Приложение 2 к конкурсной документации

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на выполнение опытно-конструкторских работ по созданию опытного образца комплексного сервиса системы контроля и управления функционированием (СКУФ) облачной платформы и оказание услуг по внедрению СКУФ

Оглавление

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование Системы

Полное наименование Системы: Информационная система «Система контроля и управления функционированием (СКУФ) облачной платформы»

1.2. Условное обозначение Системы

Условное обозначение Системы: СКУФ

1.3. Заказчик

– полное наименование: Открытое акционерное общество междугородной и международной электрической связи «Ростелеком» (далее - Заказчик);

– сокращенное наименование: ОАО «Ростелеком»;

– место нахождения: 191002, РФ, г. Санкт-Петербург, ул. Достоевского, д. 15;

– адрес для переписки: 125047, РФ, г. Москва, ул.1-я Тверская-Ямская, д. 14.

1.4. Исполнитель

Определяется по результатам проведения конкурсной процедуры в соответствии с Федеральным законом от 21.07.2005 г. № 94-ФЗ «О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд» (далее - Исполнитель).

1.5. Основание для выполнения работ

– Программа инновационного развития ОАО «Ростелеком».

1.6. Плановые сроки оказания услуг

Сроки начала и окончания выполнения работ определяются Календарным планом выполнения работ (приложение № 1 к настоящему Техническому заданию) и договором, заключаемым по итогам запроса предложений.

1.7. Источник финансирования

Финансирование работ осуществляется за счет средств Заказчика, выделяемых на указанные работы.

1.8. Порядок финансирования

Порядок финансирования работ определяется действующими нормативно-правовыми актами Российской Федерации и договором, заключаемым с Исполнителем работ по результатам открытого запроса предложений (далее – Договор).

1.9. Порядок оформления и предъявления Заказчику результатов выполненных работ

Результаты выполненных работ передаются Заказчику в порядке, определенном Договором в соответствии с Календарным планом выполнения работ, являющимся неотъемлемой частью Договора.

Исполнитель представляет Заказчику исходные коды для размещения в репозитории на CD носителях в установленном Договором порядке.

Документация на Систему передается на бумажных (два экземпляра) и на машинных носителях (CD/DVD). Текстовые документы, передаваемые на машинных носителях, должны быть представлены в форматах MSOffice.

Все материалы передаются с сопроводительными документами Исполнителя.

1.10. Перечень нормативно-технических документов, методических материалов, регламентирующих выполнение работ

Выполняемые работы и оформление их результатов должны отвечать требованиям государственных стандартов из числа Комплекса стандартов на автоматизированные системы:

– ГОСТ 12.2.003 «Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности»;

– ГОСТ 19542–83 «Совместимость средств вычислительной техники электромагнитная. Термины и определения»;

– ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение»;

– ГОСТ 25861-83 «Машины вычислительные и системы обработки данных. Требования по электрической и механической безопасности и методы испытаний»;

– ГОСТ 27.001-95 «Надежность в технике. Основные положения»;

– ГОСТ 27.003.90 «Надежность в технике. Состав и общие правила задания требований по надежности»;

– ГОСТ Р 50628-2000 «Совместимость технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний»;

– ГОСТ 27201–87 «Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования»;

– ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;

– ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

– ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Стадии создания»;

– ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

– ГОСТ 34.603-92 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем»;

– РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов».

1.11. Перечень сокращений

Сокращение	Полное наименование
CMDB	База данных, используемая для хранения Записей о КЕ на всем протяжении их Жизненного цикла
OLA	Внутреннее соглашение, обеспечивающее надлежащую поддержку организации ИТ в предоставлении своих собственных услуг ИТ, содержащее технические параметры
SLA	Соглашение об уровне сервиса или соглашение о качестве предоставления услуги/сервиса — формальный договор между потребителем услуги/сервиса и ее поставщиком, содержащий описание услуги, права и обязанности сторон и, самое главное, согласованный уровень качества предоставления данной услуги.
Upgrade	Программно-аппаратная модернизация ИТ-инфраструктуры
Администратор СРК	Сотрудник Исполнителя, осуществляющий поддержку работоспособности и решение вопросов связанных с функционированием СРК Заказчика.
АИС	Автоматизированная информационная система.
АПК	Автоматизированный программный комплекс
АРМ	Автоматизированное рабочее место
Архивирование	Перемещение (копирование с последующим удалением источника) необходимых данных и программ на резервное хранилище данных (накопители на жестких магнитных дисках, ленточные, оптические накопители и т.д.)
БД	База данных
ГУЦ	Информационная система головного удостоверяющего центра
ГЭПС	Государственная электронная почтовая система
ЕНСИ	Единая система нормативно-справочной информации
ЕПГУ (РПГУ)	Единый портал государственных и муниципальных услуг (региональный портал государственных и муниципальных услуг)
ЕСИА	Единая система идентификации и аутентификации
Заявка	запрос сотрудника Заказчика (Исполнителя) к службе технической поддержки Исполнителя на решение какой-либо технической проблемы; заявка содержит описание проблемы и электронный адрес сотрудника.
Заказчик	ОАО «Ростелеком»
ИБ	Информационная безопасность
Изменение (CHG)	Добавление, модификация или удаление компонентов ИЭП, способное оказать влияние на функционирование ИЭП или на сервисы поддержки ИЭП.
Инфраструктура	Инфраструктура Облачной платформы ОАО «Ростелеком», включающая в себя: оборудование, каналы связи, системное и прикладное ПО, сервисы обеспечивающие функционирование ИЭП и Облачной платформы.
Инфраструктура электронного правительства (ИЭП)	Совокупность автоматизированных и телекоммуникационных систем, обслуживающих процессы информационного взаимодействия всех субъектов электронного правительства созданных в рамках ФЦП «Электронная Россия» (Федеральная целевая программа «Электронная Россия (2002-2010) годы») и ФЦП «Информационное общество» (Государственная программа Российской Федерации «Информационное

Сокращение	Полное наименование
	общество (2011 – 2020 годы)»
Инцидент (INC)	Любое событие, не являющееся частью стандартного функционирования сервиса, которое приводит или может привести к сбою в предоставлении или понижению качества услуг, предоставляемых Пользователям.
Инцидент ИБ	Событие или последовательность событий, приведших к нарушению свойств безопасности защищаемой информации, технических или программных средств, предназначенных для ее обработки, репутации владельца и других активов.
ИПШ	Система «Информационно-платежный шлюз»
ИТ-инфраструктура	Совокупность аппаратного и программного обеспечения компании Заказчика, а также правил и методов их настройки, обеспечивающих технологию совместной работы сотрудников Заказчика.
КЕ	Конфигурационная единица. Любой обнаруженный компонент, необходимый для того, чтобы предоставлять ИТ-услугу. Информация о каждой КЕ регистрируется в форме Записи о КЕ в Системе управления конфигурациями и поддерживается актуальной в течение всего Жизненного цикла процессом Управления конфигурациями. КЕ находятся под контролем Управления изменениями. Типичными примерами КЕ являются ИТ- услуги, оборудование, программное обеспечение, здания, люди и документы, такие как Процессная документация и Соглашения об уровне услуг (SLA).
КЦОД РИЭП	Коллективные центры обработки данных региональной инфраструктуры Электронного правительства
ЛП	Линия поддержки
Модель здоровья	Перечень метрик мониторинга и их граничных значений, позволяющий определить штатный режим функционирования информационной системы
Наряд на работу (WO), Задача	Задание на производство работы, оформленное по установленной в форме и определяющее содержание, место работы, время ее начала и окончания, условия ее выполнения, ответственного за выполнение работы.
ОП	Облачная платформа ОАО «Ростелеком»
ОС	Операционная система
ПГП	Информационная система для анализа информации о государственных и муниципальных торгах на реализацию (продажу)
ПМ	Подсистема мониторинга
ПО	Программное обеспечение
ПОИБ	Программное обеспечение информационной безопасности
Резервирование	Копирование необходимых данных на резервное хранилище данных и программ (накопители на жестких магнитных дисках, ленточные, оптические накопители и т.д.)
РОИВ	Региональный орган исполнительной власти
Сервисно-ресурсная модель	Логическая модель сервиса, описывающая состав и взаимосвязи конфигурационных единиц (ресурсов), которые совместно обеспечивают предоставление сервиса на согласованном уровне.
СКЗИ	Средства криптографической защиты информации
СКИМ	Система контроля и мониторинга функционирования электронного правительства
СКУФ	Система контроля и управления функционированием облачной платформы.

Сокращение	Полное наименование
	Автоматизированная информационная система, реализующая функции управления ИТ-процессами и мониторинга Инфраструктуры.
СМУ	Система обеспечения взаимодействия мобильных устройств с инфраструктурой электронного правительства
СМЭВ (РСМЭВ)	Система межведомственного электронного взаимодействия (Региональная СМЭВ). Представляет собой федеральную, а также региональные государственные информационные системы, включающую информационные базы данных, в том числе содержащие сведения об используемых органами и организациями программных и технических средствах, обеспечивающих возможность доступа через систему взаимодействия к их информационным системам (далее - электронные сервисы), сведения об истории движения в системе взаимодействия электронных сообщений при предоставлении государственных и муниципальных услуг, исполнении государственных и муниципальных функций в электронной форме, а также программные и технические средства, обеспечивающие взаимодействие информационных систем органов и организаций через СМЭВ
СМФЦ ИОД	Информационная система мониторинга функционирования центров общественного доступа и инфраструктуры общественного доступа
СОИБ	Система обеспечения информационной безопасности
СПД	Система передачи данных
СРК	Система резервного копирования – программно-аппаратный комплекс, обеспечивающий резервирование, архивирование, хранение и восстановление данных и программ.
СУБД	Система управления базами данных
СХД	Система хранения данных
Техпортал СМЭВ	Технический портал Системы межведомственного электронного взаимодействия
УВИРИ	Автоматизированная информационная система «Управление ведомственной и региональной информатизацией»
Управление конфигурациями	Учет ПО и оборудования, их конфигураций, взаимосвязей и сервисов, а также поддержание собранной информации в актуальном состоянии, обеспечение процессов ИТ точной информацией о конфигурациях оборудования и ПО
УЦЭП	ИТ-инфраструктура удостоверяющего центра электронного правительства
Уязвимость ИБ	Недостаток или слабое место в системе, эксплуатация которого может привести к инциденту информационной безопасности.
ФОИВ	Федеральный орган исполнительной власти
ФРГУ	Федеральный реестр государственных и муниципальных услуг (функций)
ФЦОД ЭП	Федеральный центр обработки данных электронного правительства
ЭП	Электронное правительство
ЭС ЦТО	Экспертная система центров телефонного обслуживания

2. НАЗНАЧЕНИЕ, ЦЕЛИ И ЗАДАЧИ РАБОТ

2.1. Назначение работ

Назначением выполнения работ является обеспечение эффективного и безотказного функционирования инфраструктуры электронного правительства путем внедрения единой информационной системы автоматизации процессов управления и мониторинга ИЭП - информационной системы «Система контроля и управления функционированием» (далее – Система).

2.2. Цели работ

Целями внедрения Системы являются:

– Повышение надежности функционирования Инфраструктуры;

– Поддержка процессов принятия решений, направленных на совершенствование эксплуатации Инфраструктуры и отслеживание их эффективности на основе реализуемых в Системе инструментальных средств;

– Мониторинг и своевременное оповещение о возможных сбоях систем, информационных ресурсов и сервисов (сокращение времени обнаружения и локализации инцидентов, проблем).

2.3. Задачи работ

Для достижения выше указанных целей должны быть решены следующие задачи:

– Разработаны, автоматизированы и внедрены процессы обслуживания Инфраструктуры;

– Внедрены следующие подсистемы:

- подсистема «Комплексный сервис системы контроля и управления функционированием (СКУФ)», включающая в себя следующие компоненты;
    - подсистема мониторинга в составе СКУФ;
- подсистема управления знаниями и документацией;
- подсистема управления версиями;
- подсистема мониторинга ИЭП;
- подсистема управления сетевым адресным пространством инфраструктуры ЭП;
- подсистема автоматизации установки релизов ИС ИЭП;
- подсистема информационной безопасности;
- подсистема мониторинга и контроля оборудования ЭП;
- внедрение политик СРК на основании SLA и RTO эксплуатируемых систем;
- внедрение эксплуатационных инструкций на типовые операции инженеров и администраторов вычислительной инфраструктуры ЭП.

– Собраны, верифицированы и введены в систему данные о конфигурации аппаратно-программных компонентов Инфраструктуры;

– Разработан Технический проект.

3. ХАРАКТЕРИСТИКИ ОБЪЕКТА АВТОМАТИЗАЦИИ И МОНИТОРИНГА

3.1. Сведения об объектах автоматизации и мониторинга

Объектами автоматизации и мониторинга по результатам выполнения работ будет являться инфраструктура облачной платформы, а также информационные системы, размещенные на облачной платформе.

Кроме того, объектами автоматизации и мониторинга будут являться информационные системы проекта «Информационное общество», включая следующие элементы Инфраструктуры:

1. ГУЦ;
2. ГЭПС;
3. ЕНСИ;
4. ЕПГУ;
5. ЕСИА;
6. ИПШ;
7. ОП;
8. ПГП;
9. РПГУ;
10. РСМЭВ;
11. СКИМ;
12. СМУ;
13. СМФЦ ИОД.
14. СМЭВ;
15. УВИРИ;
16. ФРГУ;
17. ЭС ЦТО.

3.2. Общие принципы выполнения работ

В соответствии с РД 50-680–88 при внедрении Системы необходимо руководствоваться принципами системности, развития (открытости), совместимости, стандартизации (унификации) и эффективности.

3.3. Принцип концептуального единства

Развитие Системы должно осуществляться в соответствии утвержденными нормативными правовыми актами РФ и субъектов РФ, нормативно-методическими и нормативно-техническими документами, регламентирующими порядок создания, разработки, внедрения и эксплуатации автоматизированных систем.

3.4. Принцип развития (модифицируемости)

Система должна обеспечивать возможность дальнейшего развития, расширения и интеграции с другими системами (подсистемами, компонентами).

Технические решения, используемые в процессе внедрения и развития Системы должны позволять минимизировать трудозатраты по модернизации, необходимые в связи с принятием новых нормативно-правовых актов, приводящих к изменению технологического процесса.

3.5. Принцип мобильности

Все виды обеспечения внедряемой Системы должны обладать максимальной независимостью от конкретных типов применяемых технических и программных средств.

3.6. Принцип относительной независимости (принцип модульности)

Внедрение Системы должно быть реализовано как совокупность отдельных максимально независимых функциональных компонентов.

3.7. Принцип открытости

Система должна быть способна к интеграции в свою среду новых подсистем, расширения функций уже имеющихся, а так же обеспечивать возможность интеграции с внешними ИС. В Системе должны применяться общепринятые стандарты на правила передачи (протоколы, интерфейсы) и хранения информации.

3.8. Принцип многоуровневости

Процесс предоставления государственных, муниципальных и иных услуг имеет многоуровневую организационную структуру.

Внедрение Системы должно решать проблемы, которые ставятся и (или) решаются на каждом уровне.

3.9. Принцип санкционированного доступа к информации

Система должна обеспечивать санкционированный доступ к информации. Система должна иметь функции администрирования, которые позволяют устанавливать пользователям права доступа к информации или это должно решаться в рамках иной управляющей подсистемы (компонента).

4. ТРЕБОВАНИЯ К СИСТЕМЕ И РАБОТАМ

4.1. Требования в целом

Система должна функционировать в среде виртуализации, обладать показателями надежности, доступности и производительности в соответствии с требованиями, предусмотренными настоящим Техническим заданием, масштабируемой как по производительности каждого входящего в ее состав средства вычислительной техники (СВТ), так и по производительности каждого компонента.

Система должна удовлетворять следующим основным требованиям:

– Обеспечивать возможность использования Системы через сеть ОП и/или сеть Internet;

– Обеспечивать разделение доступа к данным и функциям Системы согласно ролевой модели.

4.2. Требования к опытному образцу Системы

Опытный образец Системы должен состоять из следующих подсистем:

– подсистема «Комплексный сервис системы контроля и управления функционированием (СКУФ)», включающая в себя следующие компоненты;

– подсистема мониторинга в составе СКУФ;

– подсистема управления знаниями и документацией;

– подсистема управления версиями;

– подсистема мониторинга ИЭП;

– подсистема управления сетевым адресным пространством инфраструктуры ЭП;

– подсистема автоматизации установки релизов ИС ИЭП;

– подсистема информационной безопасности;

– подсистема мониторинга и контроля оборудования ЭП;

– внедрение политик СРК на основании SLA и RTO эксплуатируемых систем;

– внедрение эксплуатационных инструкций на типовые операции инженеров и администраторов вычислительной инфраструктуры ЭП.

4.3. Требования к надежности

Спроектированные архитектурные решения Системы должны быть устойчивы по отношению к программно-аппаратным ошибкам, отказам технических и программных средств, с возможностью восстановления ее работоспособности и целостности информационного содержимого при возникновении ошибок и отказов.

Допускается остановка Системы для проведения плановых профилактических работ.

4.4. Критерии отказа Системы и (или) ее компонентов

Система должна относиться к обслуживаемым восстанавливаемым изделиям общего назначения многократного циклического применения.

Надежность должна определяться уровнем безотказности в работе и способностью к восстановлению работоспособности после отказов.

За отказ работоспособности принимается неполучение пользователем ответа на запрос в течение времени, превышающего 3-х минут, без учета времени передачи информации по сети.

Критерии отказа и (или) ее компонентов определяются:

– средним временем наработки на отказ;

– средним временем восстановления работоспособности.

Показатели надежности технических средств компонентов Системы должны оцениваться и контролироваться в соответствии с требованиями и по методикам ГОСТ 27.001-95 на всех этапах жизненного цикла Системы.

4.5. Перечень аварийных ситуаций, приводящих к отказу Системы и (или) ее компонентов и значения соответствующих показателей надежности

Система должна обеспечивать круглосуточный режим функционирования 7 дней в неделю.

Сохранность работоспособности и информации в пределах значений показателей надежности, приведенных в настоящем Техническом задании, должна обеспечиваться при возникновении следующих аварийных ситуаций:

Отказы в системе электроснабжения:

– сбои блоков питания.

Отказы комплекса технических средств (аппаратных средств):

– отказы серверного оборудования;

– отказы сетевого, телекоммуникационного оборудования и каналов связи;

– отказы оборудования подсистемы резервного копирования информации.

Отказы программных средств:

– отказы общесистемного ПО;

– отказы СПО.

Отказы в результате ошибок обслуживающего персонала и пользователей.

4.6. Критичность простоя Системы

Критичность простоя Системы должна определяться на стадии разработки Технорабочего проекта по согласованию с Пользователем в документе Описание программного обеспечения.

4.7. Требования к надежности технических средств и программного обеспечения

К программным средствам Системы предъявляются следующие требования по надежности:

– коэффициент готовности программных средств к работе Системы должен быть не менее 99.95%;

– среднее время восстановления программных средств сервера должно быть не более 80 минут.

Время восстановления работоспособности включает время на диагностирование отказа, замену или ремонт оборудования (без учета времени на заказ и поставку), конфигурирование оборудования и ПО, восстановление данных и тестирование работоспособности оборудования и ПО.

Вопросы обеспечения надежности программного обеспечения должны гарантироваться также авторским сопровождением на всех стадиях жизненного цикла Системы.

4.8. Требования к программным мероприятиям по обеспечению надежности

Надежность Системы должна достигаться комплексом организационных и технических мер, обеспечивающих требуемые уровни безотказности, ремонтопригодности, долговечности и сохранения ресурсов Системы.

Технические меры по обеспечению надежности должны предусматривать:

– резервирование критически важных компонентов и данных Системы и отсутствие единой точки отказа;

– использование программного резервирования (программной избыточности);

– конфигурирование используемых средств и применение специализированного ПО, обеспечивающего высокую надежность.

Организационные меры по обеспечению надежности должны быть направлены на минимизацию ошибок пользователей (а также обслуживающего персонала при эксплуатации и проведении работ по обслуживанию), минимизацию времени ремонта или замены вышедших из строя компонентов за счет:

– обеспечения требуемого уровня квалификации обслуживающего персонала;

– регламентации и нормативного обеспечения выполнения работ обслуживающего персонала и пользователей;

– регламентации проведения работ и процедур по обслуживанию и восстановлению Системы;

– своевременного оповещения пользователей о случаях нештатной работы компонентов Системы;

– своевременной диагностики неисправностей.

4.9. Требования к масштабированию

При увеличении числа интегрируемых систем и/или пользователей Система должна обеспечивать возможность горизонтального масштабирования подсистем путем добавления дополнительных вычислительных мощностей.

Система должна поддерживать возможность балансировки нагрузки на компоненты Системы.

Система должна быть построена по принципу распределенной архитектуры с возможностью обмена информацией между различными частями системы.

4.10. Требования к используемой операционной среде

Компоненты Системы должны быть развернуты на ОС Linux и/или ОС Windows актуальных версий.

Инфраструктурные компоненты Системы – ОС и СУБД – предоставляются Заказчиком в соответствии с требованиями технического проекта.

4.11. Требования к организации доступа

Доступ к функциям и данным Системы должен осуществляться после авторизации пользователя.

Должна обеспечиваться идентификация и проверка подлинности (аутентификация) пользователей при входе в Систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов (или с использованием механизмов одноразовых паролей, цифровых сертификатов, других средств взаимной строгой аутентификации).

Система должна препятствовать доступу к защищаемым объектам не идентифицированных пользователей, пользователей, подлинность идентификации которых при аутентификации не подтвердилась, аутентифицированных пользователей, не наделенных правом доступа к объектам.

Требуется разработать и согласовать с Заказчикам ролевую модель. Для каждой из ролей системы должны быть настроены соответствующие права доступа, меню системы, количество и вид полей на экранных формах, ограничения на редактирование атрибутов объектов согласно ролевой модели. Для администраторов Системы следует предоставить полный доступ ко всем объектам.

Система должна поддерживать работу через протокол https с использованием шифрования, при этом должна быть предусмотрена возможность использования сертификата, предоставленного Заказчиком.

4.12. Требования к рабочим местам

Система должна функционировать, обеспечивая доступ ко всем пользовательским функциям и данным подсистем через web-интерфейс с помощью веб-браузеров: Internet Explorer 7.0, Firefox 4.0 или их более поздних версий.

Для доступа к административным функциям Системы могут предъявляться дополнительные требования к рабочим местам.

4.13. Требования к режимам функционирования

Система должна обеспечивать функционирование в следующих режимах:

– штатный режим (режим, обеспечивающий выполнение повседневных функций);

– сервисный режим (режим для проведения реконфигурирования, обновления и профилактического обслуживания);

Основным режимом функционирования Системы должен являться штатный режим, при котором:

– серверное программное обеспечение реализует возможность круглосуточного функционирования с регламентированными перерывами на техническое обслуживание и обновление программного обеспечения.

В штатном режиме должен быть обеспечен полный набор функций согласно требованиям к Системе.

В штатном режиме Система должна функционировать 24 часа в сутки, 7 дней в неделю, 365 (366) дней в году с заданными показателями надежности и с плановыми перерывами для проведения регламентного или разового обслуживания.

Для обеспечения штатного режима функционирования Системы необходимо соблюдать требования и выдерживать условия эксплуатации программного обеспечения, указанные в соответствующих технических документах (техническая документация, инструкции по эксплуатации и т.д.).

Сервисный режим функционирования должен использоваться для выполнения операций подготовки и проведения испытаний или настройки Системы. В данном режиме осуществляется техническое обслуживание, реконфигурация, модернизация Системы.

4.14. Требования к интеграции

Система должна обеспечить возможность интеграции со следующими внешними системами:

– Системой управления Облачной платформой Заказчика;

– Системами ЭП:

- ЕПГУ (регистрация обращений граждан);
- СМЭВ (взаимодействие с другими системами через СМЭВ);
- ТП СМЭВ (регистрация заявок участников межведомственного взаимодействия, подаваемых через ТП СМЭВ).

– Другими системами (интеграция на базе технологий SNMP и веб-сервисов).

Система должна обеспечивать интеграции с SMS-шлюзом и почтовым сервером для отправки и получения сообщений. Должна быть обеспечена возможность регистрации входящих писем в качестве объектов Системы.

4.15. Требования к лицензированию

Лицензии на используемое при внедрении Системы ПО предоставляются Заказчиком.

4.16. Требования к обучению персонала

Должно быть проведено обучение пользователей Системы: дежурных администраторов и линий технической поддержки Инфраструктуры. Для пользователей Системы должны быть подготовлены ролевые инструкции.

4.17. Требования к способам и средствам связи для информационного обмена между компонентами Системы

В качестве протокола взаимодействия между компонентами Системы на транспортно-сетевом уровне необходимо использовать протокол TCP/IP.

Информационное взаимодействие между компонентами Системы осуществляется посредством доступа к единому хранилищу данных (СУБД).

Для организации информационного обмена между компонентами Системы должны использоваться специальные протоколы прикладного уровня.

4.18. Требования по диагностированию

В части контроля работоспособности и диагностирования неисправностей Системы должна обеспечивать решение перечисленных ниже задач:

– проверку работоспособности и обнаружение отказов;

– передачу информации по электронной почте, уведомлений по протоколу HTTP/HTTPS о возникновении отказа и результатах проверок работоспособности;

– автоматизированный (автоматический) контроль функционирования программных средств Системы с фиксацией в журналах событий (лог-файлах);

– проверку поступающей информации на соответствие формату и диапазону допустимых значений.

4.19. Требования к численности персонала

Персонал разделен на категории:

– обслуживающий персонал:

– системный администратор;

– администратор баз данных;

– пользователи.

Роли системного администратора и администратора баз данных могут быть совмещены в одну роль.

Численность персонала структурных подразделений, обеспечивающих информационное наполнение Системы, должна определяться исходя из основных параметров – объемов обрабатываемых документов.

Структура и конфигурация Системы должны быть спроектированы и реализованы с целью минимизации количественного состава обслуживающего персонала.

4.20. Требования к квалификации персонала, порядку их подготовки и контроля знаний и навыков

Основными обязанностями системного администратора являются:

– установка, настройка и мониторинг работоспособности системного и базового программного обеспечения;

– инсталляция и настройка прикладного программного обеспечения (ПО);

– ведение учетных записей пользователей Системы;

– управление правами доступа пользователей к функциям Системы.

Системный администратор должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию программных средств, применяемых в Системе, а также должен иметь профессиональные знания и практический опыт в области системного администрирования.

Основными обязанностями администратора баз данных являются:

– установка, модернизация, настройка параметров программного обеспечения систем управления базами данных (СУБД);

– оптимизация функционирования прикладных баз данных по времени отклика, скорости доступа к данным;

– резервное копирование и аварийное восстановление данных;

– конфигурирование и настройка программно-технических средств Системы;

– разработка, управление и реализация эффективной политики доступа к информации, хранящейся в прикладных базах данных.

Администратор баз данных должен обладать высоким уровнем квалификации и практическим опытом выполнения работ по установке, настройке и администрированию используемых в Системе СУБД.

Основными обязанностями специалиста по техническому обслуживанию являются:

– модернизация, настройка и мониторинг работоспособности комплекса технических средств (серверов, рабочих станций);

– конфигурирование и настройка программно-технических средств Системы;

– диагностика типовых неисправностей;

– настройка локальной компьютерной сети и сети Интернет;

– контроль доступа к сетевым ресурсам;

– настройка сетевого окружения.

Проведение более сложных операций по обслуживанию и ремонту должно осуществляться силами сервисных служб поставщиков технических средств, входящих в состав программно-аппаратного комплекса Системы.

Квалификация обслуживающего персонала должна позволять:

– использовать стандартные возможности применяемых типовых средств вычислительной техники, ОС, СУБД и другого системного ПО;

– работать с архиваторами, дисковыми утилитами, антивирусными программами и программами резервного копирования;

– определять источник сбоя функционирования и отказа Системы;

– восстанавливать работоспособность Системы после сбоя или отказа;

– проводить регламентные работы и техническое обслуживание Системы;

– обеспечивать требуемые условия эксплуатации Системы.

Пользователи должны пройти обязательную общую и специальную подготовку для работы с Системой и средствами вычислительной техники.

Общая подготовка должна включать в себя получение навыков работы с компьютером и общим ПО (ОС, офисное ПО) в объеме навыков пользователей персональных компьютеров.

Специальная подготовка пользователей должна включать в себя получение знаний и навыков работы с комплексом технических средств и СПО в объеме, необходимом для исполнения своих должностных обязанностей.

Пользователи должны обладать знаниями и навыками работы в качестве пользователя персональных компьютеров в соответствии с Приложением к приказу Мининформсвязи России от 27.12.2005 г. № 147 «Квалификационные требования к государственным служащим в области использования информационных технологий».

4.21. Требуемый режим работы персонала

Режим работы персонала должен соответствовать действующему законодательству Российской Федерации (РФ) и обеспечивать работоспособность Системы согласно требованиям, предъявленным настоящим ТЗ.

Режим работы персонала должен соответствовать Гигиеническим требованиям к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы (Санитарные правила и нормы. СанПиН 2.2.2.542-96 (Утв. Постановлением Госкомсанэпиднадзора России от 14.07.1996 г. № 14)).

Должна быть учтена возможность сменного режима работы персонала Системы.

При этом должна учитываться возможность круглосуточного подключения к работам специалистов, обеспечивающих функционирование Системы (администраторов и специалистов по техническому обслуживанию), для решения проблем по обеспечению работоспособности информационных ресурсов Системы.

4.22. Требования к безопасности

Программно-аппаратные средства Системы должны обеспечивать безопасность обслуживающего персонала при эксплуатации, техническом обслуживании и ремонте с учетом требований ГОСТ 21552-84, ГОСТ 25861-83.

Электробезопасность должна соответствовать требованиям ГОСТ 12.1.030-81, ГОСТ 12.2.003 и ГОСТ 12.2.007.0-75.

Технические средства должны отвечать действующей системе государственных стандартов безопасности труда и иметь сертификаты по электробезопасности и электромагнитной безопасности.

4.23. Требования к эргономике и технической эстетике

Интерфейсы Системы должны удовлетворять следующим требованиям:

– обеспечивать визуальное различие между рабочими и заблокированными элементами интерфейса (в случае невозможности выполнения какого-либо действия);

– цветовое оформление интерфейса должно быть выполнено в едином стиле;

– в случае возникновения ошибочных ситуаций Система должна уведомлять о ней пользователя с описанием ошибки на русском языке.

Интерфейсы Системы должны быть понятными и удобными, не перегруженными графическими элементами, должно быть обеспечено быстрое отображение экранных форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Ввод-вывод данных, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном или автоматическом режимах. Интерфейсы должны соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и сервисам Системы во всех современных браузерах (IE версии 7 и выше, Firefox версии 4.0и выше и прочие промышленно поддерживаемые браузеры).

Интерфейсы должны быть рассчитаны на преимущественное использование манипулятора типа «мышь», то есть управление должно осуществляться с помощью набора экранных меню, кнопок, значков и других графических элементов, управляемых кнопками «мыши» с дублированием управления клавиатурой. Использование клавиатурного режима должно осуществляться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений), должны быть на русском языке.

Системы должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях, пользователю должны выводиться соответствующие сообщения, после чего должно происходить возвращение в состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Экранные формы должны быть спроектированы с учетом следующих требований по их унификации:

– все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;

– для обозначения одних и тех же операций должны использоваться одинаковые графические значки, кнопки и другие управляющие (навигационные) элементы; должны быть унифицированы термины, используемые для описания идентичных понятий, операций и действий пользователя;

– реакция Системы на действия пользователя (наведение указателя «мыши», переключение фокуса, нажатие кнопки) должна быть типовой для каждого действия над одними и теми же графическими элементами, независимо от их расположения на экране.

4.24. Требования к эксплуатации и техническому обслуживанию компонентов Системы

Эксплуатация Системы должна производиться в соответствии с эксплуатационной документацией и Регламентом технического обслуживания.

Обслуживание Системы должно производиться обслуживающим персоналом.

4.25. Условия и регламент (режим) эксплуатации

Должно быть предусмотрено ежедневное/еженедельное техническое обслуживание Системы. При возникновении неисправностей должно осуществляться оперативное обслуживание.

Регламент технического обслуживания должен разрабатываться на этапе Технического проекта и утверждаться в составе эксплуатационной документации.

4.26. Требования к регламенту обслуживания

При эксплуатации Системы, входящее в ее состав системное программное обеспечение должно соответствовать рекомендациям производителя.

Должны соблюдаться правила эксплуатации компонентов Системы, а так же производиться своевременная установка обновлений программного обеспечения, рекомендованных производителями.

Исполнителем должны быть предъявлены требования к ежедневному и еженедельному обслуживанию, а также обслуживанию по возникновению особых (исключительных) ситуаций. Сюда включаются работы по обслуживанию технических средств Системы, данных в постоянных и временных хранилищах (базах данных), потоков сообщений в электронных коммуникациях, паролей и прав доступа.

В частности, в обслуживание входят работы:

– по сохранению (копированию) журналов изменений баз данных и резервных копий баз данных;

– по восстановлению баз данных при порче или разрушении данных;

– по профилактическому контролю состояния дисковых запоминающих устройств и данных на них.

Выполнение указанных требований должно обеспечивать непрерывную работу комплекса. При этом резервное копирование информации может осуществляться в двух режимах:

– создание полной копии базы данных;

– сохранение изменений, внесенных со времени создания последней архивной копии (архивные копии log-файлов).

Периодичность и очередность этих операций определяются отдельным распоряжением, политикой резервного копирования информации и положением по категорированию информационных ресурсов.

Создание полной копии базы данных осуществляется полным копированием всех файлов указанной базы на внешние носители.

При сохранении изменений, внесенных со времени создания последней архивной копии, на внешние носители переносятся только те изменения базы данных, которые были сделаны со времени последней операции архивирования (полного или частичного).

При восстановлении информации с архивных копий сначала с архивных носителей восстанавливается состояние базы данных на момент последней операции полного резервного копирования, затем в базу поочередно вносятся изменения со всех частичных архивов, созданных после полного резервирования.

Предпочтительный интервал для технического обслуживания Системы в нерабочие дни, например с 23:00 до 07:00.

При эксплуатации Системы, должен соблюдаться регламент тестирования и обновления входящего в ее состав системного и прикладного программного обеспечения.

Заказчик должен обеспечить технические средства для функционирования эталонной и промышленной платформ Системы. Версии системного программного обеспечения, версии сборок прикладного программного обеспечения и настройки, не связанные с IP-адресацией и URL веб-сервисов, должны быть идентичны на обеих платформах.

На эталонной платформе Системы Заказчика не должна вестись разработка. Эталонная платформа Системы Заказчика должна быть предназначена только для тестирования функциональных возможностей и тестирования обновлений версий ОПО и СПО.

Любые изменения или обновления версий ОПО и СПО на эталонной платформе Системы Заказчика должны применяться только в случае успешного проведения аналогичных работ на тестовой платформе Исполнителя.

К каждому обновлению версий ОПО и СПО должен прилагаться стандартизированный документ «Регламент обновления», в котором должна содержаться информация об изменениях, исправлениях ошибок и пошаговая инструкция по обновлению для специалистов Заказчика.

Обновление версий ОПО и СПО на эталонной платформе Системы Заказчика может осуществляться специалистами Исполнителя, обновление версий ОПО и СПО на промышленной платформе Системы Заказчика должно осуществляться специалистами Заказчика в соответствии с «Регламентом обновления» и внутренними регламентами.

Заказчик должен обеспечить доступ к компонентам своей эталонной платформы Системы по протоколу RDP (Remote Desktop Protocol) и\или SSH, http(s) для технических специалистов (разработчиков и тестировщиков) Исполнителя с соответствующими правами доступа необходимыми для осуществления функций управления (администрирования) и тестирования.

4.27. Общие, функциональные требования и требования к эффективности обеспечения безопасности информации

Для обеспечения защиты данных, хранящихся и обрабатываемых системой, необходимо:

- определить и соответствующим образом описать объекты данных, с которыми работает система, классифицировать данные в соответствии с законодательством РФ, а так же уровнем конфиденциальности данных, предъявляемым заказчиком;
- разработать и описать требуемые меры обеспечения безопасности, как в части технической защиты, так и в части организационных мер;

Организационные и технические меры по обеспечению информационной безопасности обеспечиваются Заказчиком и должны включать:

- антивирусную защиту;
- аудит доступа к информационной системе.

Доступ пользователей к функциям и данным Системы должен предоставляться только после прохождения пользователем процедур аутентификации и авторизации.

Доступ пользователей к функциям и данным Системы должен быть ограничен на основе ролевого принципа. Каждому пользователю Системы должна быть сопоставлена учетная запись, ассоциированная с одной из нескольких предопределенных пользовательских ролей. Для каждой

пользовательской роли должны быть определены конкретные ограничения на доступ к функциям и данным Системы.

Необходимо обеспечить обязательное ведение журнала событий в системе с указанием следующих значений для каждого события в системе:

- уникальный порядковый номер записи;
- дата и время события;
- ФИО пользователя;
- наименование события.

Необходимо обеспечить недоступность изменения записей журнала для всех пользователей системы, в том числе и административного персонала. Необходимо обеспечить доступность функции очистки журналов только для специальной роли пользователя. Функция очистки журнала должна автоматически сопровождаться обязательной записью данного события после очистки в журнал событий.

Внесению в журнал событий подлежат:

- все события административного характера;
- все события, относящиеся к изменению параметров системы.

Для заполнения атрибутов учетных записей пользователей, предназначенных для хранения данных определенных в общегородских справочниках или реестрах, должны использоваться значения из общегородских справочников или реестров.

Для конкретного Пользователя (персоны) в Системе должна быть предусмотрена только одна учетная запись.

4.28. Требования к защите данных от разрушений при авариях и Требования к контролю, хранению, обновлению и восстановлению данных

Система должна обеспечивать первичный контроль вводимых данных на соответствие формальным правилам: проверка типов, размерности, допустимости значений.

Система должна ежедневно сохранять имеющиеся данные, достаточные для полного восстановления работоспособности, в удаленном хранилище.

4.29. Технические требования по защите информации

Защита информации - деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации должна осуществляться в соответствии с требованиями ГОСТ Р 50922-2007 и включать в себя:

- **Техническую защиту информации** – защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

- **Защиту информации от утечки** - защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами[1];

- **Защиту информации от несанкционированного воздействия** - защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящего к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и

[1] Заинтересованными субъектами могут быть: государство, юридическое лицо, группа физических лиц, отдельное физическое лицо.

копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

- **Защиту информации от непреднамеренного воздействия** - защита информации, направленная на предотвращение воздействия на защищаемую информацию ошибок ее пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации событий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

- **Защиту информации от преднамеренного воздействия** - защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного воздействия, и (или) воздействия различной физической природы, осуществляемого в террористических или криминальных целях.

4.30. Требования по сохранности информации при авариях

Сохранность информации должна обеспечиваться:

– при пожарах, затоплениях, землетрясениях и других стихийных бедствиях: организационными и защитными мерами, опирающимися на подготовленность помещений и персонала, обеспечивающими сохранность хранимых копий информации на внешних носителях;

– при механических и электронных сбоях и отказах в работе компьютеров: на основе программных процедур восстановления информации с использованием хранимых копий баз данных, файлов журналов изменений в базах данных, копий программного обеспечения.

Для обеспечения сохранности информации в базах данных Системы должны быть реализованы следующие функциональные возможности:

– резервное копирование баз данных Системы;

– восстановление данных в непротиворечивое состояние при программно-аппаратных сбоях (отключение электрического питания, сбоях операционной системы и других) вычислительно-операционной среды функционирования;

– восстановление данных в непротиворечивое состояние при сбоях в работе сетевого программного и аппаратного обеспечения.

В случае потери работоспособности Системы вследствие разрушения данных восстановление работоспособности Системы должно быть обеспечено средствами СУБД, операционной системы или соответствующими сервисами платформы виртуализации, в которой размещены программные компоненты.

Резервное копирование данных должно производиться администратором Системы с использованием инструментария, входящего в состав программного обеспечения СУБД, операционной системы или платформы виртуализации.

4.31. Экономические требования

Должно быть достигнуто рациональное соотношение между затратами по обеспечению информационной безопасности Системы и достижением результатов по информационной безопасности.

4.32. Требования к патентной чистоте

Патентная чистота внедряемой Системы должна быть обеспечена в отношении патентов, действующих на территории Российской Федерации.

Реализация технических, программных, организационных и иных решений, предусмотренных проектом Системы, не должна приводить к нарушению авторских и смежных прав третьих лиц.

При использовании в развитии Системы программ (программных комплексов или компонентов), разработанных третьими лицами, условия, на которых передается право на

использование (исполнение) этих программ, не должны накладывать ограничений, препятствующих использованию Системы по ее прямому назначению.

4.33. Требования по стандартизации и унификации

Система должна быть внедрена с использованием стандартных и унифицированных методов разработки программных средств.

При развитии Системы и разработке пользовательских интерфейсов должны использоваться единые принципы организации доступа к предоставляемым функциональным возможностям.

Общесистемное программное обеспечение должно быть унифицировано по версиям. Предусматривается максимальное использование типовых решений.

4.34. Требования к лингвистическому обеспечению

Все специальное программное обеспечение Системы для организации взаимодействия с пользователем должно использовать русский язык. Интерфейс пользователя Системы должен быть полностью русифицирован за исключением системных команд.

Все документы, продуцируемые Системой, должны предоставляться пользователю на русском языке.

Вся документация, разрабатываемая в рамках выполнения работ, должна быть выполнена на русском языке.

4.35. Требования к организации функционирования Системы и порядку взаимодействия персонала

Организация функционирования Системы должна быть обеспечена в рамках выполнения должностных обязанностей сотрудниками, участвующими в эксплуатации Системы.

5. ТРЕБОВАНИЯ К СТРУКТУРЕ И ФУНКЦИОНИРОВАНИЮ СИСТЕМЫ

Функции Системы реализуются через функции следующих подсистем и компонентов, требования к которым приводятся далее в настоящем ТЗ:

- подсистема «Комплексный сервис системы контроля и управления функционированием (СКУФ)»;
- подсистема управления знаниями и документацией;
- подсистема мониторинга;
- подсистема управления версиями;
- подсистема управления сетевым адресным пространством инфраструктуры ЭП;
- подсистема мониторинга JAVA-процессов;
- подсистема автоматизации установки релизов ИС ИЭП;
- подсистема информационной безопасности;
- подсистема мониторинга и контроля оборудования ЭП;
- внедрение политик СРК на основании SLA и RTO эксплуатируемых информационных систем;
- внедрение эксплуатационных инструкций на типовые операции инженеров и администраторов вычислительной инфраструктуры ЭП.

5.1. Подсистема «Комплексный сервис системы контроля и управления функционированием (СКУФ)»

5.1.1 Характеристики объекта автоматизации

Эксплуатация Инфраструктуры осуществляется на базе следующих ИТ-процессов:

- Управление инцидентами и обращениями;
- Управление проблемами;
- Управление изменениями;
- Управление конфигурациями;
- Управление задачами;
- Управление уровнем обслуживания.

Оценка количества пользователей системы автоматизации процессов приведена в Таблице 1.

Таблица 1. Количество пользователей системы автоматизации процессов

№№	Наименование объекта	Количество единиц	Тип подключения
1.	Пользователи процессов управления инцидентами, обращениями, проблемами, задачами, конфигурациями	Не менее 40	Конкурентное
2.	Пользователи процессов управления инцидентами, обращениями, проблемами, задачами, конфигурациями	Не менее 45	Именное
3.	Пользователи процесса управления изменениями	Не менее 40	Конкурентное
4.	Пользователи процесса управления изменениями	Не менее 10	Именное
5.	Пользователи процесса управления уровнем обслуживания	Не менее 5	Именное
6.	Пользователи процесса управления уровнем обслуживания	Не менее 5	Конкурентное
7.	Пользователи портала самообслуживания	Не менее 500	Именное
8.	Пользователи системы отчетности	Не менее 20	Конкурентное

Количественная оценка объектов Инфраструктуры приведена в Таблице 2.

Таблица 2. Количество объектов Инфраструктуры

№№	Наименование объекта	Количество единиц
1.	Сетевое оборудование	Не менее 380
2.	Оборудование СХД	Не менее 315
3.	Серверное оборудование	Не менее 1020
4.	Виртуальные машины	Не менее 900
5.	Информационные сервисы и прочие объекты управления	Не менее 10 000

Требуется обеспечить мониторинг состояния оборудования от производителей:

– Сетевого оборудования – Cisco Systems, Juniper Networks, Brocade Communications Systems, Extreme networks, Palo Alto Networks, StoneGate (Stonesoft), Checkpoint, EMC;

- СХД и SAN-коммутаторов – Sun, Hitachi, HP, Brocade, EMC;
- Ленточных библиотек – HP, IBM, Sun;
- Серверного оборудования – HP, IBM, Sun, R-Style, Intel.

В состав программного комплекса Инфраструктуры входят ОС различных версий: RHEL, Solaris, HP-UX и Windows.

Базы данных реализованы при использовании Oracle, MS SQL, Postgres и MySQL.

Системы виртуализации построены на продуктах VMware vSphere.

Для построения бизнес-приложений используются middleware PHP, JBoss, Weblogic, Oracle Service Bus.

Кластеризация и балансировка нагрузки реализована на продуктах Symantec, Terracotta, Nginx, Citrix, Brocade.

5.1.2 Требования к подсистеме

5.1.2.1 Требования к подсистеме в целом

Подсистема должна удовлетворять следующим основным требованиям:

– Обеспечивать возможность использования Системы через сеть ОП и/или сеть Internet;

– Обеспечивать разделение доступа к данным и функциям Системы согласно ролевой модели;

Функции подсистемы реализуются через функции входящих в ее состав модулей, требования к которым приводятся ниже.

5.1.2.2 Требования к структуре подсистемы

Подсистема должна состоять из следующих модулей:

– Управления инцидентами и обращениями;
– Управления проблемами;
– Управления изменениями;
– Управления заданиями;
– Управления уровнем обслуживания;
– Управления конфигурациями (CMDB);
– Автоматического обнаружения оборудования;
– Управления событиями, влиянием и анализа статистики;
– Мониторинга СПД;
– Мониторинга оборудования и ПО;
– Планирования утилизации ресурсов;
– Формирования отчетности.

5.1.2.3 Требования к интеграции

Подсистема должна обеспечить возможность интеграции со следующими внешними информационными системами:

– Информационной системой управления Облачной платформой Заказчика;
– Информационными системами ЭП:
  - ЕПГУ (регистрация обращений граждан);
  - СМЭВ (взаимодействие с другими системами через СМЭВ);
  - ТП СМЭВ (регистрация заявок участников межведомственного взаимодействия, подаваемых через ТП СМЭВ).

5.1.2.4 Функциональные требования к модулям

Для всех модулей должны быть реализованы следующие механизмы:

– механизм, позволяющий отсекать заведомо некорректные значения полей при внесении информации путем ограничения возможных для выбора значений заполняемого поля;

– механизм журналирования и хранения истории изменений контролируемых параметров объектов;

– механизм поиска объектов по значению поля или по совокупности полей.

5.1.3 Требования к модулю управления инцидентами и обращениями

Должен быть спроектирован, развернут и сконфигурирован модуль управления инцидентами и обращениями, заполнены необходимые справочники, а также, при необходимости, проведены доработки ПО с целью соответствия указанным в данном разделе настоящей документации требованиям.

В рамках работ по внедрению модуля должен быть разработан регламент управления инцидентами и обращениями. Разработанный регламент должен учитывать особенности эксплуатации Инфраструктуры с использованием четырехуровневой структуры поддержки эксплуатации:

– ЛП1 – Центр поддержки пользователей;

– ЛП2 – Дежурные администраторы;

– ЛП3 – Инженеры поддержки инфраструктуры;

– ЛП4 – Производители оборудования, разработчики, иные участники эксплуатации Инфраструктуры.

Модуль управления инцидентами и обращениями должен соответствовать требованиям разработанного регламента.

Модуль должен обеспечивать централизованное хранение и предоставление информации обо всех зарегистрированных обращениях и инцидентах в единой базе данных.

Должна быть обеспечена возможность регистрации инцидентов и обращений вручную, с проверкой заполнения обязательных полей.

Должна быть предусмотрена автоматическая регистрация инцидентов и обращений в случаях:

– Поступления события от подсистем мониторинга в составе СКУФ;

– Получения e-mail сообщения в адрес СКУФ;

– Поступления событий от интегрируемых систем;

– Наступления других событий, способных инициировать вызов универсального интерфейса на базе веб сервиса.

При автоматической регистрации, должна быть предусмотрена возможность заполнения полей инцидента и/или обращения информацией, передаваемой из источника события.

Учет инцидентов должен выполняться в качестве самостоятельного типа объектов – «Инцидент». Минимальный набор полей Инцидента приведен в Таблице 4.

Таблица 4. Минимальный набор полей Инцидента

Название поля	Тип поля	Доступ пользователей	Комментарий
ID инцидента	Счетчик	Только для чтения	Уникальный, автоматически увеличиваемый номер инцидента
Тема	Текст	Изменяемое	Краткое описание инцидента
Сервис	Справочник	Изменяемое	Услуга, к которой относится инцидент
Приоритет	Справочник	Изменяемое	Приоритет инцидента
Назначено группе	Справочник	Изменяемое	Группа назначения инцидента
Статус	Справочник	Изменяемое	Статус инцидента
Решение	Текст	Изменяемое	Содержание решения инцидента

Должна быть обеспечена возможность классификации инцидентов и обращений по:

- приоритету;
- типу;
- срочности.

Должна быть обеспечена возможность автоматического выбора группы назначения инцидента/обращения в зависимости от их классификации.

Должна быть обеспечена возможность внесения дополнительной информации в инцидент/обращение путем отправки e-mail сообщения на адрес подсистемы. При этом в инциденте/обращении хранимом в подсистеме должна сохраняться как информация из тела письма, так и вложения.

Должен быть реализован механизм поиска инцидентов и обращений. Поиск должен быть возможен по всем видимым атрибутам инцидентов/обращений, включая текстовые поля. При поиске по текстовым полям, должен быть обеспечен поиск по ключевым словам (включая все слова, включая одно из слов, исключая слова) с учетом морфологии. В случае выдачи множественного результата, поисковый механизм должен обеспечивать возможность сортировки результатов выдачи по качеству совпадения с запросом.

5.1.4 Требования к модулю управления проблемами

Должен быть спроектирован, развернут и сконфигурирован модуль управления проблемами, заполнены необходимые справочники, а также, при необходимости, проведены доработки ПО с целью соответствия указанным в данном разделе настоящей документации требованиям.

В рамках работ по внедрению модуля должен быть разработан регламент управления проблемами. Разработанный регламент должен учитывать особенности эксплуатации Инфраструктуры с использованием четырехуровневой структуры поддержки эксплуатации:

- ЛП1 – Центр поддержки пользователей;
- ЛП2 – Дежурные администраторы;
- ЛП3 – Инженеры поддержки инфраструктуры;
- ЛП4 – Производители оборудования, разработчики, иные участники эксплуатации Инфраструктуры.

Модуль управления проблемами должен соответствовать требованиям разработанного регламента.

Модуль должен обеспечивать централизованное хранение и предоставление информации обо всех зарегистрированных проблемах в единой базе данных.

Должна быть обеспечена возможность регистрации проблем вручную, с проверкой заполнения обязательных полей.

Учет проблем должен выполняться в качестве самостоятельного типа объектов – «Проблема». Минимальный набор полей Проблемы приведен в Таблице 5.

Таблица 5. Минимальный набор полей Проблемы

Название поля	Тип поля	Доступ пользователей	Комментарий
ID проблемы	Счетчик	Только для чтения	Уникальный, автоматически увеличиваемый номер
Содержание	Текст	Изменяемое	Краткое описание проблемы
Сервис	Справочник	Изменяемое	Услуга, к которой относится проблема
Приоритет	Справочник	Изменяемое	Приоритет проблемы
Назначено группе	Справочник	Изменяемое	Группа назначения

Название поля	Тип поля	Доступ пользователей	Комментарий
Статус	Справочник	Изменяемое	Статус проблемы

Должна быть обеспечена возможность автоматического выбора группы назначения проблемы в зависимости от ее классификации.

Должна быть обеспечена возможность внесения дополнительной информации в проблему путем отправки e-mail сообщения на адрес подсистемы. При этом в проблеме хранимой в подсистеме должна сохраняться как информация из тела письма, так и вложения.

Должен быть реализован механизм поиска проблем. Поиск должен быть возможен по всем видимым атрибутам проблемы, включая текстовые поля. При поиске по текстовым полям, должен быть обеспечен поиск по ключевым словам (включая все слова, включая одно из слов, исключая слова) с учетом морфологии. В случае выдачи множественного результата, поисковый механизм должен обеспечивать возможность сортировки результатов выдачи по качеству совпадения с запросом.

5.1.5 Требования к модулю управления изменениями

Должен быть спроектирован, развернут и сконфигурирован модуль управления изменениями, заполнены необходимые справочники, а также, при необходимости, проведены доработки ПО с целью соответствия указанным в данном разделе настоящей документации требованиям.

В рамках работ по внедрению модуля должен быть разработан регламент управления изменениями. Разработанный регламент должен учитывать особенности эксплуатации Инфраструктуры с использованием четырехуровневой структуры поддержки эксплуатации:

– ЛП1 – Центр поддержки пользователей;

– ЛП2 – Дежурные администраторы;

– ЛП3 – Инженеры поддержки инфраструктуры;

– ЛП4 – Производители оборудования, разработчики, иные участники эксплуатации Инфраструктуры.

Модуль управления изменениями должен соответствовать требованиям разработанного регламента.

Модуль должен обеспечивать централизованное хранение и предоставление информации обо всех зарегистрированных изменениях в единой базе данных.

Должна быть обеспечена возможность регистрации изменений вручную, с проверкой заполнения обязательных полей.

Учет изменений должен выполняться в качестве самостоятельного типа объектов – «Изменение». Минимальный набор полей Изменения приведен в Таблице 6.

Таблица 6. Минимальный набор полей Изменения

Название поля	Тип поля	Доступ пользователей	Комментарий
ID изменения	Счетчик	Только для чтения	Уникальный, автоматически увеличиваемый номер
Тема	Текст	Изменяемое	Краткое описание изменения
Сервис	Справочник	Изменяемое	Услуга, к которой относится изменение
Срочность изменения	Справочник	Изменяемое	Срочность изменения
Статус	Справочник	Изменяемое	Статус изменения

Должна быть обеспечена возможность автоматического выбора группы назначения изменения в зависимости от его классификации.

Подсистема должна позволять регистрировать стандартные изменения, с заранее определенным типом проводимых набором работ и списком согласующих лиц.

Должен быть реализован механизм согласований изменений, при этом подсистема должна позволять назначать согласование как на одного пользователя подсистемы, с возможностью замещения, так и на группу лиц.

Должна быть обеспечена возможность внесения дополнительной информации в изменение путем отправки e-mail сообщения на адрес подсистемы. При этом в изменении хранимом в подсистеме должна сохраняться как информация из тела письма, так и вложения.

Должен быть реализован механизм поиска изменений. Поиск должен быть возможен по всем видимым атрибутам изменений, включая текстовые поля. При поиске по текстовым полям, должен быть обеспечен поиск по ключевым словам (включая все слова, включая одно из слов, исключая слова) с учетом морфологии. В случае выдачи множественного результата, поисковый механизм должен обеспечивать возможность сортировки результатов выдачи по качеству совпадения с запросом.

5.1.6 Требования к модулю управления заданиями

Должен быть спроектирован, развернут и сконфигурирован модуль управления заданиями, заполнены необходимые справочники, а также, при необходимости, проведены доработки ПО с целью соответствия указанным в данном разделе настоящей документации требованиям.

Настройка модуля должна учитывать особенности эксплуатации Инфраструктуры с использованием четырехуровневой структуры поддержки эксплуатации:

– ЛП1 – Центр поддержки пользователей;

– ЛП2 – Дежурные администраторы;

– ЛП3 – Инженеры поддержки инфраструктуры;

– ЛП4 – Производители оборудования, разработчики, иные участники эксплуатации Инфраструктуры.

Модуль должен обеспечивать централизованное хранение и предоставление информации обо всех зарегистрированных заданиях в единой базе данных.

Должна быть обеспечена возможность регистрации заданий вручную, с проверкой заполнения обязательных полей.

Учет заданий должен выполняться в качестве самостоятельного типа объектов – «Задание». Минимальный набор полей Задания приведен в Таблице 7.

Таблица 7. Минимальный набор полей Задания

Название поля	Тип поля	Доступ пользователей	Комментарий
ID задачи	Счетчик	Только для чтения	Уникальный, автоматически увеличиваемый номер
Содержание	Текст	Изменяемое	Краткое описание задачи
Назначено группе	Справочник	Изменяемое	Группа назначения задачи
Статус	Справочник	Изменяемое	Статус задачи

Должна быть обеспечена возможность регистрации заданий по заранее определенному шаблону.

Подсистема должна позволять регистрировать цепочки заданий для последовательного и параллельного выполнения в случае, если такие задания связаны с изменениями.

Должен быть реализован механизм поиска заданий. Поиск должен быть возможен по всем видимым атрибутам заданий, включая текстовые поля. При поиске по текстовым полям, должен быть обеспечен поиск по ключевым словам (включая все слова, включая одно из слов, исключая слова) с учетом морфологии. В случае выдачи множественного результата, поисковый механизм должен обеспечивать возможность сортировки результатов выдачи по качеству совпадения с запросом.

5.1.7 Требования к модулю управления уровнем обслуживания

Должен быть спроектирован, развернут и сконфигурирован модуль управления уровнем обслуживания заполнены необходимые справочники, а также, при необходимости, проведены доработки ПО с целью соответствия указанным в данном разделе настоящей документации требованиям.

В рамках работ в СКУФ должны быть внесены и настроены соглашения об уровне сервиса по информационным системам:

- ЕПГУ;
- РПГУ (все регионы);
- ГЭПС;
- ЕСИА;
- СМЭВ;
- РСМЭВ (все регионы);
- СКИМ;
- ЕНСИ;
- ИПШ;
- СМУ;
- ЭС ЦТО;
- ОП;
- ГУЦ;
- ПГП;
- ФРГУ;
- УВИРИ.

Модуль должен отслеживать исполнение настроенных Соглашений об уровне сервиса в процессе Управления Инцидентами и Обращениями.

SLA должно зависеть от параметров указанных при регистрации инцидента/обращения:

- сервиса
- приоритета
- типа
- уровней категоризации

Для каждого SLA должна быть доступна возможность настройки нескольких уровней реакции.

При нарушении уровня реакции модуль должен будет отправлять оповещение группе заинтересованных лиц с использованием почтовых сообщений и СМС-сообщений.

Модуль при расчете времени эскалации, должен иметь возможность использовать рабочие графики ролевых групп, с учетом выходных и праздничных дней.

5.1.8 Требования к модулю управления конфигурациями (CMDB)

Должен быть спроектирован, развернут и сконфигурирован модуль управления конфигурациями, заполнены необходимые справочники, а также, при необходимости, проведены

доработки ПО с целью соответствия указанным в данном разделе настоящей документации требованиям.

Требуется реализовать БД управления конфигурациями, как единое хранилище данных о составе объектов Инфраструктуры.

В рамках выполнения проектных работ требуется разработать модель данных, которая будет включать описание используемых классов КЕ, их параметров и типы взаимосвязей.

Требуется обеспечить наполнение CMDB данными о подключаемых в контур мониторинга информационных системах Инфраструктуры.

Требуется разработать и внести в Систему полнофункциональные сервисно-ресурсные модели по информационным системам в контуре мониторинга. Общая модель данных и сервисно-ресурсные модели должны отражать наличие компонентов Инфраструктуры и связи между ними в объеме, достаточном для эксплуатации Системы. Детальные требования к моделированию должны быть определены на этапе проектирования.

5.1.9 Требования к модулю автоматического обнаружения оборудования

Модуль должен обеспечить выполнение следующих требований:

– Возможность массового обнаружения инфраструктурных единиц по заданному диапазону сетевых адресов;

– Наличие заранее сконфигурированных профилей обнаружения КЕ, которые соответствуют типовым объектам Инфраструктуры.

Должны быть разработаны шаблоны, содержащие правила анализа Конфигурационных единиц и построения зависимостей.

Должна быть проведена интеграция с модулем управления конфигурациями для передачи перечня обнаруженных КЕ, их параметров спецификации и взаимосвязей в соответствии с принятой моделью данных и соглашением об именовании КЕ.

5.1.10 Требования к модулю управления событиями, влиянием и анализа статистики

Модуль управления событиями должен реализовать следующие функции: обеспечить регистрацию и обработку событий, происходящих в сетях, на оборудовании, в операционных системах, в СУБД, в приложениях, в информационных сервисах (услугах) и любых других объектах, которые будут включены в контур мониторинга.

Необходимо обеспечить интеграцию модуля с модулем управления конфигурациями (CMDB) для получения актуальной информации о составе и связях сервисно-ресурсной модели Инфраструктуры.

5.1.11 Требования к модулю мониторинга СПД

Необходимо реализовать сбор данных с устройств сетевого оборудования. Модуль должен работать по стандартным протоколам управления и мониторинга: snmp, icmp и принимать события и данные по протоколам snmp, netflow.

Должна быть сформирована базовая модель здоровья следующих типов устройств различных вендоров, используемых в Инфраструктуре:

– межсетевые экраны;

– коммутаторы;

– маршрутизаторы;

– Контроллеры трафика приложений.

Должна быть реализована интеграция с модулем управления событиями для передачи информации о событиях СПД.

5.1.12 Требования к модулю мониторинга оборудования и ПО

Требуется реализовать измерение параметров доступности и производительности на объектах Инфраструктуры.

После анализа объектов мониторинга при проектировании подсистемы требуется реализовать два подхода к составлению перечня измеряемых метрик:

– Модели здоровья стандартных компонентов – должны быть составлены списки метрик доступности и производительности, а также их граничных значений для типовых компонентов Инфраструктуры, по мере их включения в контур мониторинга: оборудование, системное ПО, ПО виртуализации, БД, серверы приложений;

– Набор специфичных метрик Информационных Систем – должны быть составлены списки метрик доступности, производительности и их граничных значений для нетиповых компонентов Инфраструктуры: приложений и технических сервисов. Значения специфичных метрик должны отражать статус экземпляров указанных компонентов ИС на инфраструктурном уровне и уровне бизнес-логики.

5.1.13 Требования к модулю планирования утилизации ресурсов

Требуется реализовать подсистему анализа утилизации ресурсов. Подсистема должна предоставлять возможность построения отчетов по утилизации процессорной мощности, виртуальной памяти, ресурсов дисковой подсистемы, возможность анализировать тенденции при изменении контролируемых значений и формировать прогнозы по утилизации на основе статистики.

5.1.14 Требования к модулю формирования отчетности

Должен быть реализован модуль отчетности, удовлетворяющий следующим требованиям:

Информация в модуле должна предоставляться в виде текста, таблиц и графиков.

Статистические отчеты должны предоставляться следующими способами:

– Через web-интерфейс, с возможностью задания уровней фильтрации входных данных, например периода отчета;

– Отправляться на почту заинтересованным лицам по расписанию, с заранее установленными параметрами.

5.1.15 Порядок контроля и приемки подсистемы

Испытания подсистемы и ее компонентов должны осуществляться в соответствии с этапами работ, определенными в Договоре.

Для компонентов подсистемы должны быть проведены следующие виды испытаний:

– предварительные испытания;

– опытная эксплуатация;

– приемочные испытания.

5.1.16 Требования к документированию

В рамках работ по внедрению подсистемы Исполнителем должна быть разработана документация, которая должна включать следующий перечень документов:

– Частные технические задания на создание подсистем;

– Технический проект на создание подсистемы;

– Эксплуатационная документация;

– Программа и методика приемочных испытаний;

– Протокол приемочных испытаний подсистемы.

5.2. Подсистема управления знаниями и документацией

5.2.1 Требования к функциям подсистемы

5.2.1.1 Общие требования

Подсистема управления знаниями и документацией должна обеспечивать:

– Доступность основных функций подсистемы на сайте Системы;

– При редактировании или создании статьи должна быть предусмотрена возможность использования языка разметки wiki;

– Возможность выстраивания иерархии документов;

– Уведомление пользователей;

– Безопасность документов от несанкционированного доступа;

– Выгрузка страниц в формате pdf или doc

– Сквозной поиск

5.2.1.2 Доступность основных функций подсистемы на сайте Системы

Подсистема должна предоставлять пользователю интерфейс для просмотра и редактирования документов, статей, новостей через веб браузер. Без установки дополнительного программного обеспечения.

Для администраторов подсистемы, через web-интерфейс должны быть доступны функции управления подсистемой:

– Управление учетными записями пользователей;

– Управление доступами к документам или страницам;

– Управление иерархией страниц, разделов.

5.2.1.3 Использование языка разметки wiki

В подсистеме должен быть предусмотрен выбор редактора для работы с документами, статьями. По умолчанию должен предоставляться WYSIWYG редактор, который предоставляет графический интерфейс работы с текстом очень похожим на стандартные редакторы документов. Для пользователей, которые привыкли работать с языками разметки, предусмотрена функция перехода редактора в режим работы с wiki разметкой.

5.2.1.4 Возможность выстраивания иерархии документов

Пользователь при работе в подсистеме пользователь может менять иерархию статей. Тем самым пользователю предоставляется удобный инструмент, который позволяет логично организовать контент.

5.2.1.5 Отправка уведомлений пользователям

Подсистема должна предусматривать возможность уведомлений пользователя о создании новых страниц, внесение правок в интересующие его документы, о публикации новостей, добавление комментариев. Формат уведомлений должен иметь возможность изменения.

Для обеспечения информирования пользователей подсистемы должны быть предусмотрены следующие средства оповещения пользователей:

– средства оповещения, встроенные в интерфейс подсистемы;

– через E-mail шлюз.

5.2.1.6 Выгрузка страниц

Подсистема предоставляет возможность пользователю или администратору подсистемы с соответствующими правами в подсистеме, произвести выгрузку из подсистемы документов или статей с сохранением существующей иерархии в формат pdf или doc.

5.2.1.7 Сквозной поиск

Полнотекстовый поиск подсистемы должен обеспечивать функциональность интеллектуального поиска, как по тексту внутри страницы, так и по файлам вложений с учетом семантики русского языка. Необходимо обеспечить возможность полнотекстовой индексации по основным офисным форматам документов (doc, pdf, xls и др.).

5.3. Подсистема мониторинга

5.3.1 Требования к функциям подсистемы

5.3.1.1 Общие требования

Автоматизация функций мониторинга ИТ сервисов должна обеспечивать:

- мониторинг аппаратных платформ серверной инфраструктуры;
- мониторинг систем Oracle Database;
- мониторинг систем Microsoft;
- мониторинг систем Unix/Linux;
- мониторинг доступности web сайтов;
- мониторинг сетевого оборудования;
- выполнение скриптов по исправлению типично возникающих проблем;
- отправка настроенных уведомлений по почте или СМС;
- предоставление отчетности по событиям и параметрам мониторинга

5.3.1.2 Мониторинг аппаратных платформ серверной инфраструктуры

Подсистема должна обеспечивать аппаратный мониторинг платформ HP, IBM, SUN.

Должен обеспечиваться контроль состояния жестких дисков, памяти, сетевых интерфейсов, процессоров, температуры серверов.

Должна быть предусмотрена возможность изменения параметров и пороговых значений мониторинга наблюдаемых систем.

Должна быть предусмотрена возможность расширения состава инвентарной информации и включения в объекты мониторинга новых аппаратных платформ.

5.3.1.3 Мониторинг систем Oracle Database

Должен обеспечиваться централизованный мониторинг состояния систем Oracle, в частности контроль места в таблицах, кол-во пользователей.

Должна обеспечиваться поддержка мониторинга нескольких инстанций

5.3.1.4 Мониторинг систем Microsoft

Мониторинг систем Microsoft должен осуществляться через единую консоль в разрезе по сервисам.

Должен быть предусмотрен онлайн анализ быстродействия серверов по выбранным параметрам.

В целом подсистема должна обеспечивать мониторинг различных параметров следующих систем:

- мониторинг серверов Windows;
- мониторинг сетевых сервисов.

5.3.1.5 Мониторинг систем Unix/Linux

Подсистема должна обеспечивать мониторинг следующих *nix систем:

- Sun Solaris
- Red Hat

В рамках мониторинга должна предоставляться статистика по памяти, дискам, централизованная диагностика через командную строку.

5.3.1.6 Мониторинг web сайтов

В рамках проекта должен быть реализован мониторинг доступности сайтов: проверка кодов ответа и наличие ожидаемого текста.

5.3.1.7 Мониторинг сетевого оборудования

Подсистема должна обеспечивать мониторинг сетевого оборудования ведущих производителей. Необходимые данные для сбора: стандартные метрики протокола SNMP, сообщения от оборудования, доступность ее и время ответа по выбранным каналам, загрузку интерфейсов, работоспособность компонентов оборудования.

5.3.1.8 Отправка уведомлений

Подсистема должна предусматривать создание инцидентов по возникающим проблемам, базу знаний и скрипты для исправления типовых проблем.

Формат уведомлений должен иметь возможность изменения.

5.4. Подсистема управления версиями

5.4.1 Требования к функциям подсистемы

5.4.1.1 Общие требования

Подсистема управления знаниями и документацией должна обеспечивать:

- Управление версиями документов;
- Разграничение прав пользователей;
- Просмотр и управление через веб-интерфейс;
- Возможность зеркалирования хранилища.

5.4.1.2 Управление версиями документов

Должен обеспечиваться следующий функционал для управления версиями документов:

- Хранение полной истории изменений отслеживаемых объектов в централизованном хранилище (репозитории), в том числе при изменении атрибутов, перемещении, переименовании и удалении;
- Копирование объектов с разветвлением истории — при копировании в хранилище появляются два отдельных объекта с общей историей;
- Поддержка переноса изменений между копиями объектов, в том числе полного слияния копий (в рабочей копии; без объединения истории);
- Поддержка ветвления:
  - создания ветвей (копированием директорий) и работы с ними
  - слияние ветвей (переносом изменений)
- Поддержка меток (копированием директорий)
- История изменений и копии объектов (в том числе ветви и метки) хранятся в виде связанных разностных копий — «дешевых» (не требующих больших временных и дисковых ресурсов) при создании и хранении
- Поддержка конкурентной (в том числе одновременной, с изоляцией транзакций) многопользовательской работы с хранилищем и, в большинстве случаев, автоматическим слиянием изменений различных разработчиков (в рабочей копии)
- Фиксации изменений в хранилище (в том числе многообъектные) организуются в виде атомарных транзакций
- Сетевой обмен между сервером и клиентом предусматривает передачу только различий между рабочей копией и хранилищем.

5.5. Подсистема управления сетевым адресным пространством инфраструктуры ЭП

5.5.1 Требования к подсистеме

5.5.1.1 Требования к структуре и функционированию подсистемы

Подсистема должна обеспечивать следующие возможности:

- Доступ к подсистеме через web-интерфейс;
- Просмотр и поиск заведенных интернет адресов;
- Возможность совместной работы нескольких пользователей;
- Внесение данных через графический интерфейс и терминальную консоль;
- Экспорт данных по адресам, сетям, виртуальным цепям и доменам;
- Разделение прав по различным объектам и делегирование на подобъекты;
- Учет номеров виртуальных цепей;
- Резервное копирование подсистемы;
- Иерархичность выделения блоков адресов.

5.5.2 Требования к функциям, выполняемым подсистемой

5.5.2.1 Управление адресным пространством

Подсистема должна обеспечивать возможность заведения адресов, контроль уникальности введенных данных, учет доменного имени, наличие описания, тегов по вносимому объекту.

Для сетевых префиксов должно быть поле автономной системы. Возможность добавлять сети в независимые адресные пространства(vrf).

В подсистеме должен быть предусмотрен экспорт и импорт указанных сетей и адресов в csv формате.

5.5.2.2 Управление логическими цепями.

Подсистема должна предоставлять возможность учета номеров виртуальный цепей, создание доменов виртуальный цепей.

В подсистеме необходимо показывать отношение виртуальной цепи и сетевого адреса или префикса.

5.5.2.3 Графический интерфейс подсистемы

Основным интерфейсом администрирования и пользования подсистемой должен быть web-интерфейс. Должна быть предусмотрена авторизация пользователей с разделением прав как по типам управления, так и по объектам.

Занесенные сетевые префиксы должны автоматически попадать в иерархию сетей, согласно адресу и маске. В интерфейсе по сети необходим фильтр всех занятых и свободных адресов.

5.5.2.4 Управление доменными именами

В подсистеме должна быть предусмотрена возможность выгрузки зоны. Доменная информация учитывается в полях адресов и сетей. Подсистема должна автоматически создавать конфигурацию обратных записей для занесенных адресов.

5.6. Подсистема мониторинга JAVA-процессов

5.6.1 Требования к структуре и функционированию подсистемы

Подсистема должна обеспечивать выполнение следующих основных функций:

– мониторинг состояния JAVA-процессов и выполнения транзакций в режиме реального времени;

– мониторинг исполнения OLA;

– автоматическое обнаружение и контроль состава компонентов JAVA-Инфраструктуры;

– учет компонентов JAVA-Инфраструктуры, их конфигураций и взаимосвязей между ними;

– управление событиями и влиянием на услуги;

– анализ первопричин инцидентов и корреляция событий;

– механизм приоритезации при ликвидации инцидентов в JAVA-инфраструктуре;

– возможность визуализации контролируемых параметров функционирования Java-инфраструктуры;

– генерация отчетов по доступности, производительности и другим метрикам OLA.

5.6.1.1 Требования к характеристикам взаимосвязей подсистемы со смежными информационными системами

Должна быть предусмотрена возможность взаимодействия подсистемы мониторинга с системой управления процессами в составе Системы для обмена сведениями о событиях, заявках, состоянии и связях между КЕ:

– передача информации о событиях и связанных КЕ из подсистемы мониторинга в подсистему управления процессами для автоматического и ручного создания заявок по инцидентам и проблемам;

– передача данных об изменении статуса заявок из подсистемы управления процессами в систему мониторинга;

– передача информации об изменении КЕ из подсистемы управления процессами в подсистему мониторинга и в обратном направлении.

Должна быть реализована интеграция подсистемы управления событиями с другими подсистемами мониторинга Инфраструктуры: VMware OM, Microsoft SCOM, Zabbix, Fluke Visual Performance Monitor. Развитие архитектуры подсистемы в последующих проектах должно предполагать проектные работы по созданию интеграции подсистемы управления событиями и ViPNet StateWatcher.

5.7. Подсистема автоматизации установки релизов ИС ИЭП

5.7.1 Требования к функциям подсистемы

5.7.1.1 Общие требования

Подсистема автоматизации установки релизов информационных систем ИЭП должна обеспечивать выполнение следующих основных функций:

- скачивание дистрибутива с сервера хранения дистрибутивов;
- закачивание дистрибутива на целевые сервера ИС;
- резервное архивирование компонент ИС;
- остановка серверов приложений;
- обновление компонент ИС;
- изменение конфигурационных параметров серверов приложений;
- запуск северов приложений;
- проверка состояния компонент ИС;
- откат ИС до состояния предшествующего установке релиза;
- логирование и подготовка отчетности по установки релиза.

5.7.1.2 Скачивание дистрибутива с сервера хранения дистрибутивов

Подсистема должна в автоматическом режиме скачивать дистрибутив релиза с сервера хранения дистрибутивов по протоколу SSH. Релиз определяется по тегу системы и номеру версии и задается пользователем.

Перед скачиванием должна проводиться проверка наличия достаточного свободного места, при его отсутствии – информировать пользователя подсистемы.

Подсистема должна поддерживать проверку целостности файлов дистрибутива и производить повторную закачку в случае ошибки.

Должна быть возможность изменять адрес сервера хранения дистрибутивов.

5.7.1.3 Передача дистрибутива на целевые сервера ИС

Подсистема должна в автоматическом режиме передавать (закачивать) дистрибутив релиза на целевые сервера Системы по протоколу SSH.

Перед передачей дистрибутива должна проводиться проверка наличия достаточного свободного места, при его отсутствии – информировать пользователя подсистемы.

Дистрибутив должен передаваться только в части модулей, размещенных на целевом сервере.

Передача дистрибутива должна производиться параллельными потоками.

Подсистема должна поддерживать проверку целостности файлов дистрибутива и производить повторную передачу в случае ошибки.

5.7.1.4 Резервное архивирование компонент ИС

Подсистема должна в автоматическом режиме создавать архивную копию изменяемых в релизе программных элементов и конфигурационных файлов.

Перед созданием архивной копии должна проводиться проверка наличия достаточного свободного места, при его отсутствии – информировать пользователя подсистемы.

5.7.1.5 Остановка серверов приложений

Подсистема должна корректно останавливать сервера приложений, работающих на целевом сервере ИС, используя штатные средства сервера приложений.

Подсистема должна проверять статус состояния запуска сервера приложений.

5.7.1.6 Обновление компонент ИС

Подсистема должна производить в автоматическом режиме удаление заменяемых программных компонент и установку новых в соответствии с функциональной ролью сервера в составе ИС.

5.7.1.7 Изменение конфигурационных параметров серверов приложений

Подсистема должна производить в автоматическом режиме конфигурационные изменения, заявленные в релизе в соответствии с функциональной ролью сервера в составе ИС.

5.7.1.8 Запуск северов приложений

Подсистема должна корректно запускать сервера приложений, работающих на целевом сервере ИС, используя штатные средства сервера приложений.

Подсистема должна проверять статус состояния запуска сервера приложений.

5.7.1.9 Проверка состояния компонент ИС

Подсистема должна проверять статус состояния запуска компонент ИС, в том числе на уровне предоставляемого сервиса.

5.7.1.10 Откат ИС до состояния предшествующего установке релиза

Подсистема должна предоставлять возможность произвести в автоматическом режиме откат произведенных изменений и вернуть Систему в исходное состояние.

При необходимости произвести остановку или запуск серверов приложений штатными средствами.

5.7.1.11 Логирование и подготовка отчетности по установки релиза.

Система должна производить в автоматическом режиме логирование в отдельный файл всех произведенных операций и их результат, введенных пользователем команд или данных в ходе установки релиза.

Название файла логирования формируется по тегу подсистемы и номеру релиза. Формат файла – текстовый ASCII.

По факту установки релиза формируется отчет о состоянии компонент ИС.

5.8. Информационная безопасность

5.8.1 Антивирусная защита объектов ИЭП

5.8.1.1 Общие сведения

5.8.1.1.1 Цели работ

Целью работ является обеспечение антивирусной защиты ИЭП.

5.8.1.1.2 Задачи, которые должны быть решены в ходе выполнения работ.

В рамках выполнения работ должны быть установлены и подключены к серверу централизованного управления агенты антивирусной защиты на серверах ИЭП под управлением ОС Windows.

5.8.1.1.3 Характеристики объекта автоматизации

В состав ИЭП входит не более 200 серверов Windows.

В составе ИЭП имеется сервер управления антивирусной защитой Kaspersky Administration Kit из состава пакета Kaspersky Business Space Security.

В состав ИЭП входят МЭ следующих производителей:

- Check Point;
- Palo Alto;
- Stonesoft.

Общее количество МЭ не превышает 30 штук. Все МЭ развернуты в отказоустойчивой конфигурации.

5.8.1.2 Требования к работам

5.8.2.2.1 Общие требования

Агенты антивирусной защиты не должны нарушать работоспособность систем ИЭП.

Агенты антивирусной защиты не должны существенно снижать производительность ИС ИЭП или их компонент.

5.8.2.2.2 Функциональные требования к подсистемам

Средства антивирусной защиты должны препятствовать проникновению вредоносного программного обеспечения различных типов (компьютерных вирусов, троянских программ, шпионского ПО, сетевых червей, руткитов) на серверы и рабочие станции внутренних систем.

При обнаружении вредоносного программного кода средства антивирусной защиты должны блокировать доступ к данным, содержащим такой код, регистрировать факт его обнаружения и предоставлять возможность, в зависимости от заданных настроек, выполнять удаление зараженных файлов, удаление вредоносного кода из зараженных файлов («лечение») и помещение зараженных файлов в специальное хранилище («карантин»).

Должна быть обеспечена антивирусная защита всех серверов и рабочих станций внутренних систем.

Должна быть обеспечена возможность запрета отключения антивирусных средств непривилегированными пользователями.

Должна осуществляться автоматическая загрузка и обновление антивирусных баз.

Должно быть обеспечено централизованное управление параметрами антивирусных средств, функционирующих на различных сетевых узлах внутренних

5.8.2 Донастройка модели защищаемых сайтов и политики защиты WAF Imperva

5.8.2.1 Общие сведения

5.8.2.1.1 Цели работ

Целью работ является обеспечение защиты инфраструктуры электронного правительства от атак, направленных на web сервисы.

5.8.2.1.2 Задачи, которые должны быть решены в ходе выполнения работ

В рамках выполнения работ должны быть актуализированы ПО, конфигурация и политики защиты развернутых в ИЭП WAF Imperva в связи с изменениями в составе и архитектуре защищаемых систем ИЭП.

5.8.2.1.3 Характеристики объекта автоматизации

В состав ИЭП входит 10 шлюзов защиты от атак на web сервисы Imperva X2000, 2 шлюза X6500.

В состав ИЭП входят 2 сервера управления защитой от атак на web сервисы Imperva M150.

Все шлюзы и серверы управления Imperva развернуты в отказоустойчивой конфигурации.

5.8.2.2 Требования к работам

5.8.2.2.1 Общие требования

WAF Imperva не должны нарушать работоспособность ИС ИЭП.

WAF Imperva не должны существенно снижать производительность ИС ИЭП или их компонент.

5.8.2.2.2 Функциональные требования к подсистемам

WAF Imperva должны выявлять весь проходящие через них трафик, передаваемый по протоколам http(s).

Любой запрос пользователя должен ассоциироваться с определенным в модели защищаемым сайтом.

Различные запросы, имеющие схожие URL, но относящиеся к различным сайтам или имеющие различные области допустимых значений передаваемых параметров должны ассоциироваться с различными сайтами в модели.

Пользователь должен получать сообщения об ошибке в дизайне сообщений об ошибке защищаемой системы и содержать тот же набор обязательных параметров.

Сообщение об ошибке, выдаваемое пользователю, должно содержать код события блокировки WAF.

Должны быть активированы все, рекомендуемые производителем, политики фильтрации.

Политика фильтрации может быть деактивирована, если невозможна настройка исключений из нее или порогов ее срабатывания таким образом, чтобы не нарушать работоспособность защищаемой системы.

Политика фильтрации может быть деактивирована, если ее работа с настроенными исключениями или порогами срабатываний не эффективна.

Должна быть установлена последняя, рекомендуемая производителем к использованию, версия ПО и политик фильтрации.

5.8.3 Повышение защищенности тестовых сред

5.8.3.1 Общие сведения

5.8.3.1.1 Цели работ

Целью работ является обеспечение приемлемого уровня защищенности ресурсов, размещенных в тестовых средах ИЭП.

5.8.3.1.2 Задачи, которые должны быть решены в ходе выполнения работ.

В рамках выполнения работ должны быть на основе анализа рисков сформулированы требования по обеспечению защиты тестовых сред. разработаны меры по недопущению нарушений разработанных требований во вновь развертываемых ресурсах в тестовых средах, приведены в соответствие требованиям развернутые системы.

5.8.3.1.3 Характеристики объекта автоматизации

В ТЦОД развернуты тестовые и демонстрационные среды ИС ЭП.

Пользователями сред являются:

- Администраторы;
- Разработчики;
- Контрагенты;
- Заказчики.

Бизнес требования к системам ТЦОД, ограничивающие применение защитных мер

- Демонстрационные среды должны быть доступны для заказчиков и контрагентов без ограничений по времени доступа, паролям;
- Демонстрационные среды должны быть работоспособны во время демонстраций работы сервисов;
- Требования к доступности и времени простоя среды определяются требованиями размещаемых в среде систем;
- Тестовые среды должны быть максимально приближены к продуктивным, не допускаются существенные различия, влияющие на функциональность.

5.8.3.2 Требования к работам

5.8.3.2.1 Общие требования

Мероприятия по повышению защищенности тестовых сред не должны нарушать работоспособность ИС ИЭП.

Мероприятия по повышению защищенности тестовых сред не должны существенно снижать производительность ИС ИЭП или их компонент.

5.8.3.2.2 Функциональные требования к подсистемам

Мероприятия по повышению защищенности тестовых сред должны противодействовать актуальным угрозам ИБ.

Затраты на реализацию мероприятий не должны превышать величину вероятного ущерба от реализации угроз, против которых они направлены.

При разработке методов противодействия угрозам должны использоваться имеющиеся в ИЭП средства защиты информации.

Решения по повышению защищенности должны быть унифицированы с используемыми в ИЭП.

5.8.3.3 Требования к документированию

В рамках работ Исполнителем должна быть разработан следующий комплект документов, содержащий соответствующую информацию:

1. Требования к Информационным Системам, размещаемым в тестовых средах:
   - общие требования к системам и их компонентам;
   - требования к паролям учетных записей и ключевой информации;
   - порядок отключения ИС от тестовой среды в случае несоблюдения требований.
2. Перечень конфиденциальной информации ИЭП:
   - перечень конфиденциальной информации;
   - место и способ хранения и обработки конфиденциальной информации;
   - способ обеспечения конфиденциальности информации.
3. Регламент размещения тестовых сред ИС ИЭП в ТЦОД:
   - раздел, определяющий порядок действий по обеспечению ИБ.
4. Модель защиты ИС, размещаемых в тестовых средах:
   - перечень основных типов активов и актуальных для них типов угроз;
   - описание актуальных типов нарушителей и каналов атак;
   - описание принципов противодействия актуальным угрозам;
   - разработка мер снижения рисков реализации актуальных угроз ИБ.

5.8.4 Интеграция защищаемых ресурсов со средствами контроля защищенности и управления инцидентами безопасности

5.8.4.1 Общие сведения

5.8.4.1.1 Цели работ

Целью работ является актуализация конфигурации средств контроля защищенности и управления инцидентами безопасности.

5.8.4.1.2 Задачи, которые должны быть решены в ходе выполнения работ.

В рамках выполнения работ должна быть проведена интеграция средств контроля защищенности и управления инцидентами безопасности с защищаемыми ресурсами, развернутыми или модифицированными после внедрения указанных средств защиты.

5.8.4.1.3 Характеристики объекта автоматизации

В составе ИЭП развернуто средство контроля защищенности Max Patrol.

В составе ИЭП развернуто средство управления инцидентами безопасности ArcSight.

5.8.4.2 Требования к работам

5.8.4.2.1 Общие требования

Интеграция со средствами защиты не должны нарушать работоспособность ИС ИЭП.

Интеграция со средствами защиты не должны существенно снижать производительность ИС ИЭП или их компонент.

5.8.4.2.2 Функциональные требования к подсистемам

Средство контроля защищенности Max Patrol может быть интегрировано с ресурсами любого из следующих типов:

- Microsoft Windows;
- RedHat Enterprise Linux;
- Solaris;
- HPUX;
- Juniper;
- Cisco IOS;
- Oracle;
- VMware ESX/ESXi.

Средство контроля защищенности Max Patrol должно быть интегрировано минимум с 10 новыми ресурсами.

Средство управления инцидентами безопасности ArcSight может быть интегрировано с ресурсами любого из следующих типов:

- Microsoft Windows;
- RedHat Enterprise Linux;
- Solaris;
- HPUX;
- Juniper;
- Cisco IOS;
- Oracle;
- Microsoft SQL Server;

- Microsoft IIS;
- StoneGate FW/IPS;
- Cisco ASA;
- Imperva;
- MaxPatrol;
- Kaspersky Anti-Virus;
- Weblogic;
- Apache;
- VMware ESX/ESXi;
- Cisco ACS.

5.9. Подсистема мониторинга и контроля оборудования ЭП

5.9.1. Общие требования

Подсистема и ее компоненты должны основываться на следующих общих принципах:

– Решение должно быть централизованным для обеспечения централизованного мониторинга и контроля оборудования, расположенного в территориально распределенных, коллективных центрах обработки данных (КЦОД). Всю вычислительную инфраструктуру системы необходимо сосредоточить в основном, федеральном центре обработки данных (ФЦОД), предоставляющем администраторам полный набор необходимых инструментов мониторинга и управления.

– Подсистема должна быть доступна в любое время для всех участников эксплуатационной группы оборудования (принцип работы 24x7: резервирование, отказоустойчивость, наличие дополнительных источников питания).

– Подсистема должна иметь возможность интеграции с другими системами мониторинга.

– Подсистема должна обеспечивать мониторинг оборудования производителей IBM, HP, Hitachi, Brocade.

– Подсистема должна представлять собой программно-аппаратный комплекс, обеспечивающий функционирование программного обеспечения IBM System Director, HP Systems Insight Manager, Hitachi Data Systems Hi-Track Monitor, являющегося модулями системы.

– Подсистема должна предусматривать возможность расширения вычислительных ресурсов и ресурсов хранения данных, при росте количества эксплуатируемого оборудования.

– Перед внедрением подсистемы необходимо произвести работы по инвентаризации состояния аппаратного обеспечения в КЦОДах.

– Должна быть реализована интеграция с HP Smart Update Manager для легкого и быстрого обновления прошивок всех компонентов инфраструктуры оборудования HP.

– Модули подсистемы должны обеспечивать надежное и безопасное управление посредством поддержки SSL, SSH и аутентификации ОС.

– Программное обеспечение HP Systems Insight Manager должно быть инсталлировано под управлением операционной системы - Linux.

– Модуль подсистемы HP Systems Insight Manager должен позволять группировать оборудование в иерархическом виде с возможностью группировки по типу оборудования, месту эксплуатации, используемой операционной системе.

– Модуль подсистемы HP Systems Insight Manager должен быть настроен на автоматическое обнаружение оборудования в менеджмент сети.

– Программное обеспечение IBM System Director должно быть инсталлировано под управлением операционной системы – Linux.

– Программное обеспечение, Hitachi Data Systems Hi-Track, должно быть инсталлировано под управлением операционной системы – Linux.

– В модуле подсистемы Hitachi Data Systems Hi-Track должны быть заведены эксплуатируемые системы хранения данных модульного типа - Hitachi AMS2100 и оптические коммутаторы сети хранения – Brocade.

– Модули подсистемы, должны содержать как минимум, одну административную учетную запись, с полными правами и одну учетную запись, с правами только на чтение.

– Уведомления о критических событиях должны отправляться на групповые адреса рассылки support-egov@at-consulting.ru , unix_adm@at-consulting.ru.

5.9.2. Требования к структуре и функционированию подсистемы

Подсистема должна состоять из:

- Вычислительной инфраструктуры в составе:
  - Серверного комплекса;
  - Модуля виртуализации.
- Инфраструктуры хранения данных в составе:
  - Сети хранения данных;
  - Модуля хранения данных.
- Телекоммуникационной инфраструктуры;
- Модуля управления и мониторинга.

5.10. Внедрение политик СРК на основании SLA и RTO эксплуатируемых информационных систем

5.10.1. Общие сведения

Одним из основных средств, используемых для обеспечения процесса непрерывности ИТ-услуг, является обеспечение резервного копирования данных АИС. Основной целью резервного копирования данных АИС является предотвращение безвозвратной потери информации в случае различных сбоев в аппаратном или программном обеспечении, а также сокращении времени недоступности ИТ-сервисов.

Ключевыми параметрами резервного копирования являются:

- RPO - Recovery Point Objective
- RTO - Recovery Time Objective.

RPO определяет точку отката — момент времени в прошлом, на который будут восстановлены данные, а RTO определяет время, необходимое для восстановления данных из резервной копии.

На основании данных по RPO формируется параметр "Срок хранения" политики СРК. На основании данных по RTO разрабатывается архитектура СРК и порядок действий администратора при операциях восстановления данных. Оба этих параметра должны быть отражены в SLA, требованиях в ТЗ на АИС, или иных проектных документах АИС.

Регламент резервного копирования (восстановления) программ и данных, хранящихся на серверах ИТ-инфраструктуры Заказчика разрабатывается с целью:

- определения единых требований, стратегии и порядка резервирования данных для последующего восстановления работоспособности АИС Заказчика при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- определения порядка восстановления информации в случае возникновения такой необходимости;
- упорядочения работы должностных лиц Исполнителя и Заказчика, связанной с резервным копированием и восстановлением информации

В документе должны указываться данные, необходимые при выполнении следующих мероприятий:

- резервное копирование (архивирование);
- контроль резервного копирования;
- хранение резервных копий;
- полное или частичное восстановление данных и приложений.

Для получения входных данных для реализации политики СРК необходимо провести аудит данных с целью выделения критичных данных, для которых требуется создание резервных копий (архивов), инфраструктуры, получить показатели по прогнозному росту объема данных, SLA-показателей, требований Заказчика к СРК.

По результатам исследования разрабатывается архитектура СРК.

Система резервного копирования построена по трехуровневой модели: клиент – сервер копирования данных – сервер управления. С точки зрения СРК, серверы, входящие в состав АИС, являются клиентами. Серверы копирования данных – часть серверов СРК, отвечающих за работу с устройствами хранения. Сервер управления – сервер СРК, отвечающий за управление процессами копирования и восстановления, управление потоками данных и носителями.

Клиентами СРК являются серверы, на которых развернуты информационные подсистемы АИС, в частности:

- СУБД;

– Серверы приложений;

– Серверы подсистемы виртуализации.

В состав СРК входят следующие аппаратные компоненты:

– Серверы резервного копирования;

– Ресурсы дискового массива, ленточных библиотек для целей резервного копирования.

В состав СРК входят следующие программные компоненты:

– Сервер резервного копирования под управлением ПО Symantec NetBackup;

– Агенты резервного копирования;

– Агенты интеграции с приложениями.

Для реализации СРК определяются выделенные дисковые и ленточные устройства хранения на уровне системы хранения данных, серверы СРК, серверное и клиентское ПО Symantec NetBackup 7.5, включающее в себя агенты интеграции с виртуальными подсистемами (VMware, Hyper-V), подсистемами баз данных (Oracle Database, MS SQL).

С точки зрения ПО Symantec NetBackup архитектура ПО СРК состоит из:

Мастер-сервер. Сервер управления процессами резервного копирования и восстановления в системах на основе NetBackup называется мастер-сервером. Мастер-сервер обслуживает каталог СРК, а так же управляет всеми компонентами системы резервного копирования. При централизованной архитектуре используется один мастер-сервер, или 2 и более - по количеству нод кластера при кластеризации мастер-сервера.

Медиа-сервер. Сервер, обеспечивающий запись резервных копий на устройства хранения в системах на основе NetBackup называется медиа-сервером. Медиа-серверы NetBackup версии 7.0 и выше не поддерживают кластеризацию.

Агенты резервного копирования и интеграции с приложениями. Для выполнения резервного копирования на клиенты СРК устанавливаются программные агенты, обеспечивающие сбор информации подлежащей копированию, передачу на серверы, а так же необходимое взаимодействие с прикладными системами для получения корректных и целостных копий данных.

Для создания высокодоступной (отказоустойчивой) архитектуры СРК предлагается реализовать комплекс мероприятий, которые должны быть отражены в политике СРК:

– создание кластеризованного главного управляющего мастер-сервера на основе ПО Veritas Cluster Server, или любого другого средства кластеризации, поддерживаемого ПО Symantec NetBackup. При этом основная активная нода кластера располагается на основной площадке, пассивная же нода кластера располагается на удаленной резервной площадке и активируется автоматически при сбое активной ноды кластера.

– создание локальной резервной копии на основной площадке и дополнительной копии на удаленной площадке, создаваемой в режиме клонирования. Таким образом, сначала резервная копия создается на выделенном ресурсе СХД основной площадки и затем уже происходит репликация копии с выделенного ресурса СХД основной площадки на выделенный ресурс СХД удаленной площадки. При этом в качестве транспортного канала для среды СРК на основной площадке будет использоваться SAN, на удаленной площадке – сначала по сети передачи данных WAN до медиа-сервера, расположенного на удаленной площадке, затем – по сети хранения данных SAN непосредственно до СХД, подключенного к медиа-серверу. Для детальной настройки политик резервного копирования может применяться утилита Storage Lifecycle Policies (SLP), являющаяся функциональной частью ПО Symantec NetBackup. Также для ускорения операции полного резервного копирования на удаленной площадке могут применяться синтетические полные резервные копии, а также механизмы дедупликации;

– отказоустойчивость заданий копирования и восстановления должна быть обеспечена с помощью использования множественных путей для передачи данных, на сетевом уровне – применением Link Aggregation Control Protocol (LACP), на уровне SAN транспорта – применением SAN Multipathing.

– предпочтительно использовать SAN-транспорт при резервном копировании клиентов СРК. Такая конфигурация позволит минимизировать влияние процессов резервного копирования на продуктивные физические машины.

– при реализации домена СРК, состоящего из нескольких медиа-серверов, использовать балансировку нагрузки на медиа-серверы системы резервного копирования при их неравномерной загруженности. При использовании группы устройств хранения данных, расположенных на разных медиа-серверах, ПО NetBackup при включенной опции «Media Server Load Balancing» автоматически выбирает устройство хранения на наименее загруженном медиа-сервере.

– настроить СРК виртуальной подсистемы со следующими характеристиками: резервное копирование на уровне образов виртуальных машин, используя интегрированное взаимодействие с гипервизорами (VMware ESXi, Hyper-V), с возможностью оптимизации использованием технологий инкрементального бэкапа на уровне блоков (используется механизм отслеживания измененных блоков (block change tracking) ПО VMware), исключением удаленных блоков из резервных копий образов виртуальных машин, а также содержимого swap-файлов. Такая конфигурация представляет собой резервное копирование виртуальных машин offhost-типа на основе снимков (снапшотов) виртуальных машин. Здесь "offhost" предполагает использование специализированного агента на выделенном сервере с ОС Windows Server 2008 и отсутствие клиентского ПО СРК внутри гостевых операционных систем виртуальных машин, что позволит минимизировать влияние процессов резервного копирования на продуктивные виртуальные машины, а также упростит развертывание и администрирование СРК виртуальных подсистем;

– настройка возможности гранулярного восстановления на файловом уровне отдельных файлов и директорий. Такая возможность на текущий момент реализована для виртуальных машин с гостевыми операционными системами типа Linux, Windows;

– при перемещении виртуальных машин на удаленную площадку и смене DNS-имени сервера возможно автоматическое возобновление операций копирования при использовании автоматического определения с использованием правил Query Builder;

– в качестве централизованного средства управления и мониторинга предлагается использовать консоль Java NetBackup Administration Console, а также web-консоль OpsCenter (применяется независимо от архитектуры, особенно удобна при децентрализованной архитектуре). Необходимо настроить средства отправки оповещений по почте о проблемах в СРК, а также интегрировать мониторинг наиболее критичных параметров СРК с системой мониторинга Zabbix.

Политика СРК должна в обязательном порядке включать в себя следующую информацию:

– краткое описание архитектуры домена СРК для АИС

– наименования ключевых узлов домена, список файлов/баз данных/ключевых виртуальных машин и других данных АИС

Наименование колонки	Описание колонки
Имя узла	Наименование сервера
Назначение	Назначение сервера
ПО	Сокращенное название клиента и его версия
Тип копирования	Каким образом передаются данные от клиента серверу
Агент	Размещение клиентского ПО СРК
Политика	Наименование политики СРК, внутри сервера СРК
Перечень ресурсов	Перечень ресурсов подлежащих резервному копированию

– расписание резервного копирования (время, дни недели, периодичность копирования)

Наименование колонки	Описание колонки
Политика	Наименование политики
Имя задания	Наименования задания резервного копирования
Вид копирования	Вид резервного копирования Для всех ресурсов, кроме БД: - полное

Наименование колонки	Описание колонки
	- кумулятивное инкрементальное - дифференциальное инкрементальное Для БД: - полное - полное, инкрементальное 0 уровня - инкрементальное 1 уровня - кумулятивное 1 уровня - резервное копирование архивных логов
Расписание	Расписание выполнения заданий резервного копирования
Срок хранения	Срок хранения резервных копий
Компрессия	Наличие компрессии данных в рамках задания - аппаратная компрессия - программная компрессия
Место хранения	Расположение резервных копий, после осуществления резервного копирования

– информацию о ресурсах и инструментах резервного копирования

Наименование колонки	Описание колонки
Имя	Наименование ленточного/дискового пула
Тип	Тип устройства хранения DSU - disk storage unit - дисковое устройство хранения TSU - tape storage unit - ленточное устройство хранения DSSU - disk staging storage unit - дисковое промежуточное устройство хранения
Имя медиа-сервера	Наименование медиа-сервера СРК к которому подключено устройство
Путь (для DSU, DSSU)	Логический путь до устройства хранения
Максимальный размер (capacity)	Максимальный возможный размер для записи резервных копий
Параллелизм	Наличие и степень параллелизма

Машинным носителям информации, содержащим резервную копию, присваивается гриф конфиденциальности по наивысшему грифу содержащихся на них сведений в соответствии с перечнем конфиденциальных сведений Заказчика.

Информация по резервным копиям (архивам), содержащим конфиденциальные данные или сведения содержащие государственную тайну, а также местам их хранения должна отражаться в политике СРК.

Аудит актуальности политики СРК должен проводиться на периодической основе (каждые 3 месяца). Администратор СРК должен проводить аудит корректности СРК, а также осуществлять сверку требований к резервированию АИС с реальным состоянием СРК.

По результатам сверки происходит согласование расхождений и вносятся изменения в настройки СРК, либо в политику СРК.

5.11. Внедрение эксплуатационных инструкций на типовые операции инженеров и администраторов вычислительной инфраструктуры ЭП

5.11.1. Общие сведения

5.11.1.1 Назначение эксплуатационных инструкций

Эксплуатационные инструкции предназначены для регламентированного, бесперебойного и качественного обслуживания ИТ-инфраструктуры заказчика всеми участниками процесса эксплуатации.

Документированию и регламентированию должны подлежать следующие технические процессы:

- ввод в эксплуатацию, модернизация, вывод из эксплуатации оборудования и ПО (учет ИТ-активов, оборудования и ПО);
- управление компонентами ИТ-инфраструктуры и их конфигурациями;
- управление проблемами и учет ошибок ИТ-инфраструктуры;
- управление кабельными соединениями ИТ-инфраструктуры;
- плановое техническое обслуживание (замена компонентов или изменение параметров работы) объектов ИТ-инфраструктуры;
- аварийное обслуживание объектов ИТ-инфраструктуры.

5.11.1.2 Цели внедрения эксплуатационных инструкций

Целью внедрения эксплуатационных инструкций является обеспечение эффективного и безотказного функционирования ИЭП и Облачной платформы (далее – ИТ-инфраструктура), путем регламентирования типовых операций инженеров и администраторов ИТ-инфраструктуры.

Основными целями внедрения эксплуатационных инструкций являются:

- поддержание в актуальном состоянии информация, в режиме on-line, о компонентах инфраструктуры (оборудование, программное обеспечение, лицензии, техническая поддержка) ЭП;
- поддержание в актуальном состоянии информации, в режиме on-line, о существующих ошибках и их статусах в КЦОД, ФЦОД, Облачной платформе, УЦЭП на компонентах ИТ-инфраструктуры;
- поддержание в актуальном состоянии информация, в режиме on-line, о кабельных соединениях информационной и электрической сети компонентов ИТ-инфраструктуры;
- анализ повторяющихся сбоев в ИТ-инфраструктуре и их характер, с целью прогнозирования замены оборудования в плановом режиме;
- исполнение соглашения SLA в процессе решения инцидентов;
- оперативное принятие решений по закупке ПО/upgrade железа/замена неисправных компонентов и т.п.;
- снижение времени на выполнение однотипных операций по обслуживанию ИТ-инфраструктуры;
- обеспечение взаимозаменяемости технического персонала.

5.11.1.3 Задачи, требующие решения в рамках выполнения работ

В рамках выполнения работ должны быть решены следующие задачи:

- Разработать регламент учета ИТ-активов ИТ-инфраструктуры (учет оборудования и ПО);
- Разработать регламент учета ошибок ИТ-инфраструктуры;

- Разработать регламент учета кабельных соединений ИТ-инфраструктуры (информационная и электрические сети);
- Разработать инструкции по замене основных компонентов ключевых объектов ИТ-инфраструктуры (жесткие диски, блоки питания, картриджи ленточных библиотек)
- Разработать регламент аварийного отключения оборудования и информационных систем ФЦОД.

5.11.1.4 Регламент учета ИТ-активов ИТ-инфраструктуры

Документ должен содержать:

- Описание ролей сотрудников в рамках процесса учета ИТ-активов ИЭП;
- Порядок и схему действий при постановке на учет новых ИТ-активов, с описанием ответственных и сроков исполнения;
- Порядок и схему действий при изменении данных учета материальных ИТ-активов, с описанием ответственных и сроков исполнения;
- Порядок и схему действий при изменении данных учета нематериальных ИТ-активов, с описанием ответственных и сроков исполнения;
- Правила учета договоров поставок ИТ-активов;
- Регламент должен учитывать следующую информацию:

- Номер договора
- Дата договора
- Краткое описание
- Организация - Поставщик
- Организация - Заказчик
- Контакт - Поставщик
- Контакт - Заказчик
- Код проекта
- Руководитель проекта

- Правила ведения склада ИТ-активов;

Регламент должен учитывать следующую информацию:

- Производитель
- Парт-номер (P/N)
- Название оборудования
- Количество
- Серийный номер (S/N)
- Помещение склада
- Примечание
- Тип оборудования
- Дата поступления на склад
- Дата убытия со склада
- Наличие на складе
- Договор поставки
- Дата договора

- Правила ведения Журнала перемещений ИТ-активов;

Регламент должен учитывать следующую информацию:

- Дата перемещения
- Название оборудования

- Количество
- Серийный номер (S/N)
- Номер тикета СКУФ
- Ответственный
- Цель перемещения
- Исходное местоположение
- Пункт назначения
- Примечание

- Правила учета оборудования ИЭП;

Регламент должен учитывать следующую информацию:

- Тип единицы учета
- Тип оборудования
- Производитель
- Парт-номер (P/N)
- Название оборудования
- Модель
- Количество
- Серийный номер (S/N)
- Статус системы
- Стойка
- Юнит
- Шасси
- Слот
- Объем ОЗУ, Гб
- Тип процессора
- Количество CPU
- Тип HDD
- Количество HDD
- Количество БП
- Стоимость тех. поддержки (год)
- Дата завершения бесплатной замены по гарантии
- Ответственный за использование/эксплуатацию
- Сетевое имя (маркировка)
- FQDN
- Операционная система
- Тип подключения
- Firmware
- IP-адрес OS
- IP-адрес дополнительный
- IP-адрес управления
- Роль в системе
- Подсистема (Реально используется)
- ИС (реально используется)
- Инвентарный номер
- Номер инвентарной карточки
- Номер накладной
- Дата накладной

- Договор поставки
- Договор поставки технической поддержки
- Место эксплуатации
- Помещение
- Примечание
- Дата договора поставки
- Дата договора поставки технической поддержки

- Правила учета ПО и лицензий ИЭП.

Регламент должен учитывать следующую информацию:

- Тип единицы учета
- Производитель
- Парт-номер (P/N)
- Название ПО/лицензии
- Тип лицензии
- Количество
- Статус системы
- Дата окончания расширенной поддержки вендора
- Срок действия ПО
- Ответственный за использование/эксплуатацию
- Подсистема (Реально используется)
- ИС (реально используется)
- Номер накладной
- Дата накладной
- Договор поставки
- Договор поставки технической поддержки
- Место эксплуатации
- Помещение
- Примечание
- Дата договора поставки
- Дата договора поставки технической поддержки
- Номер лицензии
- Авторизационный номер лицензиата

В данном регламенте должно быть указано географическое местоположение всех объектов ИТ-инфраструктуры Заказчика. За каждым объектом ИТ-инфраструктуры заказчика должен быть закреплен ответственный.

5.11.1.5 Регламент учета ошибок ИТ-инфраструктуры

Документ должен учитывать следующую информацию:

- Статус ошибки;
- Дата обнаружения;
- Стойка;
- Юнит;
- Имя оборудования/маркировка;
- Серийный номер;
- Инвентарный номер;
- Описание ошибки;
- Место эксплуатации;

- Помещение;
- Номер тикета в СКУФ;
- Название оборудования;
- Дата устранения ошибки.

В данном регламенте должно быть указано географическое местоположение всех объектов ИТ-инфраструктуры Заказчика. За каждым объектом ИТ-инфраструктуры заказчика должен быть закреплен ответственный.

5.11.1.6 Регламент учета кабельных соединений ИТ-инфраструктуры

Документ должен учитывать следующую информацию (для учета кабельных соединений информационной сети):

- Стойка (откуда);
- Юнит (откуда);
- Имя оборудования/маркировка (откуда);
- Оборудование (откуда);
- Инвентарный номер (откуда);
- Серийный номер (откуда);
- Порт (откуда);
- Название розетки (транзит-откуда);
- Стойка (куда);
- Юнит (куда);
- Имя оборудования/маркировка (куда);
- Оборудование (куда);
- Инвентарный номер (куда);
- Серийный номер (куда);
- Порт (куда);
- Название розетки (транзит-куда);
- Тип разъема;
- Номер кабеля;
- Примечание.

Документ должен учитывать следующую информацию (для учета кабельных соединений электрической сети):

- Номер электрического щитка;
- Маркировка автомата;
- Нагрузка автомата;
- Стойка;
- Маркировка модуля распределения питания (далее PDU);
- Модель PDU;
- Тип разъема PDU;
- Номер порта PDU;
- Маркировка блока розеток;
- Тип разъема блока розеток;
- Номер порта блока розеток;
- Юнит;
- Имя оборудования, маркировка ;
- Серийный номер;

- Инвентарный номер;
- № Блока питания;
- Мощность БП, Вт;
- Название оборудования;
- № кабеля.

5.11.1.7 Инструкции по замене основных компонентов ключевых объектов ИТ-инфраструктуры

Инструкции должны содержать пошаговую информацию о:

- Замене жестких дисков для массивов Hitachi серии AMS2000;
- Замене блоков питания для массивов Hitachi серии AMS2000;
- Замене и обслуживании элементов ленточной библиотеки SUN SL500;
- Замене и обслуживании элементов ленточной библиотеки IBM TS3200;
- Замене и обслуживании элементов ленточной библиотеки IBM TSL3310;
- Подключении к консольным портам оборудования с помощью консольного сервера Avocent ACS6032.

5.11.1.8 Регламент аварийного отключения оборудования и ИС ФЦОД

Документ должен учитывать следующую информацию:

- Типы аварий и порядок действий инженерного персонала при их возникновении;
- Порядок действий при нарушении стабильности ЦОД;
- Порядок действия при аварии в ЦОД;
- Порядок действий по восстановлению планового режима работы ЦОД после аварии;
- План экстренного выключения ЦОД;
- План перевода ЦОД в аварийный режим работы;
- План восстановления штатного режима работы ЦОД.

5.11.2. Объекты ИТ-инфраструктуры

Эксплуатационные инструкции и регламенты должны охватывать следующие объекты ИТ-инфраструктуры Заказчика:

- ФЦОД (г. Москва, ул. Сущевский вал, д. 26);
- Облачная платформа (г. Москва, ул. Сущевский вал, д. 26;г. Москва, ул. Гончарная, д. 30, стр. 1;г. Новосибирск, ул. Менделеева, д. 1);
- УЦЭП (г. Москва, ул. Сущевский вал, д. 26);
- КЦОД-2 (г. Хабаровск, ул. Тихоокеанская, д. 181);
- КЦОД-3 (г. Санкт-Петербург, ул. Синопская набережная, д. 14);
- КЦОД-4 (г. Новосибирск, ул. Менделеева, д. 1);
- КЦОД-5 (г. Екатеринбург, пер. Асбестовский, д. 4а);
- КЦОД-6 (г. Казань, ул. Можайского, д. 6а);
- КЦОД-7 (г. Краснодар, ул. Красная, д. 59).

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

6.1. Виды, состав, объем и методы испытаний

Испытания должны быть организованы и проведены в соответствии с ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем».

Должны быть проведены следующие виды испытаний:

- предварительные испытания;
- опытная эксплуатация (ОЭ);
- приемочные испытания.

Объем и методы предварительных и приемочных испытаний определяются соответствующей «Программой и методикой испытаний».

Программа и методика приемочных испытаний разрабатывается с учетом результатов ОЭ, при этом проверки Системы в части не устраненных высококритичных недостатков реализации Системы, ОЭ, выносятся в специальный раздел ПМ.

При проведении перечисленных испытаний в части информационного взаимодействия Системы с иными системами проверяется наличие в Системе и соответствие установленным требованиям сервисов приема/передачи данных. Возможность проверки реального информационного взаимодействия производится в случае предоставления сервисным оператором данных, определенных соответствующим Регламентом информационного взаимодействия.

6.2. Общие требования к приемке работ

Приемка результатов работ осуществляется поэтапно в соответствии с Календарным планом выполнения работ по Договору.

Приемка результатов выполнения работ по этапам оформляется Актом сдачи-приемки работ по каждому этапу работ, а также Финальным актом сдачи-приемки работ по завершении последнего этапа работ. Основанием для составления и подписания Акта сдачи-приемки работ по отдельному этапу является передача Исполнителем технической документации в соответствии с условиями Договора и (при проведении испытаний) утвержденных сторонами соответствующих Актов приемки в эксплуатацию.

Техническая и эксплуатационная документация и другие результаты работ передаются Заказчику в порядке, определенном пунктом 1.9 «Порядок оформления и предъявления заказчику результатов работ». Комплектность передаваемой технической документации подлежит проверке Заказчиком.

Предусмотренные испытания проводятся комиссией, формируемой Заказчиком на основании распорядительного документа, который должен определять состав комиссии проведения испытаний (предварительных и приемочных испытаний), порядок ее работы, место и сроки проведения испытаний.

В состав комиссии включаются представители организаций Заказчика, Пользователя и Исполнителя, а также специалисты, привлекаемые Заказчиком.

Результаты проведения испытаний должны быть зафиксированы в соответствующих Протоколах испытаний. Как недостатки реализации оформляются исключительно выявленные отклонения от Технического задания. Прочие недостатки могут документироваться как желательные доработки. Наличие желательных доработок не влияет на процесс передачи в эксплуатацию.

По завершении предварительных и приемочных испытаний оформляются соответствующие Акты, содержащие вывод о соответствии Системы предъявляемым требованиям, а также сроки устранения замечаний и реализации рекомендаций, данных комиссией в ходе испытаний. Результаты опытной эксплуатации отражаются в документе «Отчет о проведении опытной эксплуатации»[2] и рассматриваются в ходе приемочных испытаний.

[2] Документ включается в рабочую документацию приемочных испытаний.

Условием для передачи Системы в опытную или промышленную эксплуатацию является устранение всех замечаний с высоким уровнем критичности на предыдущих этапах.

В случае значительного отклонения Системы от требований, предъявляемых на испытаниях, сроки проведения испытаний могут быть перенесены / расширены Заказчиком в пределах сроков выполнения работ в соответствии с Календарным планом выполнения работ.

6.3. Сведения о гарантийном обслуживании

Исполнитель осуществляет бесплатное гарантийное сопровождение Системы не менее 12 месяцев со дня подписания Финального акта сдачи-приемки выполненных работ.

Исполнитель должен гарантировать, что установленное программное обеспечение Системы будет функционировать в соответствии со своим назначением не менее одного года. При этом возможны незначительные отклонения его технических и потребительских характеристик, а также отдельные ошибки, не создающие препятствий для получения положительных результатов от эксплуатации Системы.

Исполнитель не гарантирует отсутствие недостатков или сбоев в процессе работы, возникающих по причине несоответствия оборудования или установленного на рабочем месте программного обеспечения конечного пользователя требованиям, предъявляемым к характеристикам клиентских мест.

6.4. Порядок выполнения доработок и устранения допущенных исполнителем ошибок, выявленных на стадии приемки

Недостатки и ошибки в реализации системы, выявленные в ходе проведения испытаний, должны быть устранены Исполнителем в рамках выполнения работ по Договору. Порядок устранения замечаний и реализации рекомендаций комиссии должен быть определен в документах «Программа и методика испытаний» и «Программа опытной эксплуатации». Сроки устранения замечаний и реализации рекомендаций, данных приемочной комиссией в ходе испытаний, определяются в Актах приемки в эксплуатацию.

6.5. Сведения об обслуживании Системы

Состав работ (услуг) по эксплуатации Системы, а также их периодичность и требования к составу и квалификации обслуживающего персонала определяются в эксплуатационной документации на Систему. При этом требования к эксплуатации компьютерного оборудования, системного и прикладного программного обеспечения, входящего в состав Системы, указываемые в эксплуатационной документации, должны соответствовать требованиям к эксплуатации соответствующего оборудования и программного обеспечения, изложенным в документации, поставляемой вместе с данным оборудованием и программным обеспечением при его приобретении.

Системное и прикладное сопровождение, техническое сопровождение аппаратного обеспечения, системное сопровождение средств защиты информации, организация учебного процесса пользователей и другие работы (услуги) производятся на основании договоров на выполнение соответствующих работ (услуг).

7. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ В ДЕЙСТВИЕ

7.1. Развертывание и конфигурирование

Система должна быть установлена Исполнителем на оборудовании, предоставленном Заказчиком. Должен быть установлен передаваемый на машинных носителях дистрибутив и предварительная конфигурация.

Дальнейшее конфигурирование должно быть выполнено Исполнителем (сервисным оператором) в соответствии с инструкцией по развертыванию системы, приведенной в руководстве Администратора.

В случае необходимости, Исполнителем должны быть установлены обновления, выпущенные по итогам испытаний, если эти обновления не включены в состав Дистрибутива.

7.2. Приведение поступающей в систему информации к виду, пригодному для обработки с помощью ЭВМ

Для приведения поступающей в Систему информации к виду, пригодному для обработки с помощью ЭВМ должны быть проведены системно-аналитические мероприятия по формализации, категоризации, описания атрибутивного состава документов и форм аналитического и статистического учета.

Должны быть описаны и утверждены вновь вводимые справочники и классификаторы.

Исполнителем должны быть разработаны и утверждены отчетные и экранные формы компонентов Системы, включая компоненты для однократного первичного ручного ввода исходных данных в систему.

В случае необходимости Исполнитель должен обеспечить ручной ввод исходных данных в систему в случае отсутствия этих данных в электронном виде на машинных носителях.

Исполнителем должны быть разработаны механизмы для автоматической загрузки данных с существующих электронные носителей.

7.3. Изменения, которые необходимо осуществить в объекте автоматизации

7.3.1 Сроки и порядок комплектования штатов и обучения персонала

Комплектование штатов и подразделений, необходимых для функционирования Системы, а также подготовка их сотрудников должны быть завершены до начала опытной эксплуатации Системы.

Обучение персонала должно проводится Исполнителем по разработанным руководствам пользователей и документу «План-программа подготовки персонала по категориям».

Обучаемый персонал должен быть обеспечен необходимыми инструкциями и методическими материалами.

По завершении обучения должны быть оформлены протоколы о проведенной подготовке персонала Заказчика.

8. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Для СКУФ должна быть разработана следующая отчетная документация:

- Частные технические задания на создание подсистем;
- Технический проект на создание Системы;
- Эксплуатационная документация на Систему;
- Программа и методика приемочных испытаний;
- Протокол приёмочных испытаний Системы.

Отчетная документация должна прилагаться в бумажном и электронном виде (на CD или DVD носителе) на русском языке.

Вспомогательная документация (не указанная в качестве непосредственного результата работ) передается только в электронном виде.

9. ИНФОРМАЦИОННЫЕ ИСТОЧНИКИ

В настоящем документе использованы следующие нормативные документы:

- нормативно-технические документы:
  - ГОСТ 12.2.003 «Система стандартов безопасности труда. Оборудование производственное. Общие требования безопасности»;
  - ГОСТ 19542–83 «Совместимость средств вычислительной техники электромагнитная. Термины и определения»;
  - ГОСТ 21552-84 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение»;
  - ГОСТ 25861-83 «Машины вычислительные и системы обработки данных. Требования по электрической и механической безопасности и методы испытаний»;
  - ГОСТ 27.001-95 «Надежность в технике. Основные положения»;
  - ГОСТ 27.003.90 «Надежность в технике. Состав и общие правила задания требований по надежности»;
  - ГОСТ Р 50628-2000 «Совместимость технических средств электромагнитная. Устойчивость машин электронных вычислительных персональных к электромагнитным помехам. Требования и методы испытаний»;
  - ГОСТ 27201–87 «Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования»;
  - ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;
  - ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
  - ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Стадии создания»;
  - ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;
  - ГОСТ 34.603-92 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем»;
  - РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов».

Приложение № 1
к Техническому заданию

Календарный план
выполнения опытно-конструкторских работ по развитию системы мониторинга и управления функционированием сетью ЦОД в части создания опытного образца комплексного сервиса системы контроля и управления функционированием (СКУФ) облачной платформы

№ этапа	Наименование этапа	Состав работ	Результат работ	Сроки выполнения работ
Этап № 1	Анализ задачи, формирование требований к созданию Системы	Разработка ТТ на создание и внедрение Системы Разработка регламентов ИТ процессов	ТТ на внедрение Системы Частные ТЗ на подсистемы Регламенты внедряемых ИТ процессов	Минимальные и максимальные сроки выполнения работ указаны в п.2 Информационной карты
Этап № 2	Проектирование и создание Системы	Разработка технического проекта Системы Разработка эксплуатационной документации на Систему Разработка документации для проведения предварительных и приемочных испытаний Системы Проектирование и создание опытного образца системы мониторинга и управления функционированием сетью ЦОД в части создания опытного образца комплексного сервиса системы контроля и управления функционированием (СКУФ) облачной платформы	Технический проект на Систему Эксплуатационная документация на Систему Программа и методика предварительных испытаний Системы Программа и методика приемочных испытаний Системы Рабочий проект и опытный образец Системы	Минимальные и максимальные сроки выполнения работ указаны в п.2 Информационной карты
Этап № 3	Внедрение Системы	Испытания Системы: – предварительные испытания; – приемочные испытания	Протокол предварительных испытаний Протокол и акт приемочных испытаний	Минимальные и максимальные сроки выполнения работ указаны в п.2 Информационной карты
		Проведение инструктажа по работе с Системой сотрудников Заказчика	Протоколы (Акты) проведения инструктажа.	
		Проведение инструктажа сотрудников Заказчика по использованию разработанных ИТ процессов, регламентов и инструкций	Протоколы (Акты) проведения инструктажа.	

№ этапа	Наименование этапа	Состав работ	Результат работ	Сроки выполнения работ
		Разработка и внедрение Инструкций по работе ЦПП, 1ЛП и 2ЛП Инфраструктуры заказчика с использованием созданной Системы. Консультирование сотрудников эксплуатации в течение ОПЭ Проведение ОПЭ	Инструкции для ЦПП, 1ЛП, 2ЛП. Акт о проведении ОПЭ	
		Создание базы знаний и формализованных видео- и презентационных обучающих материалов по работе с Системой и использованию разработанных ИТ процессов для сотрудников ЦПП, 1ЛП и 2ЛП	Обучающие материалы Акт сдачи-приемки обучающих материалов	