содержанию документов».

Анализ и согласование разработанной Исполнителем в ходе выполнения работ документации осуществляется Заказчиком в срок не более 10 рабочих дней со дня ее предоставления. Утверждение документации осуществляется Заказчиком в системе электронного документооборота Заказчика с использование простой электронной подписи.

Документация должна быть предоставлена на русском языке. Документация на предварительное согласование должна поставляться в электронном виде по каналам электронной почты.

Документация, поставляемая на электронных носителях (в форматах Open Document), должна быть отформатирована для печати на бумаге формата A4.

Чертежи и схемы могут поставляться в составе документов или в виде отдельных документов.

Документация должна иметь все сведения, необходимые для запуска Системы (инструкции Администратора) и проверки ее функционирования с помощью соответствующих тестов, изложенных в методике (ПМИ), содержать сведения в объёме, достаточном для эксплуатации Системы (Инструкции пользователя).

## Перечень основных мероприятий и их исполнителей, которые следует выполнить при подготовке объекта автоматизации к вводу Системы в действие

При выполнении работ согласно разделу 5 настоящих ФТ на площадке Заказчика, Заказчик обеспечивает условия для выполнения работ: предоставляет удаленные рабочие места, обеспечивает доступность необходимого программного и технического обеспечения.

Заказчик предоставляет оборудование согласно требованиям, изложенным в разделе «Требования к техническому обеспечению» настоящих ФТ. Заказчик обеспечивает удалённый доступ к ИТ-инфраструктуре с использованием ПО удалённого доступа. Заказчик обеспечивает доступ к информационным ресурсам.

Заказчик формирует группы для обучения, устанавливает даты проведения обучения согласно срокам, указанным в разделе 5 настоящего ФТ.

Для подготовки Системы к ОПЭ должны быть выполнены следующие действия:

* программное обеспечение Системы должно быть установлено на оборудовании Заказчика;
* сервисная документация должна быть размещена в доступной для пользователей системы области;
* Заказчиком должен быть назначен администратор системы.

# ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Должны быть составлены, согласованы с Заказчиком и приняты следующие документы\*:

* Детализированное ТЗ c детализацией требований на разрабатываемые (дорабатываемые) функции Системы;
* Технический проект на Системы и ее компоненты в составе документов:
* Ведомость технического проекта;
* Пояснительная записка к техническому проекту;
* Общее описание системы
* Описание автоматизируемых функций;
* Описание информационного обеспечения системы;
* Описание комплекса технических средств;
* Описание организации информационной базы;
* Описание программного обеспечения;
* Описание комплекса мер и средств защиты информации;
* Описание интеграции информационной системы.
* Эксплуатационная документация на Систему:
* Руководство пользователя (пользователя ИС, пользователь СБ);
* Руководство администратора (администратора ИС);
* Программа и методика испытаний.
* План внедрения Системы, включая план проведения обучения пользователей, тестирования и проведения опытной эксплуатации;
* План запуска Системы в промышленную эксплуатацию.
* Регламент добавления библиотек в Программное средство управления сборочными зависимостями должен описывать процесс проверки библиотек на уязвимости и закладки, требования к отчету по результатам проверки, процесс признания библиотеки безопасной. Данный регламент должен быть согласован с Управлением внутренней и информационной безопасности АО РНПК и Управлением разработки программного обеспечения АО РНПК.
* Комплект документации на программную платформу должен обеспечивать самостоятельное её изучение и создание собственных разработок (например, печатные материалы (Быстрый старт, устройство платформы, коллекция практических рецептов по решению типичных задач, встающих перед разработчиками, особенности работы с базами данных, Подсистема безопасности), видео ролики).\* По согласованию с Заказчиком допустимо объединять некоторые виды документов, либо разрабатывать самостоятельные документы на отдельные компоненты Системы.

# ТРЕБОВАНИЯ К ГАРАНТИЙНОМУ ОБСЛУЖИВАНИЮ

В течение 12 (двенадцати) месяцев с даты подписания между Заказчиком и Исполнителем Акта сдачи-приемки выполненных работ по последнему этапу работ, Исполнитель должен обеспечивать гарантийное сопровождение и соответствие результатов работы требованиям настоящих ФТ, отчетной и проектной документации по Договору, устраняя (с привлечением вендора) выявленные Заказчиком блокирующие и критические дефекты/недостатки в работе Системы. Исполнитель совместно с вендором обеспечивает устранение выявленных Заказчиком дефектов/недостатков за свой счет. Под гарантийным обслуживанием понимается обслуживание

Исполнитель в течение гарантийного срока, оговоренного в Договоре, должен осуществлять гарантийное сопровождение Системы. На протяжении этого срока Исполнитель (совместно с вендором) обязуется :

- Устранять ошибки, связанные с повышением информационной безопасности системы (если OpenSource)

* устанавливает релизы, обусловленные устранением критических ошибок в системе;
* устанавливает релизы, связанные с повышением информационной безопасности системы;
* устанавливает релизы, связанные с повышением быстродействия системы;
* устанавливает релизы, связанные с плановым обновлением (улучшениями) компонентов системы.

# ИСТОЧНИКИ РАЗРАБОТКИ

## Документы и информационные материалы, на основе которых разрабатывались ФТ

* ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
* ГОСТ 34.601-90 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
* ГОСТ 34.201-89 «Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
* ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем»;
* ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы»;
* РД50-34.698-90 «Методические указания. Автоматизированные системы. Требования к содержанию документов».