

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на выполнение работ по развитию ведомственной информационной системы «Енисей-Стройнадзор» в части настройки интеграций с ФГИС Росреестр.

1 Общие сведения

1.1 Наименование Системы, полное наименование выполняемых работ

Полное наименование системы: ВИС «Енисей-Стройнадзор» (далее - Система).

Полное наименование выполняемых работ: Выполнение работ по развитию ведомственной информационной системы «Енисей-Стройнадзор» (далее - Работы).

1.2 Наименование Заказчика и Пользователей

Заказчик: Служба строительного надзора и жилищного контроля Красноярского края.

Пользователь: Служба строительного надзора и жилищного контроля Красноярского края.

1.3 Наименование Подрядчика

Подрядчиком работ является юридическое лицо, с которым будет заключен контракт в соответствии с положениями [Гражданского кодекса](#) Российской Федерации, [Федерального закона](#) от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее - Подрядчик).

1.4 Место проведения работ

Подрядчик выполняет работы по месту нахождения Пользователя: 660049, Красноярский край, г. Красноярск, ул. Парижской коммуны, д. 33.

Подрядчик имеет право выполнить работы в удаленном режиме средствами информационных технологий и телекоммуникаций.

1.5 Основания для выполнения работ

Правовым основанием для выполнения работ служат: Распоряжение Правительства Российской Федерации от 2 марта 2026 г. № 398-р «Стратегическое направление в области цифровой трансформации отраслей строительства и жилищно-коммунального хозяйства Российской Федерации до 2030 года» и [Распоряжение](#) Правительства РФ от 31.10.2022 г. №3268-р «Об утверждении Стратегии развития строительной отрасли и жилищно-коммунального хозяйства РФ на период до 2030 г. с прогнозом до 2035 г.».

Выполнение работ производится на основании Государственного Контракта.

Выполнение работ и их результаты должны соответствовать требованиям следующих нормативно-правовых актов:

- [Федеральный закон](#) от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (статья 21.3);
- [Федеральный закон](#) от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- [Постановление](#) Правительства РФ от 06.07.2015 № 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»;
- [Постановление](#) Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- [Приказ](#) ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;
- [Постановление](#) Правительства РФ от 08.09.2010 № 697 «О единой системе межведомственного электронного взаимодействия»;
- Приказ Федеральной службы государственной регистрации, кадастра и картографии от 8 апреля 2021 г. № П/0149 "Об установлении Порядка предоставления сведений, содержащихся в Едином государственном реестре недвижимости, и Порядка уведомления заявителей о ходе оказания услуги по предоставлению сведений, содержащихся в Едином государственном реестре недвижимости"

Ведомственная информационная система «Енисей-Стройнадзор» построена на микросервисной архитектуре технологической платформы «Акцент-Стройнадзор» (реестровая запись № 17794 в Едином реестре российских программ для электронных вычислительных машин и баз данных).

Интеллектуальные права на программную платформу для «Акцент-Стройнадзор», на основании которой разработано и функционирует программное обеспечение ведомственная информационная система «Енисей-Стройнадзор», принадлежат ООО «Бинго-Софт» ИНН 5259097373, ОГРН 1115259010184.

В соответствии с требованиями о патентной чистоте и законодательства Российской Федерации, регулирующего защиту интеллектуальной собственности ([статьи 1225, 1229, 1232, 1234, 1235, 1238, 1259, 1262, 1285, 1286, 1288, 1295, 1296, 1297](#) Гражданского кодекса Российской Федерации) в течение 5 (пяти) рабочих дней со дня заключения контракта Исполнитель обязан представить Заказчику надлежащим образом заверенные копии документов, подтверждающих право Исполнителя оказывать работы, предусмотренные Контрактом и связанные с программой для ЭВМ, являющейся платформой ведомственной информационной системы «Енисей-Стройнадзор», а именно:

если Исполнитель является правообладателем (обладателем исключительного права): копия свидетельства о регистрации права собственности на программу для ЭВМ или копия договора об отчуждении исключительных прав на программу для ЭВМ, или копия документа о создании служебного произведения, разработки программы для ЭВМ (решение, протокол, приказ, распоряжение или иной вид документа, предусмотренный в организации, с указанием принадлежности исключительного права или с актом приема-передачи исключительных прав, или с актом приемки/постановки на баланс актива), или копия договора заказа (разработки, создания) программы для ЭВМ с указанием принадлежности исключительного права Исполнителю (с актом приема-передачи исключительных прав), или копия договора авторского заказа (создания, разработки) программы для ЭВМ с указанием принадлежности исключительного права Исполнителю (с актом приема-передачи исключительных прав), или документ базы данных Федерального государственного бюджетного учреждения «Федеральный институт промышленной собственности» в формате результата поиска в информационно-поисковой системе Федерального государственного бюджетного учреждения «Федеральный институт промышленной собственности».

1.6 Плановые сроки начала и окончания выполнения работ

С даты заключения контракта до 10 декабря 2026 г.

1.7 Термины и определения

Таблица 1 - Используемые термины и определения в настоящем техническом задании.

Определение	Значение
Система	Ведомственная информационная система «Енисей-Стройнадзор»
Работы	Работы по развитию Системы
Заказчик	Служба строительного надзора и жилищного контроля Красноярского края
Контракт	Государственный контракт на выполнение работ по развитию информационной системы автоматизации строительного надзора
Подрядчик	Юридическое лицо в соответствии с п. 1.3 настоящего технического задания
ТЗ	Техническое задание
ВИС	Ведомственная информационная система
БД	База данных
СУБД	Система управления базами данных
РФ	Российская Федерация
СМЭВ	Система межведомственного электронного взаимодействия.
РИД	Результат интеллектуальной деятельности
ФГИС ЕГРН	Федеральная государственная информационная система «Единый государственный реестр недвижимости»
ЕГРН	Единый государственный реестр недвижимости
Росреестр	Федеральная служба государственной регистрации, кадастра и картографии
ГИС ЖКХ	Государственная информационная система жилищно-коммунального хозяйства
ЕРКНМ	Единый реестр контрольных (надзорных) мероприятий
ПОС	Платформа обратной связи
МКД	Многоквартирный дом
УКЭП	Усиленная квалифицированная электронная подпись
ЭЦП	Электронная подпись (электронная цифровая подпись)
ЦОД	Центр обработки данных
XML	Расширяемый язык разметки (eXtensible Markup Language)
XSD	Схема XML (XML Schema Definition) — язык описания структуры XML-документа

2 Цели и назначение развития автоматизированной системы

2.1 Цели выполнения работ

Целью выполнения работ является развитие Системы для настройки интеграционного взаимодействия модулей регионального государственного жилищного надзора и надзора за долевым строительством со следующими информационными системами: ФГИС Росреестр в части направления заявлений (также прилагаемых к заявлению документов) на предоставление услуг Росреестра и получение результатов оказания услуги.

2.2 Решаемые задачи

В рамках развития Системы должна быть решена задача по доработке модуля сервисного взаимодействия, позволяющая реализовывать интеграции с государственной информационной системой ФГИС ЕГРН, а также по изменению настроек внутренних бизнес-процессов позволяющих осуществлять возложенные на службу функции по рассмотрению

заявлений о внесении изменений в перечень многоквартирных домов реестра лицензий Красноярского края на осуществление предпринимательской деятельности по управлению многоквартирными домами, а также осуществления контроля за обеспечением регистрации договоров участия в долевом строительстве.

Бизнес-процесс рассмотрения указанных заявлений представлен на диаграмме (Приложение к ТЗ — файл «процесс рассмотрения заявления о внесении изменений в РЛКК.pdf»).

2.3 Назначение

Развитие системы в части интеграционных взаимодействий направлено на создание единого, автоматизированного и законодательно соответствующего информационного контура для управления сквозными процессами в рамках деятельности службы строительного надзора и жилищного контроля Красноярского края.

Основное назначение работ - обеспечение обмена данными с внешними информационными системами. Интеграции предназначены для обеспечения своевременности и достоверности данных, а также снижения ручного труда пользователей.

3 Описание Системы

3.1 Сведения о Системе

Ведомственная информационная система «Енисей-Стройнадзор» (сокращенное наименование – ЕСН) предназначена для автоматизации деятельности службы строительного надзора и жилищного контроля Красноярского края. Система построена на клиент-серверной технологии, поддерживается многопользовательская работа с аутентификацией и разграничением доступа.

Права на ВИС ЕСН переданы Заказчику на основании договора об отчуждении исключительного права на РИД № 3/24 от 07.02.2024 года.

Ранее выполнялись работы по развитию и модернизации ВИС «Енисей-Стройнадзор» на основании государственного контракта № 253/22 от 26.09.2022 года, проведенного на основании электронного аукциона ЭА-№-13528/22 ([Реестровый номер:0119200000122011700](#)).

3.2 Описание функциональных подсистем Системы

На момент выполнения работ в соответствии с настоящим ТЗ в состав Системы входят следующие модули и подсистемы:

Модули:

- «Цифровая вертикаль строительной отрасли Енисей-Стройнадзор»
- «Цифровая экосистема отрасли жилищно-коммунального хозяйства Енисей-Стройнадзор»

В модуле «Цифровая вертикаль строительной отрасли Енисей-Стройнадзор» реализованы следующие подсистемы:

- подсистема строительного надзора;
- подсистема надзора в сфере долевого строительства;
- подсистема административного делопроизводства;
- подсистема досудебного обжалования;
- подсистема формирования отчетности;
- подсистема информирования;
- подсистема ведения справочников и классификаторов;
- подсистема аналитической отчетности и мониторинга;

- подсистема картографии;
- подсистема сервисного взаимодействия;
- подсистема администрирования.

В модуле «Цифровая экосистема отрасли жилищно-коммунального хозяйства Енисей-Стройнадзор» реализованы следующие функциональные блоки:

- рабочие столы сотрудников (руководитель, инспекторы, юристы и иные категории пользователей);
- блок капитального ремонта;
- блок жилого фонда;
- блок лицензирования;
- блок мониторинга;
- блок интеграционного взаимодействия с ПОС;
- блок документов (обращения, входящая и исходящая корреспонденция);
- блок организационно-распорядительных документов;
- блок профилактических мероприятий;
- блок интеграции с ЕРКНМ и ГИС ЖКХ;
- блок протоколов общих собраний собственников;
- блок планирования проверок;
- блок журналов;
- блок административного делопроизводства;
- блок досудебного обжалования;
- блок межведомственной комиссии (МВК);
- блок контрагентов;
- отчетность;
- база знаний и инструкции;
- календарь;
- блок администрирования.

3.3 Описание технического (аппаратного и программного) обеспечения Системы

Система создана на платформе «Акцент-Стройнадзор», которая используется на основании бессрочной неисключительной лицензии.

Используемая среда функционирования Системы включает в себя следующие компоненты:

- Сервер приложений: обеспечение подключения к БД Системы.
- Сервер базы данных: обеспечение взаимодействия с системой хранения данных, содержащей информационную базу данных. База данных под управлением СУБД PostgreSQL.

4 Состав и содержание работ

4.1 Обзор работ

В рамках настоящего развития Системы должны быть выполнены следующие основные виды работ:

1) Интеграция модуля регионального государственного жилищного надзора «Цифровая экосистема отрасли жилищно-коммунального хозяйства Енисей-Стройнадзор» (Системы) с государственной информационной системой Федеральной службы государственной регистрации, кадастра и картографии. Работы включают настройку обмена на направление и

прием заявлений (также прилагаемых к заявлению документов) на предоставление услуг Росреестра и получение результатов оказания услуги в рамках блока лицензирования. Выполнение указанных работ осуществляется в соответствии с этапами бизнес-процесса рассмотрения заявлений о внесении изменений в реестр лицензий, описанного в прилагаемой диаграмме.

2) Интеграция подсистемы регионального государственного надзора за долевым строительством модуля «Цифровая вертикаль строительной отрасли Енисей-Стройнадзор» (Системы) с государственной информационной системой Федеральной службы государственной регистрации, кадастра и картографии. Работы включают настройку обмена на направление и прием заявлений (также прилагаемых к заявлению документов) на предоставление услуг Росреестра и получение результатов оказания услуги.

4.2 Функциональные требования

В рамках настоящего развития Системы должны быть реализованы следующие функциональные требования по интеграции с ФГИС Росреестр.

4.2.1 Общие требования к интеграции с ФГИС Росреестр

Интеграционное взаимодействие Системы с ФГИС Росреестр осуществляется посредством СМЭВ (Система межведомственного электронного взаимодействия) в рамках предоставления сведений, содержащихся в ЕГРН через вид сведений «Прием обращений в ФГИС ЕГРН» <https://nsud.gosuslugi.ru/pud/paip-portal/#/inquiries/card/dd0b99d3-d9cd-11eb-87f2-6dd2d98a56b1?tab=0>

Интеграция должна обеспечивать:

1. Подготовку и отправку межведомственного запроса:
 - формирование структурированного XML-документа по утвержденной XSD-схеме формата межведомственного обмена;
 - применение электронной подписи отправителя к сформированному пакету данных;
 - интеграцию с адаптером СМЭВ для отправки подписанных запросов;
 - обработку ответов от адаптера СМЭВ.
2. Прием и обработку ответной информации:
 - прием ответных сообщений через каналы межведомственного взаимодействия;
 - парсинг структурированных данных из форматов межведомственного обмена;
 - извлечение ключевых атрибутов: идентификаторы объектов недвижимости, характеристики объектов, сведения о правообладателях и зарегистрированных правах;
 - фиксацию отказов с сохранением указанных оснований и кодов ошибок.
3. Обеспечение юридической значимости и аудита:
 - гарантированное сохранение в неизменном виде всех этапов взаимодействия: исходные параметры запроса, отправленные пакеты, полученные ответы в течение 90 дней;
 - обеспечение хранения электронных документов и подписей в течение 90 дней с сохранением юридической силы.
4. Управление процессом взаимодействия:
 - поддержку асинхронной модели взаимодействия с отслеживанием статусов выполнения запросов;
 - реализацию механизмов обработки длительных операций и повторных опросов при необходимости;

4.2.2 Требования к интеграции для модуля «Цифровая экосистема отрасли жилищно-коммунального хозяйства Енисей-Стройнадзор»

4.2.2.1 Общее описание

Интеграция модуля регионального государственного жилищного надзора «Цифровая экосистема отрасли жилищно-коммунального хозяйства Енисей-Стройнадзор» с ФГИС Росреестра обеспечивает получение сведений из ЕГРН об объектах недвижимости и их правообладателях (идентификатор сценария: //req:Request/req:actionCode/text()=65951111112, пространство имен: urn://x-artefacts-rosreestr-gov-ru/virtual-services/egrn-statement/1.2.2.) в рамках рассмотрения заявлений о внесении изменений в перечень многоквартирных домов реестра лицензий Красноярского края на осуществление предпринимательской деятельности по управлению многоквартирными домами.

Процесс взаимодействия с Росреестром реализуется в следующей последовательности:

- 1) Запрос по дому
 - Формирование и отправка запроса в ЕГРН по кадастровому номеру многоквартирного дома для получения перечня всех помещений в МКД и их характеристик.
 - Ведение статуса «Запрос отправлен по дому» с момента успешной отправки запроса через СМЭВ.
 - Автоматическое обновление статуса на «Получен ответ по дому» после получения и успешной обработки ответа от Росреестра.
 - Отображение полученного перечня помещений МКД с заполнением следующих полей: кадастровый номер помещения, номер помещения, площадь помещения.
- 2) Запрос по помещениям
 - Автоматическое формирование запросов по каждому помещению в МКД для получения сведений о правообладателях.
 - Ведение статуса «Отправлен запрос по помещениям в МКД» после отправки всех запросов по помещениям.
 - Автоматическое обновление статуса на «Получен ответ по помещениям в МКД» после получения и обработки всех ответов по помещениям.
 - Обработка асинхронных ответов от Росреестра с автоматическим определением момента получения всех выписок по помещениям.
- 3) Уведомления
 - Автоматическое уведомление сотрудника, инициировавшего запрос, о получении ответа по дому.
 - Автоматическое уведомление сотрудника о получении ответов по всем помещениям.
- 4) Подписание запросов
 - Запросы в ЕГРН подписываются усиленной квалифицированной электронной подписью (УКЭП) сотрудника, инициирующего запрос.
 - Процедура подписания осуществляется через стандартное окно подписания ЭЦП.
 - Подпись фиксирует факт инициации запроса конкретным сотрудником.

4.2.2.2 Формирование реестра собственников помещений

Система должна обеспечивать формирование реестра собственников помещений на основе данных, полученных из выписок ЕГРН, со следующим составом сведений:

- Номер помещения;
- Кадастровый номер помещения;

- Сведения о собственнике (вместо полных Фамилии, Имени и Отчества - только первые заглавные буквы с точкой, например: «Иванов И.И.»);

- Доля в праве собственности;
- Площадь помещения;
- Тип помещения;
- Этаж;
- Дата получения выписки из Росреестра;
- Вид собственности;
- Дата вступления собственника в право собственности;

Реестр собственников должен формироваться в двух разрезах:

1. По помещению в многоквартирном доме - отображение собственников конкретного помещения.

2. По многоквартирному дому - отображение всех собственников всех помещений в МКД.

Реестр должен предоставлять возможность:

- Визуализации в виде таблицы на экране;
- Экспорта в формат Microsoft Excel;

4.2.2.3 Чек-лист проверки реестра собственников

На основании реестра собственников, сформированного из данных ЕГРН, система должна обеспечивать формирование чек-листа проверки сведений из Росреестра на соответствие данным, представленным управляющей организацией в составе приложения к протоколу общего собрания собственников (реестр собственников помещений в МКД на бумажном носителе).

Функциональные требования к чек-листу:

1. Чек-лист содержит перечень всех собственников помещений в МКД с указанием:
 - номера помещения;
 - сведений о собственнике (Фамилия, Имя, Отчество - полные, для идентификации);
 - доли в праве собственности;
 - площади помещения.
2. По каждому собственнику помещения инспектор службы проставляет статус проверки:
 - «Соответствует реестру на бумажном носителе» - при совпадении данных ЕГРН с данными, представленными управляющей организацией.
3. Чек-лист автоматически формирует суммарные сведения:
 - общая площадь всех помещений по данным Росреестра;
 - общая площадь помещений по данным Росреестра, прошедших сверку с бумажным носителем (статус «Соответствует реестру на бумажном носителе»).
4. Чек-лист должен предусматривать поле для подписания УКЭП инспектора, осуществлявшего проверку.
5. Подписанный чек-лист сохраняется в Системе в неизменном виде как официальный документ проверки.

4.2.2.4 Интеграция с бизнес-процессом рассмотрения заявлений

Результаты интеграции с Росреестром должны быть встроены в бизнес-процесс рассмотрения заявлений о внесении изменений в перечень многоквартирных домов реестра лицензий (диаграмма процесса приведена в Приложении к ТЗ).

1) Расширение блока «Проверочные мероприятия»

В рамках этапа «Проверочные мероприятия» бизнес-процесса наряду с существующими источниками информации (ЕГРЮЛ, ЕСН, сайт Арбитражного суда КК, ГИС ЖКХ) должен быть добавлен новый вид информационного взаимодействия - запрос сведений из ЕГРН через интеграцию с Росреестром.

Проверочные мероприятия включают:

- Формирование запроса в ЕГРН по дому (получение перечня помещений и их характеристик);
- Формирование запросов в ЕГРН по помещениям (получение сведений о правообладателях);
- Формирование реестра собственников на основе полученных данных;
- Формирование чек-листа проверки реестра собственников;
- Визуальное сравнение данных ЕГРН с данными, представленными управляющей организацией;
- Подготовку заключения, содержащего результаты проверочных мероприятий.

2) Расширение блока «Запрос о предоставлении необходимых документов»

В рамках этапа бизнес-процесса, предусматривающего направление запросов о предоставлении необходимых документов, должен быть реализован дополнительный механизм - направление запроса в Росреестр (в дополнение к существующему виду документа «Запрос на бумажном носителе»).

Запрос в Росреестр формируется и отправляется в электронном виде через СМЭВ и не требует направления запроса на бумажном носителе.

4.2.3 Требования к интеграции для модуля «Цифровая вертикаль строительной отрасли Енисей-Стройнадзор»

4.2.3.1 Общее описание

Интеграция подсистемы регионального государственного надзора за долевым строительством модуля «Цифровая вертикаль строительной отрасли Енисей-Стройнадзор» с ФГИС Росреестр должна обеспечивать получение и последующую обработку следующих документов и сведений из ЕГРН в целях осуществления контроля за деятельностью застройщиков, связанной с привлечением денежных средств участников долевого строительства:

- сведения о заключенных договорах участия в долевом строительстве;
- сведения о характеристиках объекта недвижимости в отношении земельного участка, объекта незавершенного строительства;
- документы, связанные с привлечением денежных средств участников долевого строительства (ДДУ, договоры об уступке прав требований, допсоглашения к ним);
- реестр собственников помещений в объектах, в отношении которых осуществлялось привлечение денежных средств участников долевого строительства.

4.2.3.2 Функциональные требования

В Системе должна быть реализована возможность интеграционного взаимодействия в рамках следующих сценариев руководства пользователя вида сведений:

- 1) 65951111112 «Предоставление сведений, содержащихся в ЕГРН, об объектах недвижимости и (или) их правообладателя».

Работа с запросами осуществляется в отдельном разделе карточки субъекта долевого строительства или ЖСК.

Взаимодействие с Росреестром осуществляется путем формирования и отправки запроса и получения ответа на отправленный запрос

В системе должна быть возможность формировать запросы по кадастровому номеру земельного участка и по кадастровому номеру объекта.

Система должна обеспечивать автоматическое ведение журнала отправленных запросов и полученных ответов. Автор запроса должен быть уведомлен Системой о получении ответа на запрос. Предусмотреть автоматическое заполнение статуса запроса «Запрос отправлен» после успешной отправки запроса, «Получен ответ» после получения и успешной обработки ответа.

Система должна обеспечить просмотр запроса и доступ к выбранным файлам, полученным в ответе.

Полученные в ответе сведения должны автоматически размещаться в соответствующие поля карточки в Системе.

В системе должна быть реализована возможность получения следующих сведений:

- назначение помещения;
- площадь помещения;
- этаж;
- Информация о собственнике (ФИО/наименование, ИНН, дата рождения для ФЛ;
- информация о договорах уступок;
- информация о допсоглашениях

Реализовать реестр помещений с заполнением следующих полей: кадастровый номер помещения, номер помещения, площадь помещения.

Система должна обеспечивать автоматическое формирование запросов по каждому помещению.

Реализовать автоматическое уведомление сотрудника, инициировавшего запрос, о получении ответа по дому.

Реализовать автоматическое уведомление сотрудника после получении ответов по всем помещениям.

4.2.4 Требования к хранению и защите персональных данных

4.2.4.1 Ограничение доступа к персональным данным

В рамках модернизации ВИС «Енисей-Стройнадзор» должны быть реализованы механизмы, исключающие доступ сотрудников Службы к персональным данным, содержащимся в выписках, получаемых от Росреестра, за исключением сотрудников с ролью «Администратор».

Реализация должна обеспечивать:

1. Разграничение доступа на уровне пользовательских ролей:

- Сотрудники с ролью «Администратор» имеют доступ к системным–логам всех обращений к выпискам ЕГРН.

- Сотрудники с иными ролями (инспекторы, начальники отделов, юристы и т.д.) не имеют доступа к персональным данным (полные ФИО собственников, иные идентифицирующие сведения).

2. Маскирование персональных данных:

- Для сотрудников без роли «Администратор» персональные данные в реестрах и выписках отображаются в обезличенном виде (только первые заглавные буквы Фамилии, Имени и Отчества с точкой).

- Полный доступ к персональным данным предоставляется только при наличии роли «Администратор» и обоснованной служебной необходимости.

3. Аудит доступа:

- Система должна вести журнал аудита всех обращений к выпискам ЕГРН с фиксацией: кто (пользователь), когда (дата и время), к каким данным осуществлялся доступ, вид операции с данными (сохранение, изменение, удаление).

В журналах аудита должны фиксироваться:

- чтение;
- запись;
- удаление;

- Журнал аудита должен быть доступным для проверки уполномоченными лицами.

- Журналирование операций скачивания файлов.

4.2.4.2 Хранение выписок из Росреестра

Резервное копирование:

- Хранение выписок должно быть включено в общую систему резервного копирования Системы в соответствии с требованиями п. 5.1 настоящего ТЗ.

Удаление:

- Должно быть обеспечено автоматическое удаление выписок по истечении 90 календарных дней с момента загрузки в Систему.

Частичный импорт информации:

- Система должна поддерживать возможность частичного импорта данных из выписок Росреестра без загрузки полного xml-файла выписки.

Изоляция защищаемых данных:

- Защищаемые файлы должны храниться в отдельном выделенном каталоге, изолированном от основного массива файлов системы;

- Для защищаемого каталога должны быть установлены минимально необходимые права доступа. Наследование прав от родительских каталогов должно быть отключено;

- Создать специальную служебную учётную запись (пользователя), обладающую доступом к защищаемому каталогу;

4.2.5 Требования к документированию интеграции

В дополнение к общим требованиям к документированию, изложенным в п. 5.2 настоящего ТЗ, Подрядчик обязан разработать следующую документацию по интеграционному взаимодействию:

1. Описание форматов обмена - спецификация XML-схем запросов и ответов при взаимодействии с ФГИС Росреестр через СМЭВ.

2. Руководство пользователя по работе с сервисом «Запрос в ЕГРН» - описание порядка формирования запросов, подписания, отслеживания статусов и получения результатов.

3. Руководство пользователя по работе с реестром собственников и чек-листом проверки - описание порядка формирования реестра, проведения проверки и подписания чек-листа.

4. Регламент информационного взаимодействия - описание последовательности действий при интеграции, сроков обработки запросов, порядка обработки ошибок и отказов.

5. Инструкция по администрированию интеграции - описание настроек СМЭВ, управления сертификатами электронной подписи, мониторинга статусов запросов.

5 Требования к развиваемой системе

5.1 Требования к информационной безопасности

Для обеспечения безопасности работы Системы Подрядчик обязуется:

- Выполнять требования приказа Федеральной службы по техническому и экспортному контролю от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;
- Осуществлять доступ к Системе Государственного заказчика с использованием средств защиты информации (в том числе криптографических), прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации, требуемого класса защиты в соответствии с действующим законодательством Российской Федерации;
- Обеспечить применение на рабочих местах, подключенных к Системе, средств защиты от вредоносного программного обеспечения, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации;
- Принимать меры по предотвращению воздействия на технические средства обработки информации, в результате которого нарушается (либо создаются объективные предпосылки) их функционирование;
- Устранять уязвимости программного обеспечения в согласованный между Подрядчиком и Государственным заказчиком срок, выявляемые по результатам общего сканирования Системы лицензированными, и сертифицированными средствами для сканирования данного типа Системы на предмет возможного наличия уязвимостей на этапе приемки, а также периодического анализа защищенности лицензированными, и сертифицированными средствами для сканирования данного типа Системы в процессе эксплуатации в рамках гарантийного периода;
- Исключить возможность несанкционированного доступа или воздействия на информационную систему Заказчика и обрабатываемую в ней информацию со стороны программно-аппаратных средств, каналов связи и интерфейсов, находящихся под контролем или используемых Подрядчиком.
- Для обеспечения разработки безопасного программного обеспечения руководствоваться мерами, предусмотренными разделами 4 и 5 ГОСТ Р 56939-2024.
- Для подключения к инфраструктуре руководствоваться регламентом предоставления доступа, представленным в Приложении №1 к техническому заданию.
- Ознакомить сотрудников Подрядчика с политикой защиты информации утвержденной Оператором в части, их касающейся.
- Выполнять требования политики защиты информации, утвержденной Оператором.

В ходе реализации требований к Системе в рамках настоящего Технического задания должно использоваться импортонезависимое программное обеспечение, включенное в реестр Российского программного обеспечения. Программное обеспечение, разрабатываемое в ходе реализации требований к Системе, должно быть произведено на территории Российской Федерации или быть включенным в Единый реестр российских программ для электронных вычислительных машин и баз данных.

В рамках Системы должен быть предусмотрен комплекс мероприятий по обеспечению информационной безопасности - защиты от несанкционированного доступа, нарушения целостности и достоверности хранящейся и передаваемой информации, должна быть обеспечена конфиденциальность информации.

Подрядчик не имеет права передавать третьим лицам информацию, полученную в процессе выполнения работ, и сведения о характере выполняемых работ, без согласования с Заказчиком. Данное требование не распространяется на лиц, которых Подрядчик привлекает к исполнению своих обязанностей.

Системе присвоен третий класс защищенности (КЗ).

В соответствии с [п.11](#) Постановления Правительства РФ от 01.11.2012 № 1119 «Об учреждении требований к защите персональных данных при их обработке в информационных системах персональных данных» при обработке ПДн в Системе обеспечен 4-й уровень защищенности персональных данных.

Развитие Системы (в рамках выполнения требований настоящего технического задания) осуществляется с учетом существующей Модели угроз безопасности информации, которая предоставляется Подрядчику Заказчиком.

Система должна удовлетворять одному из следующих требований:

- обеспечение функционирования на базе отечественной операционной системы, сертифицированной версии по 4-му уровню доверия в соответствии с «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020), включающей поддержку процессорных архитектур E2K и ARMv8;

- обеспечение совместимости со средствами защиты информации от несанкционированного доступа Dallas Lock и SecretNet актуальных версий и отечественными антивирусными средствами защиты информации. В подтверждение выполнения условия, Подрядчик в течение двух рабочих дней с даты заключения государственного контракта направляет Заказчику действительные сертификаты совместимости с используемой операционной системой.

Должны быть предусмотрены меры по защите Системы от компьютерных атак, направленных на отказ в обслуживании (DDos-атак).

- Использование кэширующих технологий: Кэширование статического контента, динамических страниц и результатов вычислений значительно сокращает необходимость обработки каждого отдельного запроса приложением.

- Обработка запросов с лимитом частоты обращений: Применение алгоритмов ограничения скорости (rate limiting). Например, ограничение количества запросов с одного IP адреса за определённый промежуток времени.

- Минимизация возможностей для перебора паролей: Увеличение сложности хеширования паролей и введение задержек между попытками входа при многократных неудачных попытках.

- Усиленная защита сессионных токенов, контроль сессий и предотвращение попыток обхода аутентификационных механизмов (использование JWT-токенов с короткими сроками действия)

- Использование специализированных методов доступа: система должна поддерживать взаимодействие через строго предопределённые виды запросов (представления, хранимые процедуры, запросы с использованием parameterized queries/prepared statements). Любые попытки отправки самостоятельных SQL-запросов или модификаций существующей структуры запроса должны блокироваться.

Подрядчик обязан оказать содействие при подключении Системы к системам мониторинга событий безопасности информации и централизованным средствам защиты информации, размещенным в ЦОД Электронного правительства Красноярского края.

Надежность информационного обеспечения Системы должна обеспечиваться совокупностью используемых средств управления базами данных, системой комплексного администрирования и реализацией механизмов резервного копирования информационных баз и файлов конфигурации.

Система должна обеспечивать хранение информации обо всех действиях пользователя (внесение, изменение, удаление и т.п.) в отношении объектов БД, а также должна обеспечивать возможность восстановления данных из резервных копий в случае возникновения сбоев и отказов. После сбоя серверной, клиентской операционных систем или СУБД в процессе выполнения пользовательских задач должно быть обеспечено восстановление данных в БД до состояния на момент окончания последней полностью завершенной перед сбоем операции ввода или изменения данных.

5.2 Требования к документированию

5.2.1 Состав и содержание документации

Спецификации форматов обмена данными с внешними системами должны быть разработаны на основе актуальной официальной документации, полученной с официальных порталов.

Подрядчик обязан разработать комплект эксплуатационной и технической документации на модернизированную Систему. Документация должна содержать полное и достаточное описание разработанных результатов работ для обеспечения возможности установки, настройки, эксплуатации, администрирования и дальнейшего развития Системы без привлечения Подрядчика.

В состав документации в обязательном порядке должны входить следующие документы:

- Руководство пользователя;
- Руководство администратора (при наличии изменений);
- Схема бизнес-процесса с указанием мест встраивания интеграции (на основе приложенной диаграммы, с уточнением новых действий).
- Программа и методика предварительных испытаний;
- Программа и методика опытной эксплуатации;
- Программа и методика приемочных испытаний.

Документация должна быть изложена ясным, понятным языком, снабжена иллюстрациями (при необходимости) и практическими примерами.

5.2.2 Порядок предоставления и согласования

Документация предоставляется Заказчику в следующем порядке:

- в 2 (двух) экземплярах на бумажном носителе, заверенных подписью и печатью уполномоченного лица Подрядчика;
- в 1 (одном) экземпляре в машиночитаемом формате (PDF) на электронном носителе.

Документация передается Заказчику с сопроводительным письмом, в котором указаны ее состав и объем.

Заказчик в срок не более 3 (трех) рабочих дней с момента получения документации проводит ее рассмотрение.

В случае выявления замечаний Заказчик в тот же срок направляет Подрядчику мотивированный перечень замечаний. Подрядчик обязан в срок не более 5 (пяти) рабочих дней

с момента получения замечаний устранить их и направить исправленную документацию Заказчику для окончательного утверждения.

5.3 Требования к патентной чистоте

Все проектные и технические решения Системы должны отвечать требованиям действующего законодательства Российской Федерации. Должны быть выполнены требования законов, в частности [части четвертой](#) Гражданского кодекса Российской Федерации. Система должна быть свободна от возможности предъявления любых прав и притязаний третьих лиц, основанных на промышленной, интеллектуальной или другой собственности. Выполнение требований по обеспечению лицензионной чистоты Системы должно обеспечиваться Подрядчиком.

При выполнении Работ по настоящему Техническому заданию Подрядчик должен гарантировать соблюдение авторских, исключительных и иных прав на объекты интеллектуальной собственности третьих лиц.

При использовании в Системе программ (программных комплексов или модулей), разработанных третьими лицами, условия, на которых передается право на использование (исполнение) этих программ, не должны накладывать ограничений, препятствующих использованию Системы по ее прямому назначению.

В случае использования при выполнении Работ по Контракту программ для электронных вычислительных машин (программных комплексов или компонентов), разработанных третьими лицами, условия, на которых передаются права на их использование (исполнение), должны обеспечить отсутствие ограничений, препятствующих использованию результатов работ по их назначению. При этом права, полученные Заказчиком, должны позволять ему передавать, дорабатывать, развивать результаты работ, созданные в процессе исполнения Контракта, осуществлять переработку программ для электронных вычислительных машин (программных комплексов или компонентов), разработанных ранее третьими лицами в соответствии с требованиями законодательства Российской Федерации.

6 Порядок контроля и приемки

В соответствии с [Постановлением](#) РФ от 06.07.2015 г. № 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» приёмка работ должна будет состоять из следующих мероприятий:

- а) разработка документации на ВИС ЕСН и её части
- б) адаптация программного обеспечения и разработка рабочей документации
- в) пусконаладочные работы
- г) проведение предварительных испытаний
- д) проведение опытной эксплуатации системы
- е) проведение приемочных испытаний

По факту выполнения работ в течение 3 рабочих дней Исполнитель формирует, подписывает и размещает в единой информационной системе в сфере закупок документ о приемке в соответствии с ч.13 ст.94 [Закона № 44-ФЗ](#).

Заказчик осуществляет приемку всех оказанных работ, включая оформление результатов приемки, в течение 20 рабочих дней, следующих за днем поступления Заказчику подписанного Исполнителем документа о приемке в соответствии с ч.13 ст.94 [Закона № 44-ФЗ](#).

Для проверки предоставленных Исполнителем результатов, предусмотренных Контрактом, в части их соответствия условиям Контракта Заказчик проводит экспертизу. Экспертиза результатов оказанных работ может проводиться Заказчиком своими силами или к ее проведению могут привлекаться эксперты, экспертные организации на основании контрактов, заключенных в соответствии с [Законом № 44-ФЗ](#).

6.1 Требования к разработке документации

Разработка документации на Систему и ее части осуществляется в рамках этапа разработки документации и должна включать создание и утверждение технической документации в объеме, необходимом для описания полной совокупности проектных решений (в том числе по защите информации) и достаточном для дальнейшего выполнения работ по развитию системы.

Процесс разработки документации включает:

- разработку Исполнителем проектов документов согласно составу, определенному в пункте 5.2.1 настоящего ТЗ;
- утверждение документов Заказчиком;
- передачу окончательных версий документов Заказчику в порядке и сроки, установленные пунктом 5.2.2 настоящего ТЗ.

Документация должна быть разработана с учетом действующих нормативно-методических документов в области разработки и оформления конструкторской, программной и эксплуатационной документации.

6.2 Требования к адаптации программного обеспечения

Адаптация программного обеспечения включает разработку программного обеспечения Системы, выбор и адаптацию приобретаемого программного обеспечения, а также в установленных случаях и порядке сертификацию разработанного программного обеспечения системы и средств защиты информации по требованиям безопасности.

Требования к Системе в целом:

- Подсистемы должны быть адаптированы под интеграцию с ГИС ЕГРН.
- Система должна обеспечивать стабильную работу при численности персонала более 150 человек.
- В Системе должен быть единообразный интерфейс, интуитивно понятный для пользователя системы.
- Система должна отвечать требованиям по патентной чистоте согласно действующему законодательству Российской Федерации.

6.3 Требования к пусконаладочным работам

В рамках проведения пусконаладочных работ должна быть осуществлена автономная наладка технических средств и программного обеспечения частей Системы:

- установка и настройка компонентов технического обеспечения (при необходимости);
- установка и настройка серверных компонентов ВИС «Енисей-Стройнадзор» (при необходимости);
- установка и настройка ВИС «Енисей-Стройнадзор» на серверном оборудовании объекта автоматизации, включая настройку механизмов, протоколов и форматов взаимодействия с внешними системами, настройку автоматизируемых процессов.

6.4 Предварительные испытания

Предварительные испытания включают в себя:

а) разработку Исполнителем для Системы программы и методики предварительных испытаний, в соответствии с которыми осуществляется проверка системы на работоспособность и соответствие техническому заданию;

б) проверку Заказчиком системы на работоспособность и соответствие настоящему ТЗ на их развитие (для чего Исполнитель предоставляет Заказчику демонстрационный доступ к модулю Системы);

в) устранение Исполнителем выявленных при проведении таких испытаний неисправностей и внесение им изменений в рабочую документацию на Систему;

г) оформление Исполнителем и подписание проекта протокола испытаний и акта о приемке системы в опытную эксплуатацию.

д) проведение Заказчиком сканирования уязвимостей и угроз безопасности информации, техническими средствами ЦОД Электронного правительства Красноярского края. Выявленные уязвимости критического и высокого уровня (в соответствии с терминологией регламента включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России от 26 июня 2018 г.) должны быть устранены до момента итоговой приемки работ по государственному контракту.

6.5 Опытная эксплуатация

Опытная эксплуатация включает в себя:

а) разработку Исполнителем для системы программы и методики опытной эксплуатации;

б) совместную (Исполнителем и Заказчиком) опытную эксплуатацию системы в соответствии с программой и методикой опытной эксплуатации;

в) доработку программного обеспечения систем и дополнительную наладку технических средств в случае обнаружения недостатков, выявленных при опытной эксплуатации системы (действия осуществляются Исполнителем);

г) оформление Исполнителем и подписание проекта акта о завершении опытной эксплуатации, включающего перечень недостатков, которые необходимо устранить до начала эксплуатации системы.

д) проведение сканирования уязвимостей и угроз безопасности информации, техническими средствами ЦОД Электронного правительства Красноярского края. Выявленные уязвимости критического и высокого уровня (в соответствии с терминологией регламента включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России от 26 июня 2018 г.) должны быть устранены до момента итоговой приемки работ по государственному контракту.

6.6 Приёмочные испытания

Приёмочные испытания включают в себя:

а) разработку Исполнителем для системы программы и методики приемочных испытаний;

б) испытания системы на соответствие настоящему техническому заданию в соответствии с программой и методикой приемочных испытаний;

в) анализ и устранение недостатков, указанных в акте о завершении опытной эксплуатации;

г) оформление Исполнителем и подписание Сторонами акта о приемке системы в эксплуатацию и акта сдачи-приемки выполненных работ.

д) проведение сканирования уязвимостей и угроз безопасности информации, техническими средствами ЦОД Электронного правительства Красноярского края. Выявленные уязвимости критического и высокого уровня (в соответствии с терминологией регламента включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России от 26 июня 2018 г.) должны быть устранены до момента итоговой приемки работ по государственному контракту.

Порядок предоставления удаленного доступа к ресурсам.

1. Предоставление, изменение, прекращение прав доступа Подрядчика к защищаемым ресурсам Заказчика.

1.1. До начала выполнения Работ, для предоставления доступа к защищенным ресурсам Заказчика, Подрядчик должен подтвердить соответствие требованиям о реализации мер по защите от угроз через информационную инфраструктуру Подрядчика. Для подтверждения реализации указанных мер Подрядчик в течение 5 (пяти) рабочих дней с момента начала выполнения Работ должен направить на электронный адрес mcr@digital.krskstate.ru заполненную форму в соответствии с Приложением 4 к настоящему порядку за подписью руководителя Подрядчика.

1.2. Заказчик в соответствии с настоящим порядком предоставляет Подрядчику доступ к своим защищаемым ресурсам в целях исполнения обязательств по Контракту.

1.3. Подрядчик должен иметь права доступа только к тем защищаемым ресурсам Заказчика, доступ к которым ему необходим для исполнения обязательств по Контракту.

1.4. До начала выполнения Работ Заказчик и Подрядчик согласуют и утверждают состав защищаемых ресурсов, доступ к которым Заказчик предоставляет Подрядчику в целях исполнения обязательств по Контракту, в соответствии с Приложением № 1 «Перечень защищаемых ресурсов» к настоящему порядку.

1.5. Подрядчик не вправе требовать от Заказчика предоставления доступа к иным защищаемым ресурсам, не включенным в утвержденный перечень.

1.6. Для получения прав доступа к защищаемым ресурсам Подрядчик обязан в течение 5 (пяти) рабочих дней с момента начала выполнения Работ направить Заказчику заполненную заявку в соответствии с Приложением № 2 «Заявка на предоставление прав доступа к защищаемым ресурсам» к настоящему порядку, в которой должны быть указаны следующие сведения:

- Ф.И.О. и должности специалистов Подрядчика (далее – Привилегированный пользователи);
- перечень защищаемых ресурсов, к которым Подрядчику необходим доступ для выполнения обязательств по Контракту;
- перечень запрашиваемых прав доступа: протоколы и подпротоколы доступа, нестандартные ТСР-порты доступа, либо перечень приложений (сервисов);
- планируемый график работы с защищаемыми ресурсами (с указанием времени и дней недели. Круглосуточный режим предоставления доступа к защищенным ресурсам не предоставляется.);
- необходимость наличия возможности доступа вне согласованного графика работы (в случае аварийных/внештатных ситуаций);
- дополнительные сведения об особенностях удалённой работы.

1.7. Заказчик в течение 5 (пяти) рабочих дней с момента получения заявки от Подрядчика согласует её и, в случае принятия положительного решения, предоставляет Подрядчику реквизиты доступа (логин и временный пароль).

1.8. В случае принятия отрицательного решения, Заказчик возвращает заявку Подрядчику с соответствующей резолюцией, содержащей мотивированный отказ.

1.9. Подрядчик после получения доступа, в течение 2 (двух) рабочих дней уведомляет Заказчика на электронный адрес mcr@digital.krskstate.ru о готовности к выполнению Работ по Контракту, либо об обстоятельствах, препятствующих дальнейшему выполнению Работ. В случае отсутствия от Подрядчика уведомления в указанный срок, считается, что на текущий момент обстоятельства, препятствующие выполнению Работ, отсутствуют и Подрядчик приступил к работам в соответствии с Контрактом.

1.10. После первого входа в систему Привилегированный пользователь обязан заменить временный пароль на постоянный.

1.11. При необходимости внесения изменений в перечень допущенных лиц или запрошенных прав доступа Подрядчик обязан своевременно уведомить Заказчика и при

необходимости направить новую заявку в соответствии с Приложением № 2 «Заявка на предоставление прав доступа к защищаемым ресурсам» к настоящему порядку.

1.12. Отзыв и блокирование прав доступа Подрядчика к защищаемым ресурсам Заказчика могут производиться в следующих случаях:

- инфраструктура Подрядчика не соответствует требованиям о реализации мер по защите от угроз через информационную инфраструктуру Подрядчика;
- прекращение контрактных обязательств, в рамках которых Подрядчику предоставлялся доступ к защищаемым ресурсам Заказчика;
- выявление нарушений со стороны Подрядчика в рамках процесса управления инцидентами информационной безопасности или в ходе проведения аудитов информационной безопасности.

2. Доступ Подрядчика к защищаемым ресурсам Заказчика осуществляется с использованием криптографических средств защиты информации, принадлежащих Заказчику.

2.1. В качестве криптографических средств защиты информации используются программные компоненты производства общества с ограниченной ответственностью «Код Безопасности», в частности продукт средство криптографической защиты информации «Континент-АП» (далее – VPN-клиент).

2.2. Для получения сертификатов VPN-клиента в соответствии с регламентом подключения к защищенной сети передачи данных Электронного правительства Красноярского края (размещенном в сети Интернет по адресу <https://www.krskcit.ru/upload/iblock/173/1736ad76ee483229f77d67121ce65071.pdf>), Подрядчик обязан в течение 5 (пяти) рабочих дней с момента начала выполнения Работы направить Заказчику заполненную заявку в соответствии с Приложением № 3 «Заявление на предоставлении доступа к информационным ресурсам, размещенным в Центре обработки данных (ЦОД) краевого государственного казенного учреждения «Центр Информационных Технологий Красноярского края» через ЗСПД» к настоящему порядку в формате *.doc на адрес электронной почты info@krskcit.ru.

2.3. Заявка для получения сертификата оформляется органом власти, являющимся заказчиком на выполнение работ по развитию Системы или оператором Системы.

2.4. При установке VPN-клиента Подрядчик получает от Оператора системы ключевую информацию, необходимую для организации защищенного доступа.

2.5. Подрядчик имеет право запрашивать у Оператора системы актуальную версию VPN-клиента.

2.6. Подрядчик обязан обеспечить установку предоставленного VPN-клиента на собственном оборудовании и вычислительных ресурсов с использованием которых, планирует осуществлять доступ к защищаемым ресурсам, в том числе путем закупки за счет собственных средств дополнительного программного обеспечения.

2.7. При необходимости перевыпуска сертификата VPN-клиента Подрядчик направляет новую заявку в соответствии с Приложением № 3 «Заявление на предоставлении доступа к информационным ресурсам, размещенным в Центре обработки данных (ЦОД) краевого государственного казенного учреждения «Центр Информационных Технологий Красноярского края» через ЗСПД» к настоящему порядку в формате *.doc на адрес электронной почты info@krskcit.ru.

3. Осуществление и прекращение доступа Привилегированных пользователей к защищаемым ресурсам.

3.1. Привилегированные пользователи осуществляют доступ к защищаемым ресурсам Заказчика только посредством специализированной системы контроля действий привилегированных пользователей в соответствии с порядком, определенным в Приложении № 5 «Порядок осуществления доступа привилегированных пользователей к защищаемым ресурсам Заказчика» к настоящему порядку.

3.2. Для работы с защищаемым ресурсом Привилегированный пользователь проходит авторизацию в СКДПП и получает доступ к перечню ресурсов, который был согласован и утверждён на этапе предоставления ему расширенных прав доступа (в соответствии с п. 4 настоящего порядка).

3.3. Привилегированный пользователь может беспрепятственно осуществлять работу с защищаемыми ресурсами, доступными для него в СКДПП, в соответствии с графиком и правами, которые были ему согласованы на этапе предоставления расширенных прав доступа (в соответствии с п. 4 настоящего порядка).

3.4. В случае возникновения внештатных (аварийных) ситуаций или необходимости проведения внеплановых работ с защищаемым ресурсом вне согласованного графика, Привилегированный пользователь может получить необходимые права доступа посредством процедуры согласования, реализованной в СКДПП. Для этого Привилегированный пользователь подключается к защищаемому ресурсу, где ему предлагается сформировать запрос на предоставление доступа.

3.5. При формировании запроса на предоставление доступа Привилегированному пользователю необходимо указать основание и планируемую длительность проведения работ (рекомендуется указывать длительность с запасом).

3.6. Подрядчик после формирования запроса уведомляет Заказчика по телефону 8 (391) 263-10-20 о необходимости предоставления доступа для проведения внеплановых работ с защищаемым ресурсом вне согласованного графика.

3.7. Данный запрос проходит процедуру согласования Заказчиком, по результатам которой Привилегированному пользователю предоставляется запрошенный доступ к защищаемому ресурсу на согласованный период времени или приходит уведомление, что в запрашиваемом доступе отказано.

3.8. В случае, если Привилегированному пользователю требуется дополнительное время для работы с защищаемым ресурсом, он формирует повторный запрос на согласование доступа в соответствии с процедурой, описанной выше (п. 3.5-3.6).

3.9. В процессе осуществления доступа Привилегированного пользователя к защищаемому ресурсу Заказчик производит контроль его действий посредством методов, реализованных в СКДПП (в соответствии с п. 4 настоящего порядка).

3.10. Прекращение доступа Привилегированного пользователя к защищаемому ресурсу может происходить в следующих случаях:

- окончание рабочего времени в соответствии с утверждённым графиком работ;
- окончание запрошенного периода времени в соответствии с согласованным запросом на предоставление доступа;
- по решению Заказчика в случае выявления инцидента информационной безопасности (в случае неправомерных действий Привилегированного пользователя, которые могут привести к возникновению негативных последствий).

3.11. Прекращение доступа Привилегированного пользователя к защищаемому ресурсу осуществляется путём разрыва рабочей сессии.

4. Контроль действий Подрядчика в рамках осуществления доступа к защищаемым ресурсам Заказчика.

4.1. Заказчик осуществляет контроль действий Подрядчика в рамках осуществления доступа к защищаемым ресурсам посредством СКДПП. Управление СКДПП и настройка её компонентов осуществляется на основании установленной Заказчиком политики информационной безопасности.

4.2. Заказчик реализует процесс контроля действий Подрядчика в рамках осуществления доступа к защищаемым ресурсам Заказчика путём организации следующих мероприятий:

- идентификация и аутентификация Привилегированных пользователей Подрядчика;
- управление и контроль доступа Привилегированных пользователей Подрядчика к защищаемым ресурсам;
- запись рабочих сеансов Привилегированных пользователей Подрядчика;
- мониторинг действий Привилегированных пользователей Подрядчика;
- формирование статистических отчётов по действиям Привилегированных пользователей Подрядчика;

- управление компонентами СКДПП;
- протоколирование работы СКДПП и просмотр журналов;
- контроль целостности компонентов СКДПП.

ПЕРЕЧЕНЬ ЗАЩИЩАЕМЫХ РЕСУРСОВ

№	№	Наименование защищаемого ресурса	Характеристики
	1	2	3

ЗАЯВКА НА ПРЕДОСТАВЛЕНИЕ ПРАВ ДОСТУПА К ЗАЩИЩАЕМЫМ РЕСУРСАМ

№	ФИО	Должность	Запрашиваемые ресурсы, к которым необходим доступ	Запрашиваемые права доступа	График работы с защищаемыми ресурсами	Необходима ли процедура согласования доступа	e-mail + Дополнительные сведения
1	2	3	4	5	6	7	8
1	Иванов Иван Иванович	должность	Наименование ресурса 1	Протоколы подключения (RDP/SSH)	08:00-18:00 пн-пт	да	e-mail Особенности работы
			Наименование ресурса 2	Протоколы подключения (RDP/SSH)	08:00-18:00 пн-пт	нет	
			Наименование ресурса 3	Протоколы подключения (RDP/SSH)	08:00-18:00 пн-пт	да	

Столбец 5 – Указывается протокол для работы (пример RDP. SSH)

Столбец 7 – Согласование доступа необходимо для работ с защищенным ресурсом, в нерабочем времени. В случае ответа «ДА» необходимо при заходе на сервер осуществить связь с техподдержкой КГКУ «ЦИТ» для согласования начала и окончания работы.

Заявление

предоставлении доступа к информационным ресурсам, размещенным в Центре обработки данных краевого государственного казенного учреждения «Центр информационных технологий Красноярского края» через ЗСПД

1.	Данные о подрядной организации	
1.1.	Наименование подрядной организации	
1.2.	ОГРН подрядной организации	
1.3.	№ контракта	
1.4.	Срок действия контракта	
2.	Подключение к ЗСПД с применением СКЗИ «Континент-АП» (для нового пользователя)	
2.1.	Наименование информационных ресурсов(с указанием IP адресов, портов), доступ к которым необходим через ЗСПД	
2.2.	Предполагаемое количество АРМов, с которых планируется подключение пользователей к ресурсам ЗСПД, с учетом их территориального распределения	
Данные о сотруднике, на кого необходимо выпустить сертификат		
2.3.	2 ФИО	
2.4.	Должность	
2.5.	Номер телефона	
2.6.	Адрес электронной почты	
2.7.	Фактический адрес подключения	
2.8.	Информационные ресурсы для этого сотрудника (помимо основных)	
3.	Требуется перевыпуск сертификата на СКЗИ «Континент-АП»	
Данные о сотруднике, у кого есть сертификат, но его необходимо перевыпустить		
3.1.	ФИО	
3.2.	Должность	
3.3.	Номер телефона	
3.4.	Адрес электронной почты	
3.5.	Причина перевыпуска сертификата	1. Окончание срока действия текущего сертификата; 2. Компрометация текущего сертификата; 3. Изменение в данных пользователя

4.	Подключение к новому ресурсу, через ЗСПД с применением СКЗИ «Континент-АП»	
4.1.	Наименование информационных ресурсов(с указанием IP адресов, портов), доступ к которым необходим через ЗСПД	
Данные о сотруднике, у кого есть сертификат и необходимо предоставить доступ до новых ресурсов		
4.2.	ФИО	
4.3.	Должность	
4.4.	Номер телефона	
4.5.	Адрес электронной почты	
4.6.	Информационные ресурсы для этого сотрудника (помимо основных)	

**Меры по защите от угроз через информационную инфраструктуру
Администратора системы**

Обозначение и номер меры	Меры обеспечения безопасности	Реализация меры (каким образом это реализовано + регламентирующий документ)
	II. Управление доступом (УПД)	
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	
	IV. Защита машинных носителей информации (ЗНИ)	
ЗНИ.1	Учет машинных носителей информации	
ЗНИ.2	Управление доступом к машинным носителям информации	
	V. Регистрация событий безопасности (РСБ)	
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	
	VI. Антивирусная защита (АВЗ)	
АВЗ.1	Реализация антивирусной защиты	
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	
	VIII. Контроль (анализ) защищенности информации (АНЗ)	
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	
	XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)	

Обозначение и номер меры	Меры обеспечения безопасности	Реализация меры (каким образом это реализовано + регламентирующий документ)
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	

Порядок осуществления доступа Привилегированных пользователей к защищаемым ресурсам Оператора системы

1. Подключение для смены пароля, адреса электронной почты и просмотра своих прошлых подключений:

Запуск веб-браузера:

а) <https://192.168.151.130/>

2. Подключение для консольных сессий (SSH, SFTP, SCP):

Запуск клиента SSH:

а) Подключение к СКДПУ «Бастион» по SSH – 192.168.151.130 / порт 22

б) Подключение к целевому устройству посредством интерактивного логина и протокола SCP – `Interactive@hostname:SSH:username?lp`

3. Подключение для графических сессий:

Запуск клиента RDP:

а) Подключение к СКДПУ «Бастион» по RDP – 192.168.151.130 / порт 3389