

ПРИЛОЖЕНИЕ К ОПИСАНИЮ ОБЪЕКТА НА ЗАКУПКУ

ТЕХНИЧЕСКОЕ ЗАДАНИЕ 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Таблица 1.1 – Перечень терминов и определений

Термин	Определение
Время доступности функции (рабочее время)	Период времени, в течение которого должно обеспечиваться исполнение функции СТП
Время реакции на обращение (время реакции), T1	Период времени от момента регистрации обращения до наступления одного из следующих событий: - принятия заявки в работу и подтверждения типа обращения; - запрос дополнительной информации по обращению у заявителя.
Время решения обращения (время решения), T2	Время от момента регистрации заявки до момента закрытия заявки, с учетом приоритета заявки, без учета времени уточнения у Инициатора обращения дополнительных сведений и времени реакции на предоставленные Инициатором обращения уточнения.
ГК	Государственный контракт (Контракт).
Дефект в РНИС СО (программный дефект)	Программным дефектом называется ошибка в программном коде РНИС СО, вследствие которой работа функций РНИС СО отличается от описанной в проектной и рабочей документации на РНИС СО.
Заявка, обращение	Обращение Государственного заказчика с описанием проблемы в работе РНИС СО
Инициатор обращения	Пользователь РНИС СО, обратившийся в СТП в рамках оказания услуг по ГК.
ОПО	Общее программное обеспечение ИС. Часть программного обеспечения ИС, представляющая собой совокупность программных средств, разработанную вне связи с созданием и/или развитием ИС. В состав общего программного обеспечения входят: - операционные системы (ОС); - системы управления базами данных (СУБД); - серверы приложений (веб-серверы) и их компоненты; - интерпретаторы; - средства разработки; - системные утилиты и драйверы; - программные средства безопасности (антивирусы, средства защиты информации от несанкционированного доступа и тд.)
Ответственный представитель Государственного заказчика	Представитель Государственного заказчика, координирующий и контролирующий ход оказания услуг по Контракту. Представитель вправе: - выбирать сроки устранения программных дефектов путем выбора соответствующей операции (см. Таблица 1.8); - запрашивать внеочередное предоставление отчетов для контроля оказания услуг по технической поддержке.
Рабочие дни, (D)	По умолчанию количество рабочих дней равно 5 рабочим дням в неделю. Рабочие дни устанавливаются в соответствии с Трудовым кодексом РФ. Выходные и праздничные дни в соответствии с Постановлениями Правительства РФ.
Регистрация обращения	Процедура, позволяющая зарегистрировать факт обращения пользователя в СТП. Регистрация обращений производится в системе учета обращений Исполнителя.
Режим доступности функции (режим работы)	График рабочего времени, в течение которого осуществляется исполнение функций СТП, состоящий из количества рабочих часов и количества рабочих дней.

	Возможные варианты: - 8xD – 8 рабочих часов, D рабочих дней в неделю; - 9xD – 9 рабочих часов D рабочих дней в неделю; - 24x7 – круглосуточно. Время, находящееся за пределами, указанного режима является нерабочим.
РНИС СО, Система	Региональная навигационно-информационная система Сахалинской области
СТП Заказчика	Представители Государственного заказчика, курирующие функционирование РНИС СО
СТП Исполнителя	Служба технической поддержки Исполнителя – функция Исполнителя, обеспечивающая оказание услуг по технической поддержке Системы.
Тип обращения	Признак, по которому производится классификация обращений в СТП Исполнителя
ЦОД	Центр обработки данных

2. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ

2.1. Общие требования.

РНИС СО функционирует в соответствии с приказом Министерства транспорта и дорожного хозяйства Сахалинской области от 19.01.2024 № 1-3.09-30/24 «О государственной информационной системе Сахалинской области «Региональная навигационно-информационная система Сахалинской области».

РНИС СО обеспечивает выполнение следующих задач:

- контроль передвижения и диспетчеризация транспортных средств;
- сбор и систематизация информации о функционировании транспортного комплекса Сахалинской области, в том числе для обеспечения анализа качества транспортного обслуживания населения, а также пассажирских и грузовых потоков;
- консолидацию, обработку и визуализацию данных транспортного комплекса, мониторинг ключевых показателей и информационную поддержку принятия управленческих решений;
- автоматизированный учет транспортных работ на территории Сахалинской области, включая учет аварийных ситуаций на транспорте;
- информационное обеспечение потребителей услуг транспортного комплекса Сахалинской области;
- взаимодействие с внешними информационными системами.

РНИС СО имеет модульную структуру, включающую в себя следующие подсистемы и функциональные модули:

- Подсистема мониторинга и управления пассажирскими перевозками;
- Подсистема мониторинга и управления пассажирскими и грузовыми морскими перевозками;
- Подсистема мониторинга и управления дорожной техникой;
- Модуль отчетности;
- Модуль диспетчеризации;
- Модуль оповещения.

В рамках оказания услуг Исполнитель обеспечивает техническую поддержку РНИС СО, введённой в эксплуатацию распоряжением Министерства транспорта и дорожного хозяйства Сахалинской области от 10.10.2024 № 3.09-181-р, а также дополнительных модулей и подсистем, включаемых в состав системы при её модернизации и развитии, независимо от периода их ввода в эксплуатацию.

Оказание услуг по технической поддержке РНИС СО должно осуществляться СТП Исполнителя в полном объёме с момента подписания контракта и в соответствии с требованиями настоящего технического задания.

СТП Исполнителя должна:

- выполнять функции/задачи СТП в соответствии с распределением ответственности, указанным в Таблице 3.1;

- обеспечить режим доступности функций в соответствии с режимами, определенными в Таблице 3.2.

СТП Исполнителя организует учет и обработку обращений в систему учета обращений Исполнителя.

Место оказания услуг – в соответствии с условиями Контракта.

Организация удалённого подключения осуществляется в соответствии с пунктом 3.8 настоящего Технического задания и заключенным Соглашением о конфиденциальности (Приложение № 1 к Техническому заданию).

Услуги оказываются по местному времени Заказчика (10-я часовая зона (МСК+8, московское время плюс 8 часов, UTC+11), Сахалинская область) в соответствии с п. 10 ч. 1 ст. 5 Федерального закона от 03.06.2011 № 107-ФЗ «Об исчислении времени».

2.2. Перечень услуг по технической поддержке РНИС СО.

В рамках технической поддержки РНИС СО Исполнитель должен оказывать следующие виды услуг в отношении компонентов РНИС СО (Таблица 2.1):

Таблица 2.1 – Обслуживаемые компоненты РНИС СО

№ п/п	Типы услуг	Охватываемые компоненты
1.	Консультирование пользователей РНИС СО, а также обеспечение наполнения и актуализации РНИС СО в соответствии с поступившими в адрес СТП Исполнителя заявками	Все компоненты РНИС СО
2.	Плановое и внеплановое техническое обслуживание РНИС СО	
3.	Восстановление работоспособности РНИС СО при возникновении или обнаружении программных сбоев, дефектов, ошибок и иных инцидентов, выявленных в процессе эксплуатации	
4.	Техническое обслуживание ОПО	
5.	Резервное копирование и проверка целостности резервных копий РНИС СО	
6.	Мониторинг доступности и работоспособности (производительности) РНИС СО	

2.3. Требования к услугам консультирования пользователей РНИС СО, а также обеспечения наполнения и актуализации РНИС СО в соответствии с поступившими в адрес СТП Исполнителя заявками.

В процессе оказания услуг Исполнитель должен обеспечить выполнение следующих операций:

- консультирование Государственного заказчика и пользователей по вопросам эксплуатации РНИС СО;
- подготовка и предоставление инструкций пользователям по функционалу РНИС СО;
- наполнение РНИС СО, включая заведение и обновление маршрутной сети, формирование и корректировку расписаний движения транспортных средств, а также занесение справочных значений.

2.4. Требования к услугам по плановому и внеплановому техническому обслуживанию РНИС СО.

В процессе оказания услуг Исполнитель должен выполнять операции, указанные в таблице 2.2.

Таблица 2.2 – Перечень операций по плановому и внеплановому обслуживанию

№ п/п	Перечень операций	Периодичность
Плановые		
1.	Проверка корректности функционирования основных пользовательских сценариев РНИС СО	ежемесячно
2.	Проверка корректности работы функций экспорта и формирования отчетных данных РНИС СО	
3.	Проверка корректности функционирования механизмов обмена данными в рамках действующих интеграционных	

	взаимодействий РНИС СО	
Внеплановые		
4.	Изменение параметров РНИС СО	На основании заявок, зарегистрированных в СТП, в соответствии со сроками, установленными таблицей 3.6
5.	Корректировка и выгрузка данных, непредусмотренных для изменения и выгрузки через интерфейс РНИС СО	
6.	Выполнение обновлений компонентов РНИС СО	
7.	Организация новых интеграционных взаимодействий РНИС СО в соответствии с протоколом API РНИС СО, а также восстановление ранее созданных интеграционных взаимодействий с подсистемами, внешними информационными системами, сервисами передачи данных и источниками информации.	

Плановые работы, предусмотренные таблицей 2.2, выполняются Исполнителем ежемесячно, начиная с даты начала оказания услуг.

Исполнитель обязан предварительно согласовать с Государственным заказчиком даты и время проведения плановых работ за два рабочих дня до их проведения. При определении сроков проведения работ Исполнитель должен учитывать необходимость обеспечения непрерывности функционирования РНИС СО и минимизации влияния выполняемых операций на ее работу.

По завершении плановых работ Исполнитель обязан зафиксировать в СТП сведения о результатах проведенных проверок и выявленных замечаниях. При выявлении неисправностей Исполнитель обязан уведомить об этом Государственного заказчика посредством СТП и согласовать дальнейшие действия по их устранению.

2.5. Требования к услугам по восстановлению работоспособности РНИС СО при возникновении или обнаружении программных сбоев, дефектов, ошибок и иных инцидентов, выявленных в процессе эксплуатации.

Исполнитель должен обеспечить устранение инцидентов (критических и не критических дефектов), возникших в процессе эксплуатации РНИС СО, не позволяющих использовать функции РНИС СО в соответствии с эксплуатационной документацией.

Решение инцидентов, возникающих в процессе работы РНИС СО, производится в следующих ситуациях:

- в случае возникновения аварийных ситуаций, сбоев или программных дефектов в РНИС СО (контрольные сроки обработки обращений определены в Таблице 3.6);
- в случае сбоев и аварий в аппаратном обеспечении серверов и в средствах виртуализации, восстановление работоспособности РНИС СО.

Решение инцидента заключается:

- в анализе причин возникновения сбоев и аварий в функционировании РНИС СО;
- в устранении причин нарушения функционирования РНИС СО, включая восстановление данных, конфигурационных и исполняемых файлов РНИС СО и ОПО из резервной копии, а также исправление дефектов в коде РНИС СО.

В случае возникновения нарушения работоспособности продуктивного стенда РНИС СО, вследствие которого необходимо восстановление данных из резервных копий, Исполнитель должен обеспечить восстановление информации продуктивного стенда РНИС СО из резервной копии, предоставленной Государственным заказчиком по запросу Исполнителя. Восстановление данных из резервной копии должно производиться в сроки, соответствующие приоритету инцидента.

В случае устранения дефектов в РНИС СО, Исполнитель должен:

- при необходимости провести актуализацию документации (Инструкции, Руководства) на РНИС СО;
- предоставить обновленную документацию на РНИС СО в срок не позднее 7 (семи) рабочих дней со дня устранения дефекта.

2.6. Требования к оказанию услуг по техническому обслуживанию ОПО.

Исполнитель в рамках оказания услуг по техническому обслуживанию ОПО должен:

- выполнять техническое обслуживание ОПО в соответствии с перечнем, указанным в Таблице 2.3;
- обеспечивать развертывание ОПО и настройку его компонентов при вводе в эксплуатацию дополнительных виртуальных или физических серверов в центре обработки данных

(ЦОД) Государственного заказчика, необходимых для обеспечения стабильного функционирования РНИС СО, в соответствии с перечнем операций, установленным таблицей 2.3, и в сроки, предусмотренные таблицей 3.10.

Таблица 2.3 – Перечень операций по техническому обслуживанию ОПО

№ п/п	Перечень операций
1.	Контроль и выполнение обновления ОПО
2.	Изменение настроек операционной системы
3.	Развертывание и изменение настроек СУБД
4.	Развертывание и изменение настроек сервера приложений

2.7. Требования к резервному копированию и проверке целостности резервных копий РНИС СО.

Исполнитель в рамках оказания услуг настраивает и обеспечивает выполнение операций по резервному копированию РНИС СО на хранилище (S3, FTP, NFS-сервер), предоставленное Государственным заказчиком и доступное Исполнителю, в объеме, определенном таблицей 2.4, и с периодичностью, установленной таблицей 3.9 настоящего технического задания. Резервные копии предназначены для восстановления работоспособности РНИС СО в случае сбоев.

Исполнитель самостоятельно осуществляет проверку целостности резервных копий средствами используемого программного обеспечения резервного копирования с периодичностью, установленной таблицей 3.9 настоящего технического задания. Результаты проверок фиксируются в журналах или отчетах указанного программного обеспечения с указанием даты и времени проверки, проверенной резервной копии и результата проверки.

В случае сбоя Исполнитель самостоятельно использует созданные резервные копии для восстановления работоспособности РНИС СО.

Таблица 2.4 – Виды операций резервного копирования РНИС СО

№ п/п	Виды операций	
1.	Резервное копирование базы данных с нормативно-справочной информацией и бизнес-сущностями системы	Полное резервное копирование всех серверов, входящих в состав РНИС СО (альтернативный способ)
2.	Резервное копирование конфигурации системы (etcd)	
3.	Резервное копирование файлового хранилища (отчеты, загрузки пользователей)	
4.	Проверка целостности резервных копий РНИС СО	

В качестве альтернативы резервному копированию отдельных компонентов системы допускается полное резервное копирование всех серверов, входящих в состав РНИС СО.

2.8. Требования к оказанию услуг по мониторингу доступности и работоспособности (производительности) РНИС СО.

Услуги по мониторингу доступности и работоспособности (производительности) РНИС СО должны оказываться непрерывно с даты начала оказания услуг в соответствии с требованиями, указанными в Таблице 3.2.

В рамках оказания услуг по мониторингу и обеспечению доступности и работоспособности (производительности) РНИС СО Исполнитель обязан:

- осуществлять мониторинг доступности и работоспособности (производительности) РНИС СО;

- выявлять события, способные привести к нарушению доступности или работоспособности (производительности) РНИС СО, принимать меры по предупреждению инцидентов на основании данных мониторинга, а также предоставлять Государственному заказчику рекомендации по предотвращению возникновения инцидентов и наращиванию вычислительных ресурсов с учетом изменения профиля нагрузки;

- обеспечить режим работы (доступность) РНИС СО в соответствии с требованиями, указанными в Таблице 3.11.

Для обеспечения доступности и работоспособности (производительности) Исполнителем должен осуществляться мониторинг РНИС СО с использованием системы мониторинга. Порядок

предоставления и первоначальной настройки определен ниже (Таблица 2.5).

Таблица 2.5 – Порядок начальной настройки сервера мониторинга

№ п/п	Операции	Ответственный
1.	Установка ПО сервера мониторинга	Исполнитель
2.	Установка и настройка ОПО сервера мониторинга	Исполнитель
3.	Настройка параметров ПО сервера мониторинга	Исполнитель
4.	Предоставление вычислительных мощностей для размещения сервера мониторинга	Государственный заказчик

Система мониторинга должна обеспечивать контроль следующих параметров РНИС СО и ОПО:

- загрузка вычислительных ресурсов серверов, включая процессор (CPU), оперативную память (RAM) и дисковое пространство (HDD);
- доступность подсистем РНИС СО;
- внутрисистемные метрики РНИС СО и ОПО.

При срабатывании системы мониторинга Исполнитель обязан в течение 8 часов с момента получения соответствующего уведомления системы мониторинга уведомить Государственного заказчика посредством СТП или иных согласованных Сторонами средств коммуникации. Уведомление должно содержать информацию о выявленном событии, его возможном влиянии на доступность и работоспособность (производительность) РНИС СО, а также рекомендации по предупреждению возникновения аналогичных неполадок в дальнейшем.

2.9. Требования к обеспечению отказоустойчивости РНИС СО.

Исполнитель в рамках оказания услуг по технической поддержке РНИС СО должен выполнять следующие требования для обеспечения ее отказоустойчивости:

- осуществлять контроль работоспособности всех компонентов отказоустойчивого кластера РНИС СО;
- своевременно выявлять и фиксировать сбои и нарушения в работе компонентов отказоустойчивого кластера РНИС СО;
- анализировать причины возникновения сбоев и нарушений в работе компонентов отказоустойчивого кластера РНИС СО и принимать меры по их устранению;
- актуализировать эксплуатационную документацию на РНИС СО в части изменений, внесенных в ходе оказания услуг.

При выявлении сбоев и нарушений в работе компонентов отказоустойчивого кластера РНИС СО Исполнитель обязан в течение 8 часов с момента выявления соответствующего события уведомить Государственного заказчика посредством СТП или иных согласованных Сторонами средств коммуникации. Уведомление должно содержать информацию о выявленном сбое или нарушении, его возможном влиянии на доступность и работоспособность РНИС СО, а также сведения о принимаемых мерах по устранению и рекомендации по предупреждению возникновения аналогичных сбоев и нарушений в дальнейшем.

2.10. Требования к конфиденциальности.

Исполнитель не должен разглашать и использовать информацию, которая может стать ему известной в ходе оказания услуг. Исполнитель несет ответственность за соблюдение этого требования в соответствии с законодательством Российской Федерации.

Исполнитель обязан использовать доступ к информационным ресурсам Государственного заказчика только в целях оказания услуг, не копировать, не размножать и не распространять в любой форме любые материалы, содержащиеся на рабочих местах, серверах и прочих средствах хранения информации Государственного заказчика.

2.11. Требования к организационному обеспечению.

Не позднее 3 (трех) рабочих дней с даты заключения Контракта Государственный заказчик направляет Исполнителю контактные данные Ответственного представителя Государственного заказчика, Исполнитель направляет Государственному заказчику контактные данные Ответственного представителя Исполнителя, курирующих оказание услуг, для решения вопросов, возникающих в период оказания услуг.

2.12. Требования к актуализации эксплуатационную документацию на РНИС СО.

При внесении изменений или обновлении РНИС СО Исполнитель обязан обеспечить

актуализацию эксплуатационной документации в части, затронутой соответствующими изменениями.

Актуализация эксплуатационной документации должна выполняться:

- в составе текстовых документов;
- во встроенных пользовательских интерфейсах Системы.

Перечень документации, подлежащей обязательной актуализации:

- Руководство пользователя;
- Руководство администратора.

Исполнитель обязан обеспечить соответствие актуализированной документации фактической функциональности и настройкам РНИС СО. Актуализация должна быть завершена и актуализированная документация предоставлена Государственному заказчику не позднее 7 (семи) рабочих дней с даты ввода соответствующих изменений в эксплуатацию.

Предоставление актуализированной документации осуществляется посредством СТП или иным согласованным Сторонами способом. Если изменения не затрагивают содержание соответствующего документа, его актуализация не требуется.

2.13. Перечень документов, на основании и в соответствии с которыми происходит оказание услуг:

- Приказ Министерства транспорта и дорожного хозяйства Сахалинской области от 19.01.2024 № 1-3.09-30/24 «О государственной информационной системе Сахалинской области «Региональная навигационно-информационная система Сахалинской области»;
- Приказ Минцифры России от 17 декабря 2020 № 715 «Об утверждении типовых условий контрактов на выполнение работ по созданию и (или) развитию (модернизации) государственных (муниципальных) и (или) иных информационных систем»;
- Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 14 февраля 2009 № 22-ФЗ «О навигационной деятельности»;
- Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27 декабря 2002 № 184-ФЗ «О техническом регулировании»;
- Постановление Правительства РФ от 6 июля 2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;
- Указ Президента Российской Федерации от 31 марта 2010 № 403 «О создании комплексной системы обеспечения безопасности населения на транспорте»;
- Указ Президента Российской Федерации от 17 мая 2007 № 638 «Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации»;
- Указ Президента Российской Федерации от 6 марта 1997 № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Постановление Правительства РФ от 01 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 24 октября 2011 № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)»;
- Постановление Правительства Российской Федерации от 31 декабря 2021 № 2607 «Об утверждении Правил оказания телематических услуг связи»;
- Постановление Правительства Российской Федерации от 16 ноября 2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;
- Постановление Правительства Российской Федерации от 25 августа 2008 № 641 «Об оснащении транспортных, технических средств и систем аппаратурой спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS»;
- Методические документы в области выполнения работ по созданию системы защиты информации и аттестации информационных систем, разрабатываемые и утверждаемые

ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 № 1085;

- Приказ ФСТЭК России от 11 апреля 2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

- Приказ Федеральной службы безопасности Российской Федерации от 22.08.2026 № 321 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5-1 статьи 13 Федерального закона от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с использованием шифровальных (криптографических) средств»;

- Приказ ФСТЭК России от 18 февраля 2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСБ России от 10 июля 2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Федеральный закон от 30 апреля 1999 № 81-ФЗ «Кодекс торгового мореплавания Российской Федерации»;

- Федеральный закон от 7 марта 2001 № 24-ФЗ «Кодекс внутреннего водного транспорта Российской Федерации»;

Комплекс стандартов на автоматизированные системы:

- ГОСТ 54023-2010 «Система навигационного диспетчерского контроля выполнения государственного заказа на содержание федеральных автомобильных дорог. Назначение, состав и характеристики подсистемы картографического обеспечения»;

- ГОСТ Р 59793-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

- ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов»;

- ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

- ГОСТ Р 59792-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем»;

- ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;

- ГОСТ 34.602-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

- ГОСТ Р 2.531-2023 «Единая система конструкторской документации. Электронная конструкторская документация. Виды преобразований»;

- ГОСТ Р 54593-2011 Национальный стандарт РФ. «Информационные технологии. Свободное программное обеспечение. Общие положения»;

- ГОСТ Р 2.105-2019 «Единая система конструкторской документации (ЕСКД). Общие требования к текстовым документам»;

- ГОСТ Р ИСО/МЭК 12207-2010. «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств»;

- ГОСТ Р ИСО/МЭК 14764-2002 «Информационная технология. Сопровождение программных средств»;

- ГОСТ Р ИСО/МЭК 15271-2002 «Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)»;
- ГОСТ Р ИСО/МЭК 15026-2002 «Информационная технология (ИТ). Уровни целостности систем и программных средств»;
- ГОСТ Р 52870-2007 Национальный стандарт РФ. «Средства отображения информации коллективного пользования. Требования к визуальному отображению информации и способы измерения»;
- ГОСТ Р 57193-2025 «Национальный стандарт Российской Федерации. Системная и программная инженерия. Процессы жизненного цикла систем»: утвержден и введен в действие Приказом Росстандарта от 25.03.2025 № 212-ст;
- ГОСТ Р О 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».

3. РЕЖИМЫ ОКАЗАНИЯ УСЛУГ И ФУНКЦИИ СТП

3.1. Функции СТП.

Распределение функций/задач между СТП Исполнителя и СТП Заказчика должно осуществляться в соответствии с установленными требованиями (см. Таблица 3.1).

Таблица 3.1 – Распределение ответственности за выполнение функции СТП

№ п/п	Функция (задача) СТП	Ответственный за выполнение
1.	Прием обращений от пользователей, направление в СТП Исполнителя	СТП Заказчика
2.	Регистрация обращений	СТП Исполнителя
3.	Классификация обращений	
4.	Исполнение обращений	
5.	Отправка ответов пользователям	СТП Заказчика
6.	Выполнение операций	СТП Исполнителя
7.	Выполнение регулярных работ	
8.	Обеспечение доступности РНИС СО	
9.	Обеспечение работоспособности (производительности) РНИС СО	

3.2. Режим оказания услуг СТП.

Предоставление функций СТП должно осуществляться в соответствии с режимом оказания услуг и рабочим временем (Таблица 3.2).

Таблица 3.2 – Режимы доступности функций СТП

№ п/п	Функция (задача) СТП	Режим доступности функции	Время доступности функции*
1.	Прием обращений	9xD	09:00 до 18:00 без перерыва на обед
2.	Регистрация обращений	9xD	
3.	Классификация обращений	9xD	09:00 до 18:00 без перерыва на обед
4.	Отправка ответов СТП Заказчика		
5.	Исполнение обращений		
6.	Выполнение операций		
7.	Выполнение регулярных работ	24x7	По согласованию
8.	Обеспечение доступности РНИС СО		-
9.	Обеспечение работоспособности (производительности) РНИС СО		

* Указано местное время Заказчика (10-я часовая зона (МСК+8, московское время плюс 8 часов,

UTC+11), Сахалинская область) в соответствии с п. 10 ч. 1 ст. 5 Федерального закона от 03.06.2011 № 107-ФЗ «Об исчислении времени».

3.3. Порядок обработки обращений в СТП.

Таблица 3.3 – Порядок работы с обращениями в рамках функций СТП Исполнителя

№ п/п	Функция (задача) СТП	Порядок
1.	Прием обращений	Прием обращений осуществляется в соответствии с режимом доступности функций СТП (Таблица 3.2). Для обращений, полученных в выходные и праздничные дни или в нерабочее время, отсчет времени по обработке обращения производится со следующего рабочего дня после получения обращения в соответствии с режимом доступности функций СТП (Таблица 3.2).
2.	Регистрация обращений	В рамках регистрации обращения осуществляется: – информирование Инициатора обращения о номере обращения, зарегистрированном в системе учета обращений Исполнителя (система учета обращений Исполнителя может осуществлять автоматическое присвоение номера обращению и информирование Инициатора обращения о его регистрации); – первичная классификация обращения в соответствии с типом работ и типом обращения (Таблица 3.6). Регистрации подлежат все обращения пользователей в СТП.
3.	Классификация обращения	В рамках классификации обращения осуществляется проверка и окончательное определение: – типа обращения (Таблица 3.6); – выполняемой операции (Таблица 3.6); – приоритета Инцидента (Таблица 3.4); – контрольного срока обработки (Таблица 3.6). Ответственный за выполнение функции производит информирование Инициатора обращения об ориентировочных сроках решения обращения (Таблица 3.6).
4.	Исполнение обращений	В рамках функции СТП по исполнению обращений производится: – подтверждение правильности классификации обращения; – назначение специалиста ответственного за обработку обращения; – получение дополнительной информации от Инициатора обращения; – отражение в заявке детальной информации о порядке решения обращения и взаимодействии с Инициатором обращения; – приостановка и возобновление выполнения обращений при необходимости направления уточняющих вопросов инициатору обращения; – установка статуса «Выполнено» для выполненных операций. Выполнение операции должно начаться в течение времени реакции соответствующего обращения (Таблица 3.6). В процессе исполнения обращения может потребоваться дополнительная информация или действия инициатора обращения, необходимые для решения обращения – на период запроса указанных данных исполнение обращения приостанавливается: статус обработки обращения может быть изменен на «Приостановлено» (Таблица 3.7). Время, в течение которого обращение находится в статусе «Приостановлено» не входит в длительность решения обращения. В случае если заявка находится в статусе «Приостановлено» по причине отсутствия реакции Инициатора обращения более 20 дней, такая заявка переводится в статус «Закрыто».

5.	Выполнение операций	В рамках функции СТП по выполнению операций осуществляется: – устранение Инцидентов (тип обращения «Инцидент») в соответствии с установленным приоритетом и контрольными сроками (Таблица 3.6); – выполнение Обслуживания (тип обращения «Обслуживание») в соответствии с контрольными сроками (Таблица 3.6).
		В процессе обработки обращения типа «Инцидент» может быть выявлен дефект (ошибка в программном коде) в РНИС СО. Устранение дефектов производится в соответствии с контрольными сроками обработки обращений (Таблица 3.6). При этом устранение дефектов, попадающих под действующие гарантийные обязательства по любому Государственному контракту на создание и развитие РНИС СО в рамках услуг по технической поддержке РНИС СО не производится.
		В процессе обработки обращения может потребоваться дополнительная информация или действия инициатора обращения, необходимые для решения обращения – на период запроса указанных данных обработка обращения приостанавливается: статус обработки обращения может быть изменен на «Приостановлено» в соответствии с Таблица 3.7.
		Время, в течение которого обращение находится в статусе «Приостановлено» не входит в длительность решения обращения.
		В случае если заявка находится в статусе «Приостановлено» по причине отсутствия реакции Инициатора обращения более 20 дней, такая заявка переводится в статус «Закрыто».
		Перевод обращения в статус «Выполнено» после окончания выполнения работ по заявке осуществляет СТП Исполнителя.
6.	Выполнение регулярных работ	В рамках функции СТП по выполнению регулярных работ осуществляются операции, предусмотренные Таблицей 3.8.
		Периодичность проведения регулярных работ должна соответствовать требованиям по периодичности работ (Таблица 3.9, Таблица 3.10).
7.	Обеспечение доступности РНИС СО	В рамках функции СТП по обеспечению доступности РНИС СО осуществляется мониторинг доступности РНИС СО.
		По фактам нарушения доступности РНИС СО, обнаруженным Системой мониторинга РНИС СО, ответственный за выполнение функций СТП Исполнителя должен зарегистрировать обращение типа «инцидент» в течение 30-ти минут после выявления факта недоступности Системой мониторинга РНИС СО.
		Назначение приоритета инциденту осуществляется ответственным за выполнение функции в соответствии с установленными приоритетами (Таблица 3.4).
8.	Обеспечение работоспособности РНИС СО	Устранение обнаруженного инцидента осуществляется в соответствии с контрольными сроками (Таблица 3.6).
		В рамках функции СТП по обеспечению работоспособности РНИС СО осуществляется мониторинг работоспособности (производительности) РНИС СО.
		По фактам нарушения работоспособности (производительности) РНИС СО, обнаруженным Системой мониторинга РНИС СО, ответственный за выполнение функций СТП должен: - Зарегистрировать обращение типа «инцидент» в течение 30-ти минут после выявления факта нарушения работоспособности (производительности) Системой мониторинга РНИС СО; - Оповестить ответственного представителя Государственного заказчика в течение 30-ти минут после выявления факта нарушения работоспособности (производительности) Системой мониторинга РНИС СО.

		Назначение приоритета инциденту осуществляется ответственным за выполнение функции в соответствии с установленными приоритетами (Таблица 3.4).
		Устранение обнаруженного инцидента осуществляется в соответствии с контрольными сроками обработки обращений (Таблица 3.6).

3.4. Приоритеты обработки инцидентов/заявок на дефекты.
При регистрации обращений ответственный за выполнение функции СТП назначает приоритет в зависимости от влияния отказа или сбоя на функционирование РНИС СО (Таблица 3.4).

Таблица 3.4 – Приоритеты инцидентов

№ п/п	Приоритет	Описание
1.	Критичный	- полная недоступность РНИС СО; - полная недоступность подсистемы РНИС СО; - ошибки/сбои, которые приводят к полной неработоспособности всех функций РНИС СО.
2.	Высокий	- ошибки/сбои, которые приводят к частичному нарушению работоспособности или недоступности функций РНИС СО; - снижение быстродействия РНИС СО (время отклика РНИС СО на операции превышает 2 минуты); - невозможность информационного обмена с РНИС СО для внешних ИС; - невозможность управления правами и ролями пользователей; - недоступность формирования отчетов.
3.	Стандартный	- отклонение в работе РНИС СО, не влияющее на корректную работу функционала; - другие сбои и ошибки, затрагивающие основной функционал РНИС СО.

	3.5. Ответственность за устранение инцидентов. Ответственность за устранение возникших инцидентов устанавливается в соответствии с зонами ответственности, приведенными ниже (Таблица 3.5).
--	--

Таблица 3.5 – Зоны ответственности при устранении инцидентов

Тип аварии или инцидента	Причины возникновения аварии или инцидента	Способ устранения	Ответственный за устранение
Аппаратно-программный сбой	Отказы: - серверного оборудования; - систем хранения данных; - сетевого оборудования; - каналов передачи данных; - систем электропитания; - системы управления виртуализацией.	- ремонт и восстановление оборудования; - восстановление каналов передачи данных; - ремонт и восстановление инженерных систем; - восстановление производительности и работоспособности СХД и средств виртуализации.	Государственный заказчик
Аппаратно-программный сбой	Отказы: - серверного оборудования; - систем хранения данных; - сетевого оборудования; - каналов передачи данных; - систем электропитания;	- полное восстановление ОПО и РНИС СО (включая настройки); - полное восстановление ОПО и РНИС СО из резервных копий (включая настройки); - восстановление данных из резервных копий.	СТП Исполнителя

	- системы управления виртуализацией.		
Программный сбой	Сбой на уровне ОПО или РНИС СО	- восстановление настроек ОПО и РНИС СО; - установка обновлений безопасности ОПО и РНИС СО; - установка обновлений ОПО.	СТП Исполнителя
Программный сбой	Программные дефекты, связанные с оказанием услуг по текущему контракту	– внесение изменений в программный код и настройки РНИС СО; – установка обновлений РНИС СО.	СТП Исполнителя

3.6. Контрольные сроки решения (выполнения) обращений.

СТП Исполнителя должна производить обработку обращений в соответствии с контрольными сроками, указанными ниже (Таблица 3.6)

Таблица 3.6 – Контрольные сроки обработки обращений

Тип обращения	Тип работ	Операции	Приоритет	T1 (рабочих часов)	T2 (рабочих часов)
Обслуживание	Запрос на консультирование и наполнение РНИС СО	Консультирование Инициатора обращения либо Государственного заказчика по вопросам использования функций и эксплуатации РНИС СО	-	0,5	4
		Подготовка и предоставление инструкций пользователям по функционалу РНИС СО	-	0,5	9
		Наполнение и актуализация учетов РНИС СО, включая заведение и обновление маршрутной сети, формирование и корректировку расписаний движения транспортных средств, а также занесение справочных значений.	-	0,5	9
	Запрос на внеплановое обслуживание РНИС СО	Изменение параметров РНИС СО	-	0,5	4
		Корректировка и выгрузка данных, непредусмотренных для изменения и выгрузки через интерфейс РНИС СО	-	0,5	4
		Выполнение обновлений компонентов РНИС СО	-	12	По согласованию

		Организация новых интеграционных взаимодействий РНИС СО в соответствии с протоколом API РНИС СО, а также восстановление ранее созданных интеграционных взаимодействий с подсистемами, внешними информационными системами, сервисами передачи данных и источниками информации.	-	1	18
Инцидент	Устранение инцидентов	Восстановление работоспособности РНИС СО	Критичный	1	6
			Высокий		9
			Стандартный		18

3.6.1. Статусы обработки Обращений.

В процессе обработки обращение может принимать соответствующий статус обработки. Статусы обработки обращений описаны в Таблице 3.7.

Таблица 3.7 – Статусы обработки обращений

№ п/п	Наименование статуса	Описание
1.	Создана	Обращение с присвоенным номером.
2.	В работе	Обращение принято, действия по сути выполнения обращения уже начаты.
3.	Приостановлено	Данных, полученных от Инициатора обращения, недостаточно для анализа проблемы, Инициатору обращения направлены уточняющие вопросы. Работы по обращению приостановлены. Со стороны Инициатора обращения требуются дополнительные действия/информация. Обращение должно быть автоматически закрыто, если находится в этом статусе более 20 дней. Срок действия приостановки не учитывается в общем сроке обработки обращения.
4.	Выполнено	Обращение выполнено с возможными резолюциями: 1) Решено - решение предоставлено Инициатору обращения; 2) Не воспроизводится – с поясняющим ответом Инициатору обращения: - Ошибка пользователя – не является дефектом РНИС СО; - Инфраструктура – проблема не связана с ПО или с ошибкой пользователя. Инициатор обращения в течение двух рабочих дней подтверждает выполнение работ либо сообщает о наличии мотивированных замечаний к результатам решения заявки. В случае получения замечаний по исполнению заявки сотрудник СТП Исполнителя исправляет выявленные замечания и повторно посылает запрос на подтверждение исполнения заявки. При отсутствии от

		инициатора заявки мотивированного отказа или подтверждения ее выполнения в течение 5 (пяти) рабочих дней, обращение будет считаться выполненным. Если в течение 10 дней после перевода обращения в статус «Решено» Инициатор обращения не подтвердил его решение, сотрудник СТП Заказчика обязан перевести данное обращение в статус «Закрето».
--	--	---

3.6.2. Порядок регистрации обращений.

При обращении в СТП Исполнителя Инициатором обращения указывается, в том числе, следующая информация:

- описание шагов, в результате выполнения которых произошла ошибка/ проблема;
- снимки экрана с сообщением об ошибке (при наличии);
- ссылки на неработающие экранные формы/объекты справочников;
- информация о причинах смены приоритета (при наличии).

В целях уточнения информации, необходимой для обработки обращения, сотрудник СТП Исполнителя может перевести обращение в статус «Приостановлено» и вернуть его в работу после получения необходимых сведений.

3.6.3. Порядок выполнения регулярных работ.

Регулярные работы выполняются в соответствии с установленными требованиями (Таблица 3.8).

Таблица 3.8 – Порядок выполнения регулярных работ

№ п/п	Типы работ	Периодичность
1.	Резервное копирование и проверка целостности резервных копий РНИС СО	В соответствии с установленными требованиями (Таблица 3.9)
2.	Техническое обслуживание ОПО	В соответствии с установленными требованиями (Таблица 3.10)

В рамках выполнения работ по резервному копированию ответственный за выполнение функции (задачи) СТП должен выполнять установленный перечень операций (Таблица 3.9). Применяемые методы резервного копирования: полное, разностное и инкрементальное.

Таблица 3.9 – Перечень операций и периодичность резервного копирования РНИС СО

СО

№ п/п	Виды операций		Периодичность выполнения
1.	Резервное копирование базы данных с нормативно-справочной информацией и бизнес-сущностями системы	Полное резервное копирование всех серверов, входящих в состав РНИС СО (альтернативный способ)	Ежедневно — создание инкрементных резервных копий с хранением резервных копий за два последних календарных дня.
2.	Резервное копирование конфигурации системы (etcd)		Еженедельно, каждую субботу — создание полной резервной копии с хранением одной последней еженедельной копии.
3.	Резервное копирование файлового хранилища (отчеты, загрузки пользователей)		Ежемесячно, в первую субботу месяца — создание полной резервной копии с хранением одной последней ежемесячной копии.
4.	Проверка целостности резервных копий РНИС СО		После каждого создания полной резервной копии.

В рамках выполнения работ по обслуживанию ОПО ответственный за выполнение функции (задачи) СТП должен выполнять установленный перечень операций (Таблица 3.10).

Таблица 3.10 – Перечень операций по техническому обслуживанию ОПО

№ п/п	Перечень операций	Сроки и периодичность выполнения
1.	Контроль и выполнение обновления ОПО	Контроль наличия обновлений — не реже 1 раза в месяц. При обнаружении обновлений Исполнитель обязан уведомить Заказчика посредством СТП Исполнителя с указанием сведений о доступных обновлениях. Установка обновлений осуществляется после согласования с Заказчиком в срок не более 5 рабочих дней с даты согласования, если иной срок не установлен Заказчиком.
2.	Изменение настроек операционной системы	При первоначальной настройке или по необходимости. Осуществляется по запросу Заказчика в срок не более 5 рабочих дней с даты регистрации запроса в СТП Исполнителя, если иной срок не согласован сторонами.
3.	Развертывание и изменение настроек СУБД	При первоначальной настройке или по необходимости. Осуществляется по запросу Заказчика в срок не более 5 рабочих дней с даты регистрации запроса в СТП Исполнителя, если иной срок не согласован сторонами.
4.	Развертывание и изменение настроек сервера приложений	При первоначальной настройке или по необходимости. Осуществляется по запросу Заказчика в срок не более 5 рабочих дней с даты регистрации запроса в СТП Исполнителя, если иной срок не согласован сторонами.

3.7. Режим работы РНИС СО.

СТП Исполнителя должна обеспечить режим работы (доступность) РНИС СО в соответствии с установленными параметрами (Таблица 3.11).

Таблица 3.11 – Режимы работы (доступность) РНИС СО

№ п/п	Параметр	Значение
1.	Режим работы РНИС СО	24x7
2.	Разрешенные дни проведения плановых регламентных работ	Вторник – Четверг или по согласованию с СТП Заказчика
3.	Проведение внеплановых регулярных работ	Обязательное согласование за 50 минут до начала проведения работ
4.	Проведение плановых регламентных работ	В соответствии с Перечнем операций по обслуживанию ОПО и РНИС СО
5.	Общее (суммарное) время проведения плановых регламентных работ (в месяц)	Не более 8 часов
6.	Общее (суммарное) время недоступности РНИС СО, в месяц, измеряемое в часах (не регламентные задержки)	Не более 4 часа

3.8. Требования к Исполнителю по защите информации в ГИС/МИС.**3.8.1. Общие требования к защите информации.**

Государственная информационная система «Региональная навигационно-информационная система Сахалинской области» (далее – ГИС «РНИС СО», ИС) содержит сведения ограниченного доступа (информацию, подлежащую защите в соответствии с требованиями законодательства Российской Федерации). Обработка информации, содержащей сведения, составляющие государственную тайну, в компонентах ГИС «РНИС СО» не осуществляется.

Применяемые технологии в программно-технических средствах компонентов информационной системы и интегрированных с ней систем (далее – Компоненты ИС) должны соответствовать требованиям к государственным (муниципальным) информационным системам Российской Федерации, для которых необходимо обеспечить 3 класс защищенности

государственных информационных систем и требованиям, предъявляемым к информационным системам персональных данных, для которых необходимо обеспечить 3 уровень защищенности, в соответствии с приказом ФСТЭК России от 11.04.2025 № 117.

3.8.2. Требования к надёжности.

Компоненты ИС должны сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

- при сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке операционной системы, восстановление программы должно происходить после перезапуска операционной системы и автоматического запуска исполняемого файла Компонентов ИС;

- при ошибках в работе аппаратных средств (кроме носителей, данных и программ) восстановление функции Компонентов ИС возлагается на Государственного заказчика;

- при ошибках, связанных с системным программным обеспечением, а именно, операционной системой и драйверами устройств, восстановление работоспособности возлагается на Государственного заказчика.

Для защиты аппаратуры от бросков напряжения и коммутационных помех применяются сетевые фильтры.

Исполнителем должны быть предусмотрены программные средства резервного копирования и восстановления информации, позволяющие осуществлять резервное копирование и восстановление информации, как в автоматическом, так и ручном режимах. Сохранение и восстановление информации должно быть обеспечено средствами применяемой вычислительной техники и специализированными программными средствами.

Требования к надёжности компонентов ИС устанавливаются в соответствии с ГОСТ 24.701-86. «Единая система стандартов автоматизированных систем управления. Надёжность автоматизированных систем управления. Основные положения» и ГОСТ Р МЭК 62628-2021. «Национальный стандарт Российской Федерации. Надёжность в технике. Руководство по обеспечению надёжности программного обеспечения».

3.8.3. Требования к защите информации от несанкционированного доступа.

Компоненты ИС должны соответствовать, но не ограничиваться, требованиям, предъявляемым к ИС по обеспечению защиты данных от несанкционированного доступа в следующем объеме:

- аутентификация пользователей при доступе к рабочей станции должна осуществляться средствами операционной системы;

- аутентификация пользователей в ресурсах ИС должна осуществляться с использованием индивидуального пароля пользователя;

- привилегированный доступ должен осуществляться с применением строгой аутентификации, а в случае технической невозможности применения строгой аутентификации - с использованием усиленной многофакторной аутентификации.

Разграничение доступа пользователей к функциям ИС:

- доступ пользователей к функционалу ИС должен реализовываться администратором в соответствии с эксплуатационной документацией;

- вход в пользовательскую часть ИС и дальнейшая работа должна осуществляться только при указании имени пользователя и его пароля;

- для паролей пользователей (в т.ч. привилегированных) и технологических учетных записей должны быть предустановлены требования длины пароля: для пользователей – не менее 12 символов; для привилегированных пользователей – не менее 12 символов; для технологических учетных записей – не менее 16 символов. Для паролей должны быть реализованы механизмы проверки сложности и повторяемости, использования специальных символов, строчных и заглавных букв;

- для каждого пользователя должна быть предусмотрена возможность назначения одной или более ролей, которые этот пользователь выполняет в ИС.

В ИС должна быть реализована поддержка актуального списка пользовательских ролей.

Для целей защиты данных сервера БД от несанкционированного доступа конечные пользователи ИС не должны знать пароль доступа непосредственно к самому серверу БД.

Компоненты ИС должны осуществлять регистрацию и учет следующих событий: регистрация входа/выхода пользователя в/из ИС (параметры регистрации: дата и время события;

результат попытки входа (успешная/неуспешная); имя или идентификатор пользователя, предъявленный при попытке доступа).

Компоненты ИС должны обеспечивать протоколирование и сохранение сведений о предоставлении доступа и о других операциях с документами и метаданными в автоматизированном режиме, а также автоматизированное ведение электронных журналов учета точного времени и фактов размещения, изменения и удаления информации, содержания вносимых изменений.

3.8.4. Требования по сохранности информации.

Решения по защите данных при авариях и сбоях в электропитании должны обеспечить уровень защиты, определяемый принятой политикой информационной безопасности, профилями защиты и соответствовать категории защищаемых информационных активов, вероятности угрозы и степени возможного влияния факторов воздействия с учетом установленной категории риска и стоимости защиты.

Компоненты ИС должны обеспечивать хранение документации в форме электронных документов, предусматривая резервное копирование документации в форме электронных документов и метаданных, восстановление документации в форме электронных документов и метаданных из резервных копий.

3.8.5. Требования к совместимости со средствами защиты информации.

Исполнителем должна обеспечиваться полная совместимость компонентов ИС с применяемыми для ее защиты средствами от НСД и средствами антивирусной защиты.

3.8.6. Требования к безопасности программного обеспечения.

При доработке/разработке функциональных возможностей компонентов ИС должны применяться положения «ГОСТ Р 56939-2024. Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования» (утв. и введен в действие Приказом Росстандарта от 24.10.2024 № 1504-ст).

При сдаче результатов работ Исполнитель должен письменно подтвердить факт проверки исходного кода программы на наличие уязвимостей с предоставлением соответствующего отчета.

3.8.7. Требования к организации удаленных подключений.

Исполнитель обеспечивает безопасность всей информации, полученной им в рамках оказания услуг (далее - Информация), в том числе:

- информация, содержащаяся в ГИС «РНИС СО»;
- информация, отражающая состав и содержание принятых мер по обеспечению информационной безопасности ГИС «РНИС СО»;
- информация, отражающая состав и содержание архитектуры ГИС «РНИС СО»;
- информация, доступ к которой ограничен Федеральными законами;
- информация, относящаяся к персональным данным;
- информация, отнесенная Государственным заказчиком к категории ограниченного распространения.

Исполнитель обязуется:

При оказании услуг, принимать организационные и технические меры по обеспечению безопасности информации, обрабатываемой в информационной системе Государственного заказчика, предусмотренные законодательством Российской Федерации, а также установленными Государственным заказчиком требованиями по защите информации, предъявляемые при подключении к сети и системам Государственного заказчика. Перед получением доступа Исполнитель и Государственный заказчик заключают соглашение о конфиденциальности (Приложение № 1 к Спецификации).

Обеспечивать организацию удаленного доступа к защищённой сети передачи данных Государственного заказчика с автоматизированных рабочих мест Исполнителя с использованием средств технической и криптографической защиты информации. Доступ осуществляется через терминальный сервер Государственного заказчика. Исполнитель обязуется самостоятельно приобрести необходимый перечень средств технической (далее – СЗИ) и криптографической защиты информации (далее – СКЗИ) для организации

защищенных подключений ViPNet Client KC3 версии не ниже 4 после согласования данного мероприятия с Государственным заказчиком. Использование эквивалента недопустимо в связи с имеющейся сетью криптографической защиты информации ViPNet KC3 № 3220. Исполнитель обязан использовать актуальные сертифицированные версии средств защиты информации. Для установки и настройки СЗИ и СКЗИ Исполнитель за свой счет может привлечь организацию, имеющую действующую лицензию ФСБ, ФСТЭК России на осуществление данного вида деятельности или выполняет работы самостоятельно

При получении удалённого доступа предоставить Государственному заказчику копию документа, подтверждающего соответствие Инфраструктуры Исполнителя требованиям безопасности информации, предъявляемым к государственным информационным системам не ниже 3-го класса защищённости, в соответствии с приказом ФСТЭК России от 11.04.2025 № 117. Соответствие требованиям безопасности информации должно подтверждаться аттестатом соответствия по приказу ФСТЭК России от 11.04.2025 № 117 или иным документом по результатам проведения оценки эффективности принимаемых мер по защите информации для подключаемых автоматизированных рабочих мест (информационной системы).

По требованию Государственного заказчика предоставлять информацию о состоянии дел по защите Информации.

Предоставить Государственному заказчику по запросу список своих сотрудников, допущенных к работе с Информацией, документы, определяющие полномочия этих работников, в том числе должностные инструкции и приказы о назначении ответственных сотрудников.

Не распространять и не предоставлять Информацию третьим лицам, включая своих сотрудников и работников Государственного заказчика, не допущенных к работе с Информацией, без письменного разрешения Заказчика, за исключением случаев, предусмотренных действующим законодательством.

Незамедлительно сообщить Государственному заказчику о допущенном Исполнителем, его представителями либо ставшем известным Исполнителю факте разглашения или угрозы разглашения, незаконном получении или незаконном использовании Информации.

Исполнитель несет ответственность за действия своих сотрудников, приведшие к раскрытию Информации любым третьим лицам.

В процессе оказания услуг по технической поддержке Системы, включающих разработку и(или) доработку компонентов, на Исполнителя возлагаются обязанности по устранению уязвимостей Системы, выявляемых по результатам общего сканирования Системы на предмет возможного наличия уязвимостей, а также периодического анализа защищенности в процессе эксплуатации.

3.8.8. Общие требования по защите информации, предъявляемые к Исполнителю.

При получении доступа до ИС (в том числе удаленного) или компонентов ИС Исполнителем должны проводиться дополнительные мероприятия по защите информации, направленные на исключение возможности несанкционированного доступа или воздействий на ИС и содержащуюся в ней информацию через взаимодействующие с ИС программно-аппаратные средства Исполнителя или каналы передачи данных и интерфейсы, используемые для доступа Исполнителя к ИС.

Не допускается копирование Исполнителем информации, к которой ему предоставлен доступ, если такое копирование не предусмотрено в документах оператора (обладателя информации) ИС, на основании которых Исполнителю предоставлен доступ к ИС.

Исполнитель в своих локальных документах должен установить требования по обеспечению защиты информации, к которой получен доступ.

В ИС, отдельных программно-аппаратных средствах Исполнителя, в которых осуществляются обработка и хранение полученной в результате предоставленного доступа информации, должны быть приняты меры по защите информации.

Разработка (развитие) и (или) тестирование программного обеспечения непосредственно в эксплуатируемой (находящейся в промышленной эксплуатации) ИС Заказчика Исполнителем не допускается. Указанные работы производятся на выделенных изолированных от ИС стендах разработки и (или) тестирования.

3.8.9. Требования, предъявляемые к защите автоматизированных рабочих мест Исполнителя.

Требования к защите информации автоматизированных рабочих мест (далее – АРМ), используемых при доработке/разработке функциональных возможностей компонентов ИС, а также АРМ, применяемых для организации удаленных подключений к ресурсам Государственного заказчика, включают:

- определение правил и процедур защиты АРМ;
- реализацию мер контроля физического доступа к техническим средствам АРМ;
- обеспечение безопасной настройки системного и прикладного ПО АРМ;
- реализацию парольной защиты и авторизации;
- применение средств защиты информации.

Детальные требования по защите АРМ пользователей могут быть уточнены (усилены) по результатам определения угроз безопасности информации и проектирования систем/подсистем защиты информации конкретной ИС.

Защита АРМ должна предусматривать контроль эффективности мер и средств защиты информации. Такой контроль должен быть периодическим (не реже одного раза в год). Исполнитель должен назначить администратора безопасности, на которого должны быть возложены задачи организации работ по защите АРМ, а также контроль за соблюдением предъявляемых требований.

Минимальные общие обязанности, предъявляемые к пользователям АРМ, должны предусматривать обязанности по:

- осуществлению выполнения требований парольной защиты;
- блокированию сеансов удаленного доступа и сеансов локального использования при покидании своего АРМ;
- выполнения требований эксплуатационной документации на используемые им средства защиты информации;
- оказания содействия в расследовании инцидентов информационной безопасности в ИС в рамках своей компетенции;
- информированию администратора безопасности в случае аппаратных или программных ошибок, сбоев в механизмах защиты информации АРМ;
- уведомлению администратора безопасности об обнаружении попыток или фактов несанкционированного доступа к информации, обнаружения инцидентов информационной безопасности.

Реализация мер контроля физического доступа к техническим средствам АРМ должна предусматривать:

- организацию контролируемой зоны, в пределах которой постоянно размещаются АРМ, обрабатывающие информацию, средства защиты информации, а также средства обеспечения функционирования АРМ;
- определение лиц, допущенных к АРМ, средствам защиты информации, средствам обеспечения функционирования АРМ, а также в помещения и сооружения, в которых они установлены;
- санкционирование физического доступа к АРМ, средствам защиты информации, средствам обеспечения функционирования АРМ, а также в помещения и сооружения, в которых они установлены;
- учет физического доступа к АРМ, средствам защиты информации, средствам обеспечения функционирования АРМ, а также в помещения и сооружения, в которых они установлены;
- размещение устройств вывода (отображения) информации (мониторов, принтеров) АРМ, исключающее ее несанкционированный просмотр;
- принятие мер, исключающих возможность несанкционированного изменения аппаратной части технических средств АРМ (например, путем опечатывания системного блока АРМ пользователя);
- применение средств доверенной загрузки (при необходимости).

Требования по настройке системного и прикладного программного обеспечения АРМ должны предусматривать соблюдение следующих минимальных требований:

- использование только лицензионного ПО фирм-изготовителей;
- установку ПО на АРМ только с официального дистрибутива, доверенного внутреннего репозитория или репозитория в российском сегменте «Интернет»;

- установку на АРМ сертифицированных средств антивирусной защиты и средств защиты от НСД, а также реализацию запрета на возможность их отключения;

Администратор безопасности должен сконфигурировать ОС, средство защиты от НСД и средство антивирусной защиты, а также прикладное ПО и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные версии ОС и прикладного ПО;
- исключить возможность загрузки и использования ОС, отличной от штатной;
- исключить возможность неконтролируемого Администратором безопасности удаленного управления, администрирования и модификации ОС и её настроек;
- режимы безопасности, реализованные в ОС и прикладном ПО, должны быть настроены на максимальный уровень;
- всем пользователям и группам, зарегистрированным в ОС, необходимо назначить минимально возможные для выполнения должностных обязанностей права;
- должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные пользователю привилегии;
- необходимо регулярно устанавливать пакеты обновлений безопасности ОС, обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС и прикладное ПО;
- необходимо использовать средство обнаружения уязвимостей, организовать регулярный анализ результатов аудита;
- организовать постоянный мониторинг и анализ событий безопасности, а также реагирование и предотвращение компьютерных атак.

На АРМ должны применяться следующие виды паролей:

- пароли BIOS/UEFI;
- пароли для входа в операционную систему и доступа к ресурсам информационных систем.

На АРМ привилегированных пользователей должны быть реализованы механизмы личной идентификации сотрудника.

Изменение аутентификационной информации (средств аутентификации), заданных их производителями или используемых при настройке ПО должно обеспечиваться администратором безопасности.

Администратор безопасности должен организовывать или осуществлять генерацию (назначение) паролей пользователя АРМ и присвоение им персональных идентификаторов.

Для паролей пользователей АРМ (в т.ч. привилегированных) и технологических учетных записей должны быть предустановлены требования:

- длина пароля для пользователей – не менее 12 символов; для привилегированных пользователей – не менее 12 символов; для технологических учетных записей – не менее 16 символов. Для паролей должны быть реализованы механизмы проверки сложности и повторяемости, использования специальных символов, строчных и заглавных букв;
- максимальное количество неудачных попыток аутентификации (ввода неправильного пароля) до блокировки не более 15 попыток;
- в качестве пароля не может быть использован один и тот же повторяющийся символ либо повторяющаяся комбинация из нескольких символов;
- в качестве пароля не может быть использована комбинация символов, набираемых в закономерном порядке на клавиатуре (например, 123456, qwerty и т. п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
- в качестве пароля не должны использоваться ранее использовавшиеся пароли.

Для защищаемых АРМ должно обеспечиваться:

- применение сертифицированных средств антивирусной защиты;
- применение сертифицированных средств защиты от НСД;
- применение средств межсетевого экранирования;
- применение средств (сервисов) анализа защищенности;
- применение средств мониторинга событий информационной безопасности или альтернативные меры мониторинга информационной безопасности и реагирования на инциденты;
- применение сертифицированных средств криптографической защиты информации.

Схема организации защищенного соединения должна быть согласована с Государственным заказчиком платформы. В зависимости от схемы организации защищенного соединения возможно предъявление дополнительных требований к средствам защиты информации.

Применяемые сертифицированные средства защиты информации должны быть сертифицированы в системе сертификации ФСТЭК России на соответствие требованиям по безопасности информации, заявленным для класса защищенности ИС, к которой осуществляется доступ с защищаемого АРМ.

Настройка и эксплуатация средств защиты информации должна осуществляться в соответствии с эксплуатационной документацией, достаточной для выполнения требуемого класса защищенности и уровня защищенности персональных данных ИС.

Применяемые средства защиты информации должны быть обеспечены со стороны их разработчиков поддержкой безопасности на территории Российской Федерации, включая выпуск и применение обновлений программного обеспечения, обеспечивающих устранение выявленных уязвимостей, дефектов и недостатков.

Средства защиты информации должны применяться с соблюдением запретов, установленных пунктом 6 Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Вышеуказанные требования могут быть скорректированы в соответствии с техническими условиями подключения внешних пользователей и конкретной ИС Заказчика.

По требованию Государственного заказчика Исполнитель должен предоставить Государственному заказчику копию документа, подтверждающего соответствие системы защиты информации подключаемых АРМ Исполнителя, установленным требованиям защиты информации для ИС Заказчика.

4. ОПИСАНИЕ СИСТЕМЫ

4.1. Архитектура системы.

Многоуровневая клиент-серверная архитектура.

4.2. Серверная часть.

Виртуальные серверы РНИС СО размещены на вычислительных ресурсах, расположенных в ЦОД Заказчика.

Исполнитель вправе в целях обеспечения функционирования РНИС СО вносить предложения об изменении состава и параметров вычислительных и сетевых ресурсов, а также их конфигурации. Государственный заказчик вправе запросить у Исполнителя обоснование предлагаемых изменений, а также принять либо отклонить указанные предложения.

Для обеспечения функционирования вычислительных ресурсов Государственный заказчик обеспечивает бесперебойную работу серверного оборудования.

Установленное программное обеспечение:

- операционная система — ALT Linux
- программное обеспечение, обеспечивающее функционирование РНИС СО: Docker, Rancher 1.6, CoreDNS, Apache Kafka, RabbitMQ, Ingress, Nginx.

4.3. Языки программирования, использованные при разработке данного программного обеспечения:

PHP, Golang, Javascript.

4.4. Используемые протоколы при работе данного программного обеспечения:

HTTPS, SOAP, EGTS, WebApi, gRPC.

4.5. Используемые СУБД:

Redis, PostgreSQL, ClickHouse, MongoDB.

«ЗАКАЗЧИК»

Руководитель учреждения

«ИСПОЛНИТЕЛЬ»

Должность

_____ А.А. Поколов

_____ ФИО

М.П.

М.П.

СОГЛАШЕНИЕ О КОНФИДЕНЦИАЛЬНОСТИ № _____

г. Южно-Сахалинск

«___» _____ 202__ г.

_____ именуемое Сторона-1, в лице _____, действующего на основании _____, с одной стороны, и _____, именуемое в дальнейшем Сторона-2, в лице _____, действующего на основании _____, вместе именуемые «Стороны», заключили настоящее Соглашение о конфиденциальности (далее – Соглашение) о нижеследующем:

Предмет соглашения:

1.1. Соглашение регулирует отношения, связанные с передачей и охраной конфиденциальности информации ограниченного доступа, которой Стороны будут обмениваться на всех этапах договорных отношений по _____

1.2. В рамках настоящего Соглашения Сторона, передающая информацию, именуется в дальнейшем «Передающая сторона», а Сторона, принимающая информацию, именуется в дальнейшем «Принимающая сторона». Обе Стороны настоящего соглашения могут быть, как Передающей стороной, так и Принимающей стороной.

1.3. Передающая сторона обязуется передавать по запросу Принимающей стороны в пользование Принимающей стороне информацию ограниченного доступа, а Принимающая сторона обязуется принимать, обеспечивать её сохранность и неразглашение.

Термины и определения:

2.1. В рамках настоящего Соглашения применяются термины и определения:

- «информация ограниченного доступа» - согласно части 2 статьи 5 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», за исключением сведений, составляющих государственную тайну;

- «конфиденциальность информации» согласно пункту 7 статьи 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- «персональные данные» - согласно пункту 1 статьи 3 Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных»;

- «служебная информация ограниченного распространения» согласно ст. 1.2 Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности, утвержденного постановлением Правительства Российской Федерации от 03.11.1994 № 1233 (далее - Положение 1233)

- «режим служебной тайны» - правовые, организационные, технические и иные меры, принимаемые Стороной для обеспечения ограничения на распространение служебной информации ограниченного доступа, и на доступ к этой информации.

Право на отнесение сведений к информации ограниченного доступа

3.1. Право на отнесение сведений к информации ограниченного доступа принадлежит обладателю такой информации.

3.1.1. Не является информацией ограниченного доступа следующая информация:

- информация, сведения или данные, носящие общеизвестный характер и являющиеся публично доступными;

- информация, которая на дату заключения настоящего Соглашения находилась в законном пользовании Принимающей стороны;

- информация, которая на момент ее передачи Принимающей стороне не была обозначена Передающей стороной как информация ограниченного доступа;

- информация, подпадающая под действие пункта 4 статьи 8 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Охрана конфиденциальности информации ограниченного доступа

4.1. Обладателем информации ограниченного доступа принимаются следующие меры по охране ее конфиденциальности:

4.1.1. Определение перечня информации ограниченного доступа.

4.1.2. Ограничение доступа к информации ограниченного доступа путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка.

4.1.3. Учет лиц, получивших доступ к информации ограниченного доступа и (или) лиц, которым такая информация была предоставлена или передана.

4.1.4. Регулирование отношений по использованию информации ограниченного доступа работниками на основании трудовых договоров, контрагентами на основании гражданско-правовых договоров и иными организациями на основании контрактов (договоров).

4.2. Принимающая Сторона обязуется с момента получения информации ограниченного доступа:

4.2.1. Не использовать ее полностью или частично в иных, непредусмотренных Соглашением, целях, кроме указанных в пункте 1.1. Соглашения, без получения предварительного письменного согласия Передающей Стороны.

4.2.2. Сохранять и защищать полученную информации ограниченного доступа, с соблюдением требований законодательства в области защиты информации.

4.2.3. Не разглашать и не способствовать прямо или косвенно разглашению третьим лицам информации ограниченного доступа.

4.2.4. Не копировать информацию ограниченного доступа, не размножать, не воспроизводить, не дублировать полностью или частично, пока такое копирование, размножение, воспроизведение или дублирование не будет разрешено в письменной форме Передающей стороной.

4.3. После получения письменного требования Передающей Стороны, а также после окончания срока действия договорных обязательств, и в случае собственной реорганизации или ликвидации, Принимающая сторона обязана за свой счет возвратить Передающей Стороне в течение 10 (десяти) календарных дней на основании соответствующего акта приема-передачи все полученные оригиналы и копии носителей информации ограниченного доступа или уничтожить по акту все оригиналы и копии информации ограниченного доступа, включая размноженные экземпляры, в любой форме, находящиеся в распоряжении Принимающей стороны. Один экземпляр акта об уничтожении предоставить Передающей Стороне.

4.4. Работниками, допускаемыми к информации ограниченного доступа и привлекаемыми к выполнению договорных обязательств, должны быть приняты обязательства о неразглашении информации ограниченного доступа (подписано соглашение о неразглашении информации ограниченного доступа). Сторона, получающая в соответствии с настоящим Соглашением информацию, составляющую коммерческую или служебную тайну, гарантирует, что ее работники, получившие доступ к этой информации, приняли обязательства о неразглашении информации ограниченного доступа (подписано соглашение о неразглашении информации ограниченного доступа).

4.5. Не передавать третьей стороне информацию ограниченного доступа, без письменного разрешения обладателя данной информации. Стороны при передаче информации ограниченного доступа третьей стороне должны убедиться, что последней приняты меры по охране её конфиденциальности не ниже мер, установленных настоящим Соглашением

4.5.1. Информация ограниченного доступа может быть раскрыта Принимающей стороной без согласия Раскрывающей стороны в следующих случаях:

- по запросу государственных органов, уполномоченным запрашивать такую информацию в соответствии с применимым законодательством, на основании должным образом оформленного запроса на предоставление указанной информации;

- по запросу судебных органов для целей защиты и исполнения прав по настоящему Соглашению и/или иным соглашениям, заключенным между Сторонами.

4.5.2. Если какая-либо из Сторон получит надлежащим образом выданное административное или судебное требование предоставить Информацию другой Стороны, получатель такого требования обязан незамедлительно уведомить вторую Сторону и предложить ей защитить свои интересы от такого требования.

4.5.3. В случае получения надлежаще оформленного мотивированного запроса уполномоченного государственного органа, на основании которого у Принимающей стороны возникнет обязанность раскрыть информацию ограниченного доступа без получения прямо выраженного письменного согласия Передающей стороны, Принимающая сторона обязуется раскрыть исключительно ту часть информации ограниченного доступа, раскрытие которой необходимо в силу законного требования государственного органа, в пределах, допустимых в соответствии с действующим законодательством Российской Федерации.

Регулирование отношений, связанных с защитой служебной информации ограниченного распространения

5.1. На материальные носители, содержащие служебную информацию ограниченного распространения, передаваемые одной Стороной другой Стороне, должна быть нанесена пометка «Для служебного пользования». Каждая Сторона считает полученную от другой Стороны или иной организации служебную информацию – информацией ограниченного распространения, если на носителях информации проставлена пометка «**Для служебного пользования**» или, в случае если при устной передаче информации сделано соответствующее сообщение.

5.2. Сторона, получившая служебную информацию ограниченного распространения от другой Стороны, обязуется:

5.2.1. Принять меры по охране ее конфиденциальности.

5.2.2. Сообщать ее исключительно работникам из числа граждан Российской Федерации, принявших согласно п. 4.4 Соглашения обязательства о неразглашении информации ограниченного доступа (подписавших соглашение о неразглашении информации ограниченного доступа), которым она необходима для достижения целей, определяемых договорными отношениями Сторон.

5.2.3. Не использовать ее полностью или частично в иных, не предусмотренных договорными отношениями, целях.

5.2.4. Не передавать третьей стороне служебную информацию ограниченного распространения, без письменного разрешения обладателя данной информации. Стороны при передаче служебной информации ограниченного распространения, третьей стороне должны убедиться, что последней приняты меры по охране её конфиденциальности не ниже мер, установленных настоящим Соглашением.

5.2.5. Не разглашать ее и не способствовать прямо или косвенно ее разглашению третьим лицам, а также лицам, не указанным в п. 5.2.2. Соглашения.

5.2.6. Не копировать и не вносить изменения в полученную служебную информацию ограниченного распространения без письменного разрешения Передающей стороны.

5.2.7. По окончании срока действия настоящего Соглашения обеспечить возврат служебной информации ограниченного распространения и зафиксированной на материальных носителях, Стороне, предоставившей указанную информацию.

5.3. В отношении информации с пометкой «Для служебного пользования» и ее материальных носителей (воспроизведений), переданных одной Стороной другой Стороне, действует режим служебной тайны.

5.4. Обязательства Сторон о неразглашении служебной информации ограниченного распространения, действуют в течение срока ее нахождения в режиме служебной тайны.

5.5. Стороны обязуются не использовать для обработки и передачи служебной информации ограниченного распространения каналы связи, не соответствующие установленным требованиям по технической защите информации.

5.6. В случае своей реорганизации Стороны примут меры по охране служебной информации ограниченного распространения не ниже мер, установленных настоящим Соглашением.

5.7. В случае ликвидации Стороны, она обязана в согласованный Сторонами срок до своей ликвидации обеспечить возврат служебной информации ограниченного распространения и зафиксированной на материальных носителях, Стороне, предоставившей указанную информацию.

Передача информации ограниченного доступа

6.1. Передача информации ограниченного доступа осуществляется:

- почтовыми отправлениями с уведомлением о вручении;
- нарочным;
- по средствам защищенного удаленного подключения с использованием ViPNet Client;
- в устной форме.

6.1.1. При передаче информации ограниченного доступа почтовыми отправлениями с уведомлением о вручении с вложением вышеуказанной Информации, зафиксированной на машинном и/или бумажном носителе, Передающая Сторона включает в почтовое отправление опись вложения, в которой указывается тип носителя и состав передаваемой информации ограниченного доступа. Если Принимающая Сторона не направит Передающей стороне уведомление об отсутствии в почтовом отправлении вложения или несоответствии вложения описи, Информация считается полученной почтовым отправлением с момента получения Передающей Стороной уведомления о вручении почтового отправления.

6.1.2. При передаче информации ограниченного доступа на машинном и/ или бумажном носителе посредством почтового отправления, фельдъегерской связью, либо с нарочным, Передающая Сторона оформляет в своей части Акт приема-передачи по форме соответствующего приложения (Приложение №1) к Соглашению. Принимающая Сторона при получении информации ограниченного доступа заполняет и подписывает Акт приема-передачи в своей части и отправляет его Передающей Стороне (почтовым отправлением с уведомлением о вручении, либо с нарочным) не позднее 5 календарных дней с даты получения. В случае неполучения Передающей Стороной подписанного Акта приема-передачи от Принимающей Стороны в течение вышеуказанного срока, Акт считается подписанным Принимающей Стороной.

6.1.3. При передаче информации ограниченного доступа в устной форме Передающая Сторона уведомляет Принимающую Сторону о том, что передаваемые в устной форме сведения и/или данные являются информацией ограниченного доступа. Передающая Сторона обеспечивает подготовку документа по переданной в устной форме информации ограниченного доступа в форме протокола совещания, переговоров, записи бесед, памятной записки и т.п., который подписывают обе Стороны. Передающая Сторона устанавливает в отношении данного документа требование об отнесении сведений к информации ограниченного доступа и осуществляет передачу документа в кратчайшие сроки Принимающей Стороне. Информация ограниченного доступа считается полученной с момента передачи ее в устной форме (при условии наличия подписанного с двустороннего подтверждения получения информации в устной форме).

6.2. Передача информации ограниченного доступа по открытым каналам телефонной, телеграфной и факсимильной связи, а также с использованием сети Интернет без соответствующих средств защиты (ViPNet Client) в соответствии с действующим законодательством, запрещена.

6.3. Раскрытие и/или передача информации ограниченного доступа в соответствии с Соглашением **не означает** предоставление Принимающей Стороне каких-либо прав (полностью или в их части) в отношении раскрытой/переданной информации ограниченного доступа, в том числе, прав на изобретения, открытия в ноу-хау, авторских прав, прав на товарные знаки, словесные обозначения торговые и технологические секреты, принадлежащие Передающей Стороне.

6.4. Относительно любого обмена информации ограниченного доступа, который может происходить между Сторонами в рамках Соглашения, Сторонами принято и согласовано, что нижеперечисленные сотрудники каждой из Сторон являются уполномоченными лицами, которым разрешено принимать и/или передавать информацию ограниченного доступа от имени соответствующей Стороны:

От имени организации _____

- ФИО, электронная почта

От имени организации _____:

- ФИО, электронная почта

6.5. Вся корреспонденция и переписка между Сторонами в соответствии с Соглашением, либо в связи с ним, а также все сопутствующие документы, в том числе Акты приема-передачи, направляемые Сторонами друг другу, должны быть совершены в письменной форме и переданы почтовым отправлением с уведомлением о вручении, либо доставлены нарочным по следующим адресам:

ГКУ «Сахдормониторинг»

Место нахождения:

693020, Сахалинская область, г. Южно-Сахалинск, ул. Сахалинская, д. 48

ИНН: 6501281755

КПП: 650101001

Адрес электронной почты: cdm@sakhalin.gov.ru

Исполнитель:

Место нахождения:

ИНН:

КПП:

Адрес электронной почты:

6.6. При передаче информации ограниченного доступа, не относящейся к служебной информации ограниченного распространения, Передающая сторона обязана осуществить её классификацию в соответствии с Указом Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015)

«Об утверждении Перечня сведений конфиденциального характера» и сообщить Принимающей стороне особенности правовой охраны данной такой информации.

6.7. При передаче **персональных данных** Передающая сторона обязана осуществить такую передачу с оформлением поручения на обработку персональных данных в соответствии с требованиями части 3 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 30.12.2020) «О персональных данных».

6.8. Риски ненадлежащего оформления Информации, в соответствии с требованиями настоящего раздела Соглашения, несет Передающая сторона.

Разглашение информации:

7.1. Под разглашением информации ограниченного доступа понимается действие или бездействие, в результате которого информация ограниченного доступа в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации, либо вопреки трудовому или гражданско-правовому договору.

7.2. При утрате, разглашении или подозрении на разглашение информации ограниченного доступа, Стороны обязуются незамедлительно информировать друг друга и принять все необходимые меры по предотвращению дальнейшего разглашения ограниченного доступа, а также выявлению причиненного ущерба или иных отрицательных последствий, вызванных ее утратой или разглашением.

7.3. Принимающая Сторона не несет никаких обязательств или ограничений относительно любой Информации в случае, когда может доказать, что:

- информация ограниченного доступа стала общественным достоянием до ее раскрытия Принимающей Стороной;
- информация ограниченного доступа была передана с нарушением требований раздела 5 и 6 настоящего Соглашения.
- информация ограниченного доступа в течение действия Соглашения или до истечения, указанного в п.9.1 Соглашения срока, стала общеизвестной и публичной иначе, чем в результате нарушения Соглашения;
- информация ограниченного доступа уже была известна Принимающей Стороне, о чем свидетельствует соответствующий письменный документ в архиве Принимающей Стороны;
- информация ограниченного доступа была независимо добросовестно разработана сотрудниками Принимающей Стороны, не имевшими доступа к такой Информации;
- информация ограниченного доступа одобрена для раскрытия третьим лицам посредством ясно выраженного письменного разрешения Передающей Стороны.

Ответственность:

8.1. Принимающая Сторона, допустившая разглашение Информации, при условии предоставления Передающей Стороной доказательств вины Принимающей Стороны, обязана компенсировать в полном объеме весь действительный ущерб, причиненный Передающей Стороне таким разглашением.

8.1.1. Принимающая Сторона несет ответственность в соответствии с действующим законодательством Российской Федерации за разглашение информации ограниченного доступа, то есть за свои действия или бездействие, в результате которых информация ограниченного доступа становится известной Третьим лицам в нарушение условий настоящего Соглашения. Ответственность Принимающей стороны ограничивается размером реального документально подтвержденного ущерба, понесенного Передающей стороной в результате виновных действий Принимающей стороны.

8.2. Все разногласия и споры, возникающие при исполнении Соглашения или в связи с ним, Стороны будут решать путем проведения переговоров. В случае не достижения согласия, споры будут передаваться на рассмотрение в Арбитражный суд г. Южно-Сахалинска.

Срок действия:

9.1. Соглашение вступает в силу с даты его подписания Сторонами и действует в течении действия договорных отношений сторон.

9.2. Во всем остальном, что не предусмотрено условиями Соглашения, Стороны будут руководствоваться действующим законодательством Российской Федерации.

9.3. Ни одна из Сторон не вправе передавать свои права и обязанности по Соглашению третьим лицам без письменного согласия на это другой Стороны.

9.3.1. В случаях реорганизации Принимающей стороны, последняя обязуется не позднее чем за 60 (шестьдесят) календарных дней уведомить о предстоящей реорганизации Передающую сторону.

9.3.2. Права и обязанности Сторон по настоящему Соглашению в случае реорганизации какой-либо из Сторон переходят к соответствующему правопреемнику (правопреемникам) реорганизованной Стороны, и такие правопреемники будут нести все права и обязанности по настоящему Соглашению в отношении другой Стороны.

9.3.3. В случае ликвидации Принимающей стороны, она обязана до завершения ликвидации вернуть Передающей стороне все оригиналы и копии (или обеспечить уничтожение копий) всех материальных носителей с информацией ограниченного доступа, переданной по настоящему Соглашению

9.4. Любые изменения и дополнения к Соглашению действительны, только если они составлены в письменной форме и подписаны уполномоченными представителями обеих Сторон.

9.5. Соглашение подписано в двух экземплярах, имеющих равную юридическую силу, по одному для каждой из сторон.

«ЗАКАЗЧИК»

Руководитель учреждения

«ИСПОЛНИТЕЛЬ»

Должность

_____ А.А. Поколов
М.П.

_____ ФИО
М.П.

ОБРАЗЕЦ

**Акт
приема-передачи документов, содержащих информацию ограниченного доступа**

г. Южно-Сахалинск _____ 20__ г.

Мы, нижеподписавшиеся, Наименование организации _____ (далее – «Сторона - 1»), в лице уполномоченного представителя _____, действующего на основании _____, с одной стороны, и Наименование организации (далее – «Сторона - 2»), в лице уполномоченного представителя _____, действующего на основании _____, с другой стороны, совместно именуемые «Стороны», составили настоящий Акт о том, что «_____» передал, а «_____» принял нижеперечисленные документы, содержащие информацию ограниченного доступа:

№ п/п	Номер и дата документа (индекс и крайние даты дела)	Заголовок документа (дела)/описание содержимой информации	Количество листов документа (дела)

Всего _____ (_____) документов (дел).

От «_____» передал:
_____(должность)

подпись ФИО

От «_____» принял:
_____(должность)

подпись ФИО

Сторона 1

_____/ ФИО.
М.П.

Сторона 2

_____/ ФИО
М.П.

«ЗАКАЗЧИК»

Руководитель учреждения

М.П. А.А. Поколов

«ИСПОЛНИТЕЛЬ»

Должность

М.П. ФИО