

«Региональная навигационно-информационная система Пермского края на
базе технологий ГЛОНАСС и ГЛОНАСС/GPS»

РНИС ПК

**Техническое задание
на выполнение работ по развитию «Региональная навигационно-
информационная система Пермского края на базе технологий
ГЛОНАСС и ГЛОНАСС/GPS»**

Пермь
2026

Содержание

1	Общие сведения.....	4
1.1	Полное наименование Системы и ее условное обозначение.....	4
1.2	Наименование работ.....	4
1.3	Государственный заказчик.....	4
1.4	Подрядчик.....	4
1.5	Сроки выполнения работ.....	4
1.6	Источник финансирования.....	4
1.7	Порядок оформления и предъявления Заказчику результатов работ.....	5
1.8	Порядок внесения изменений и дополнений.....	6
1.9	Перечень документов, методических материалов, регламентирующих развитие Системы.....	6
1.10	Перечень терминов, сокращений и обозначений.....	9
2	Цели и назначение развития Системы.....	12
2.1	Цели и задачи развития Системы.....	12
2.2	Назначение Системы.....	12
3	Характеристика объекта автоматизации.....	14
3.1	Основные сведения об объекте автоматизации.....	14
3.2	Сведения об условиях эксплуатации объекта автоматизации и характеристиках окружающей среды.....	14
3.3	Перечень функций, реализуемых Системой.....	14
3.4	Общие принципы развития Системы.....	17
3.5	Взаимодействие с иными информационными системами.....	19
3.6	Структура Системы и назначение ее частей.....	19
3.7	Программно-аппаратное обеспечение Системы.....	24
3.8	Сведения о ранее исполненных контрактах.....	27
4	Требования к Системе.....	28
4.1	Требования к способам и средствам связи для информационного обмена между компонентами Системы.....	28
4.2	Требования к характеристикам взаимосвязей Системы с иными информационными системами.....	28
4.3	Требования к функциям (задачам), реализуемым в рамках выполнения работ.....	29
4.3.1	Требования к оптимизации работоспособности программного обеспечения Системы.....	29
4.3.2	Требования к разработке подсистемы «Информационная система обеспечения мониторинга отходов строительства и сноса».....	30
4.4	Общие технические требования к Системе.....	39
4.4.1	Требования к функционированию системы.....	39
4.4.2	Требования к численности и квалификации персонала Системы и режиму его работы.....	41
4.4.3	Показатели назначения.....	42
4.4.4	Требования к надежности.....	43
4.4.5	Требования к безопасности.....	44
4.4.6	Требования к эргономике и технической эстетике.....	45
4.4.7	Требования к защите информации от несанкционированного доступа.....	46
4.4.8	Требования по сохранности информации при авариях.....	51

4.4.9	Требования к патентной чистоте.....	52
4.4.10	Требования по стандартизации и унификации.....	55
4.5	Требования к видам обеспечения.....	56
4.5.1	Требования к информационному обеспечению.....	56
4.5.2	Требования к лингвистическому обеспечению.....	56
4.5.3	Требования к программному обеспечению.....	56
4.5.4	Требования к техническому обеспечению.....	57
4.5.5	Требования к организационному обеспечению.....	58
5	Состав и содержание работ по развитию системы.....	59
5.1	Этапы выполнения работ.....	59
6	Порядок развития системы.....	65
6.1	Требования к разработке документации.....	65
6.2	Требования к разработке программного обеспечения и рабочей документации.....	66
6.3	Требования к проведению пусконаладочных работ и предварительных испытаний Системы.....	68
6.4	Требования к проведению опытной эксплуатации.....	70
6.5	Требования к проведению пусконаладочных работ и приемочных испытаний.....	72
6.6	Требования к проведению работ по защите информации.....	74
6.6.1	Требования к определению класса защищенности, уровня защищенности персональных данных и оценки вреда.....	77
6.6.2	Требования к актуализации модели угроз.....	78
6.6.3	Требования к актуализации частного технического задания на систему защиты информации.....	81
6.6.4	Требования к актуализации проектной документации на систему защиты информации.....	82
6.6.5	Требования к актуализации эксплуатационной документации на систему защиты информации.....	87
6.6.6	Требования к предоставлению прав использования СЗИ и/или СКЗИ.....	88
6.6.7	Требования к установке и настройке СЗИ и/или СКЗИ.....	88
6.6.8	Требования к проведению аттестационных испытаний информационной системы.....	89
7	Порядок контроля и приемки выполненных работ.....	98
7.1	Общие требования к приемке работ.....	98
7.2	Виды, состав, объем и методы испытаний Системы и ее составных частей.....	98
7.3	Порядок выполнения доработок и устранение допущенных Подрядчиком ошибок, которые выявлены в процессе испытаний и в период гарантийного обслуживания.....	100
8	Сведения о гарантийном обслуживании Системы.....	102
9	Требования к документированию.....	104
	Приложение А Правила присвоения номеров отчетной документации.....	106
	Приложение Б Форма документа «Ведомость передаваемых файлов».....	108

1 Общие сведения

1.1 Полное наименование Системы и ее условное обозначение

«Региональная навигационно-информационная система Пермского края на базе технологий ГЛОНАСС и ГЛОНАСС/GPS» (далее – Система, РНИС ПК).

1.2 Наименование работ

Полное наименование работ: Выполнение работ по развитию «Региональная навигационно-информационная система Пермского края на базе технологий ГЛОНАСС и ГЛОНАСС/GPS» (далее – Система, РНИС ПК).

Краткое наименование работ: Выполнение работ по развитию РНИС ПК (далее - выполнение работ)

1.3 Государственный заказчик

Государственный заказчик (далее – Заказчик) – Министерство информационного развития и связи Пермского края.

Место нахождения: 614000, Пермский край, г. Пермь, ул. Ленина, д. 66.

Почтовый адрес: 614000, Пермский край, г. Пермь, ул. Ленина, д. 66.

1.4 Подрядчик

Подрядчик определяется по результатам проведения конкурентной процедуры в соответствии с Федеральным законом от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

1.5 Сроки выполнения работ

Сроки выполнения работ в разрезе этапов указаны в п. 5.1 настоящего Технического задания.

1.6 Источник финансирования

Источником финансирования выполнения работ является бюджет Пермского края

Порядок финансирования определяется условиями ГК.

1.7 Порядок оформления и предъявления Заказчику результатов работ

Результаты выполнения работ должны передаваться Заказчику в порядке, определенном в заключаемом по результатам конкурентной процедуры ГК, в соответствии с требованиями к срокам начала и окончания выполнения работ, установленными в ТЗ. Требования к составу и оформлению предъявляемых Заказчику результатов работ определены в разделах 5 и 9 настоящего ТЗ.

При передаче Заказчику программ для ЭВМ, созданных в рамках выполнения работ в виде объектного кода, Подрядчик должен передать Заказчику дистрибутивы и исходные тексты (коды) указанных программ для ЭВМ в электронном виде через Систему управления репозиториями кода Государственного Заказчика (далее – СУРК. Созданные в рамках выполнения работ по ГК базы данных передаются Подрядчиком Заказчику в электронном виде через СУРК.

Отчетная документация передается в соответствии с п.5.1 на бумажных носителях (два экземпляра – по одному экземпляру для каждой стороны ГК) и через СУРК. Текстовые документы в электронном виде должны быть представлены в форматах, позволяющих осуществить их просмотр средствами OpenOffice.

Все материалы за каждый этап и по итогам выполнения работ по ГК передаются Заказчику с сопроводительными документами Подрядчика в соответствии с условиями ГК.

Заказчик производит проверку результатов работ и представленной отчетной документации в порядке, предусмотренном ГК и ТЗ.

Объем передаваемых материалов (при необходимости) может быть описан в документе «Ведомость передаваемых файлов» (шаблон документа представлен в приложении Б к настоящему документу).

В случае если при проверке установлены неактуальность, противоречивость, недостоверность, несоответствие требованиям ГК, ТЗ, либо неполнота сведений, представленных в отчетной документации, Заказчик в порядке, определенном ГК, возвращает Подрядчику отчетную документацию на доработку с указанием причин отказа в приемке отчетной документации. В этом случае приемка отчетной документации откладывается в порядке, определенном ГК, до момента полного устранения замечаний Заказчика по представленной отчетной документации.

1.8 Порядок внесения изменений и дополнений

Изменения настоящего ТЗ не предусмотрены. Дополнительные, детализирующие требования и уточнения могут быть предъявлены в составе Частного технического задания (далее – ЧТЗ).

При выявлении случаев нецелесообразности или невозможности реализации требований настоящего ТЗ Подрядчик должен предложить, согласовать с Заказчиком и реализовать другое более эффективное решение, а также отразить этот факт в отчетной документации. При этом, предлагаемое решение не должно противоречить основным требованиям данного ТЗ и приводить к существенному изменению объема работ и иных существенных условий, предусмотренных ГК.

1.9 Перечень документов, методических материалов, регламентирующих развитие Системы

Выполняемая работа должна отвечать требованиям нормативных правовых актов, а также соответствующих государственных стандартов:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Постановление Правительства Российской Федерации от 6 июля 2015 г. № 675 «О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона «Об информации, информационных технологиях и о защите информации».
3. Постановление Правительства Российской Федерации от 6 июля 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».
4. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
5. Приказ ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении Требований по защите информации, содержащейся в государственных информационных системах и иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

6. Приказ ФСБ России от 10 июля 2014 г. № 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»;

7. Методический документ «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 5 февраля 2021 г.

8. Постановление Правительства Пермского края от 3 февраля 2014 г. № 56-п «Об обеспечении предоставления государственных и муниципальных услуг (исполнения функций) в электронной форме на территории Пермского края».

9. Постановление Правительства Пермского края от 25 сентября 2013 г. № 1270-п «Об утверждении государственной программы Пермского края «Развитие информационного общества».

10. Закон Пермского края от 25 декабря 2009 г. № 569-ПК «Об управлении и распоряжении интеллектуальной собственностью Пермского края».

11. Указ губернатора Пермского края от 11 апреля 2017 г. № 53 «О централизации функций в сфере региональной информатизации и использования информационно-коммуникационных технологий в Пермском крае».

12. Указ губернатора Пермского края от 28 декабря 2017 г. № 165 «Об утверждении Порядка взаимодействия исполнительных органов государственной власти Пермского края, Администрации губернатора Пермского края, подведомственных им учреждений при осуществлении функций в сфере региональной информатизации и использования информационно-коммуникационных технологий в Пермском крае и внесение изменений в Указ губернатора Пермского края 11 апреля 2017 г. № 53 «О централизации функций в сфере региональной информатизации и использования информационно-коммуникационных технологий в Пермском крае».

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

14. ГОСТ Р 57100-2025 «Системная и программная инженерия. Описание архитектуры»

15. ГОСТ Р 56939-2024. «Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования».

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

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

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

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

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

21. ГОСТ Р 2.105-2019 «Единая система конструкторской документации. Общие требования к текстовым документам».

22. ГОСТ Р 71784-2024 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортировка, хранение».

23. СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания».

24. Постановление Главного государственного санитарного врача Российской Федерации от 2 декабря 2020 г. № 40 «Об утверждении санитарных правил СП 2.2.3670-20 «Санитарно-эпидемиологические требования к условиям труда».

Перечисленный выше перечень документов не является исчерпывающим. К выполнению работ предъявляются иные требования, предусмотренные применимыми нормативными правовыми актами, методическими документами, положения которых учитываются при выполнении работ в рамках настоящего ТЗ.

В случае внесения изменений, признания утратившими силу нормативных правовых актов, методических документов, предусмотренных настоящим разделом, положения указанных актов применяются с даты вступления в силу указанных документов и распространяются на выполнение работ по ГК. Положения нормативных правовых актов, методических документов, принятых взамен признанных утратившими силу документов, предусмотренных настоящим разделом, распространяются на выполнение работ по ГК.

1.10 Перечень терминов, сокращений и обозначений

Перечень используемых в настоящем документе терминов и сокращений представлен в таблице ниже (Таблица 1).

Таблица 1 – Перечень терминов, сокращений и обозначений

Термин, сокращение, обозначение	Определение
EGTS	Era GLONASS Telematics Standard – это протокол для передачи телеметрических данных, который законодательно закреплён на территории Российской Федерации
HTTP	HyperText Transfer Protocol – это протокол передачи гипертекста
REST	Representational State Transfer – это архитектурный стиль взаимодействия компонентов распределённого приложения в сети
RMI	Remote Method Invocation – это программный интерфейс вызова удалённых методов в языке Java
SOAP	Simple Object Access Protocol - это протокол обмена сообщениями в виде XML
БНСО	Бортовое навигационно-связное оборудование
ВИС	Внешняя информационная система
ВМ	Виртуальная машина
ГК	Государственный контракт
ГОСТ	Государственный стандарт
АТП	Автотранспортное предприятие
Государственный заказчик	Министерство информационного развития и связи Пермского края

Термин, сокращение, обозначение	Определение
ГРЗ	Регистрационные знаки транспортных средств в России
ЕИС	Единая информационная система в сфере закупок
ЕПУТС ПГА	Единая платформа управления транспортной системой Пермской городской агломерации
ЕХД ПК	Единое хранилище данных Пермского края
ИС	Информационная система
ИТС	Интеллектуальная транспортная система
КТС	Комплекс технических средств
НСД	Несанкционированный доступ
НСИ	Нормативно-справочная информация
ОГВ ПК	Органы государственной власти Пермского края ¹
ОП	Остановочный пункт
Оператор Системы	Организация, осуществляющая деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных
ОС	Операционная система
ПМД	Подсистема мониторинга и диагностики
ПО	Программное обеспечение
РСАА ПК	Региональный сервис аутентификации и авторизации сотрудников органов государственной власти и учреждений Пермского края
РФ	Российская Федерация
СЗИ	Средство защиты информации
Система, РНИС ПК	«Региональная навигационно-информационная система Пермского края на базе технологий ГЛОНАСС и ГЛОНАСС/GPS»
СКЗИ	Средство криптографической защиты информации
СПО	Специальное программное обеспечение Системы, перерабатываемое в рамках ГК
СУБД	Система управления базами данных
СУРК, репозиторий	Система управления репозиториями кода
ТЗ	Техническое задание
ТКО	Твёрдые коммунальные отходы
ТС	Транспортное средство
ФЗ	Федеральный закон
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

¹Законодательный орган государственной власти Пермского края; высшее должностное лицо Пермского края; высший исполнительный орган государственной власти Пермского края и исполнительные органы государственной власти Пермского края, включенные в систему исполнительных органов государственной власти Пермского края; образованные в Пермском крае судебные органы; иные органы государственной власти Пермского края, образуемые в соответствии с Уставом Пермского края.].

Термин, сокращение, обозначение	Определение
ЦОД ППК	Центр обработки данных Правительства Пермского края
ЧТЗ	Частное техническое задание
ЭВМ	Электронная вычислительная машина
ЭП	Электронная подпись

2 Цели и назначение развития Системы

2.1 Цели и задачи развития Системы

Целью выполнения работ по развитию Системы является расширение функциональных возможностей Системы.

Задачи по развитию Системы могут быть решены путем:

- модернизации существующих подсистем и модулей Системы;
- работ по обеспечению взаимодействия с иными информационными системами

Основанием для развития Системы являются, в том числе:

- изменения действующих нормативно-правовых актов Российской Федерации и Пермского края в сфере деятельности объекта автоматизации, влекущие необходимость реализации новой или модернизацию существующей функциональности;
- наличие новых целевых задач, определенных Заказчиком, включая необходимость использования накопленных данных во внешних информационных системах и ресурсах;
- изменения, произошедшие в информационных системах, с которыми осуществляется интеграция Системы;
- наличие потребностей, замечаний пользователей Системы к пользовательским интерфейсам и/или функциональности Системы.

2.2 Назначение Системы

Система предназначена для создания единого технологического и информационного пространства, обеспечивающего возможность проведения объективного анализа предметной деятельности с помощью различных инструментов, подходов и методов обработки как структурированных, так и неструктурированных данных:

1. информационно-навигационного обеспечения деятельности автомобильного транспорта, в том числе городского наземного электрического транспорта, на территории Пермского края с использованием технологий ГЛОНАСС или ГЛОНАСС/GPS;

2. обеспечения безопасности и эффективности функционирования транспортного комплекса Пермского края;
3. сбора, обработки, хранения и предоставления навигационных данных в режиме реального времени;
4. создания и ведения базы актуальных данных объектов транспортной инфраструктуры;
5. импорта информации (ТС, БНСО, пользователи (водители, диспетчеры), маршруты расписания из ведомственных систем Функционального заказчика) посредством WebAPI;
6. обеспечения сгенерированных план-нарядов транспортными средствами и водителями;
7. ведения реестров контрактов (договоров) предприятий-подрядчиков, маршрутов и расписаний маршрутной сети регулярных пассажирских перевозок региона;
8. контроля режимов работы исполнительных механизмов дорожной техники (при наличии технических возможностей);
9. определение факта превышения разрешенной на участке дороги скорости для ТС предприятий;
10. участников информационного взаимодействия подсистем РНИС ПК;
11. определение факта исполнения условий государственных и муниципальных контрактов, свидетельств и договоров предприятий;
12. участников информационного взаимодействия подсистем РНИС ПК, на основе навигационных данных и НСИ РНИС ПК;
13. интеграции на базовом уровне с РНИС ПК других (соседних) регионов для ТС, осуществляющих межрегиональные перевозки (а именно, ретрансляция навигационных данных по протоколу EGTS, приём данных по протоколу EGTS);
14. повышения качества транспортного обслуживания населения Пермского края за счет предоставления информационных сервисов и данных о движении транспортных средств в сети Интернет.

3 Характеристика объекта автоматизации

3.1 Основные сведения об объекте автоматизации

Объектом автоматизации в рамках выполнения работ по-настоящему ТЗ является деятельность Министерства информационного развития и связи Пермского края в части формирования единого технологического и информационного пространства, обеспечивающего возможность проведения объективного анализа предметной деятельности с помощью различных инструментов, подходов и методов обработки как структурированных, так и неструктурированных отраслевых данных.

3.2 Сведения об условиях эксплуатации объекта автоматизации и характеристиках окружающей среды

Для размещения Системы используется виртуальная инфраструктура Заказчика и отечественная, сертифицированная ОС и СУБД.

Условия эксплуатации комплекса технических средств Системы соответствуют условиям эксплуатации группы 2 ГОСТ Р 71784-2024 «Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортировка, хранение».

3.3 Перечень функций, реализуемых Системой

РНИС ПК представляет собой единую автоматизированную навигационно-информационную систему, предназначенную для формирования навигационных сигналов, передачи, приёма, обработки, хранения и визуализации навигационной информации, а также:

- процессы создания, изменения и управления справочниками системы, необходимыми для функционирования РНИС ПК;
- процессы диспетчеризации и оперативного управления пассажирским автотранспортом, в части сбора, хранения и аналитической обработки информации, необходимой для оперативного управления пассажирским автотранспортом, планирования и учёта транспортной работы по перевозке пассажиров, а также для обеспечения контроля передвижения и диспетчеризации ТС;
- процессы контроля общественного транспорта, а именно контроля объёмов работы пассажирского транспорта, контроля качества пассажирских перевозок, в

части контроля выполнения перевозчиками параметров и показателей транспортной работы в соответствии с условиями государственных контрактов и свидетельств;

- процессы диспетчеризации и оперативного управления дорожной техникой, в части планирования и оперативного управления дорожной техникой;
- процессы диспетчеризации и оперативного управления коммунальной техникой, в части планирования и оперативного управления коммунальной техникой;
- процессы диспетчеризации и оперативного управления службами эвакуации в части распределения заявок, контроля их исполнения и оценки подрядных организаций;
- процессы контроля дорожной техники, в части осуществления мониторинга за передвижением дорожной техники, включая ретроспективный просмотр передвижения ТС, а также процент выполненных работ и соблюдение регламентных сроков производства работ, формирование отчётности о работе ТС;
- процессы контроля коммунальной техники, в части осуществления мониторинга за передвижением коммунальной уборочной техники, включая ретроспективный просмотр передвижения ТС, формирование отчётности о работе ТС;
- процессы контроля перевозок специальных, опасных, крупногабаритных и тяжеловесных грузов автомобильным транспортом, формирование отчетности о работе ТС;
- процессы контроля транспортных средств территориального центра медицины катастроф, скорой и неотложной медицинской помощи, в части осуществления мониторинга за передвижением ТС, включая ретроспективный просмотр передвижения ТС, формирование отчётности о работе ТС;
- процессы контроля работы автобусов, предназначенных для организованной перевозки групп детей в части сбора, хранения и аналитической обработки информации необходимой для обеспечения контроля работы школьных автобусов, предназначенных для организованной перевозки групп детей, мониторинг качества и безопасности перевозок учащихся, соответствие параметров перевозок учащихся условиям государственных контрактов, свидетельств;

- процессы контроля вывоза ТКО предназначены для сбора, хранения и аналитической обработки информации необходимой для обеспечения контроля работы транспорта при осуществлении вывоза ТКО;
- процессы контроля вывоза медицинских отходов предназначены для сбора, хранения и аналитической обработки при осуществлении работ по вывозу медицинских отходов;
- процессы оперативного управления ведомственным транспортом органов государственной власти в части осуществления мониторинга, включая ретроспективный просмотр передвижения ТС, фиксации нарушений установленных параметров движения и формирования отчётности о деятельности ведомственного транспорта органов государственной власти;
- процессы информирования пассажиров о расписаниях общественного транспорта и прогнозном времени прибытия в части информирования пассажиров о расписаниях движения, о фактическом местоположении и движении пассажирского транспорта в режиме реального времени, обеспечения возможности построения маршрута с учётом настраиваемых условий запросов и расчёт прогнозного времени прибытия пассажирского транспорта, прогноза прибытия/отправления пассажирского транспорта конкретных маршрутов по остановочным пунктам;
- процессы информирования населения о дате и времени эвакуации транспортного средства, причин эвакуации транспортного средства и месте прибытия эвакуированного транспортного средства;
- процессы сбора, обработки и предоставления навигационных данных во все смежные подсистемы РНИС ПК в режиме реального времени;
- процессы обеспечения информационной безопасности, в части предотвращения несанкционированного доступа к информационным ресурсам РНИС ПК, предотвращения несанкционированной модификации информации, и её уничтожения, обеспечения безопасности информации при информационном обмене с внешними системами и подсистемами РНИС ПК;
- процессы обеспечения функционирования РНИС ПК и предоставление доступа к информации РНИС ПК, в том числе о передвижении ТС;

- процессы обеспечения взаимодействия между подсистемами РНИС ПК, а также с внешними информационными системами (ВИС) в рамках информационного ландшафта РНИС ПК;
- процессы управления ролями и учётными записями пользователей РНИС ПК и настройки прав доступа пользователей;
- процессы мониторинга работоспособности и диагностики неисправностей РНИС ПК в части фиксации и просмотра параметров функционирования ПО РНИС ПК и БНСО, установленных на ТС транспортных предприятий, подключённых к РНИС ПК.

В процессе функционирования РНИС ПК обеспечивает её пользователей необходимыми и достоверными данными для осуществления мониторинга текущей ситуации дорожно-транспортного комплекса Пермского края и оперативного принятия управленческих решений в области дорожного хозяйства и транспортного обслуживания населения на территории Пермского края.

3.4 Общие принципы развития Системы

При развитии Системы необходимо руководствоваться следующими принципами:

1. Принцип системности. Заключается в том, что при декомпозиции должны быть установлены такие связи между структурными элементами системы, которые обеспечивают цельность Системы и ее взаимодействие с другими информационными системами. При развитии Системы ее компоненты реализовываются комплексно со всеми возможными информационными связями, а не автономно от других.

2. Принцип развития (открытости). Заключается в том, что, исходя из перспектив развития объекта автоматизации, Система должна развиваться с учетом возможности пополнения и обновления функций и состава Системы без нарушения ее функционирования с учетом:

- возможности добавления новых функций или изменения уже имеющихся при неизменных остальных функциональных частях Системы;

- адаптируемости Системы к изменениям требований нормативных правовых актов Российской Федерации, Пермского края, потребностей пользователей Системы;
- внедрения новых информационных технологий.

3. Принцип совместимости. Заключается в том, что при развитии Системы должны быть реализованы информационные интерфейсы, благодаря которым она может взаимодействовать с другими информационными системами в соответствии с установленными правилами. Взаимодействие с другими системами должно отвечать требованиям:

- совместимости вычислительных и телекоммуникационных устройств;
- информационной безопасности Системы, обеспечения защиты персональных данных;
- соблюдения протоколов взаимодействия пользователей Системы.

4. Принцип стандартизации (унификации). Заключается в том, что при развитии системы должны быть рационально применены типовые, унифицированные и стандартизованные элементы, проектные решения, пакеты прикладных программ, комплексы, компоненты. Должно быть обеспечено:

- единство используемых терминов, нормативной и справочной информации, системы показателей, формирования и представления отчетности;
- единство стандартов технологий, форматов;
- полнота, актуальность и достоверность обрабатываемой в Системе информации;
- унификация эксплуатации (общность эксплуатационных требований).

5. Принцип эффективности. Заключается в достижении рационального соотношения между затратами на развитие Системы и целевыми эффектами, включая конечные результаты, получаемые в результате автоматизации.

3.5 Взаимодействие с иными информационными системами

Система взаимодействует со следующими информационными системами¹:

- Единое хранилище данных Пермского края (ЕХД ПК);
- Транспортная платформа Яндекс карты;
- Транспортная платформа 2ГИС;
- Интеграционная платформа ИТС Пермской городской агломерации (ЕПУТС ПГА);
- Региональный сервис аутентификации и авторизации сотрудников органов государственной власти и учреждений Пермского края (РСАА ПК) и система идентификации и аутентификации (ЕСИА)

3.6 Структура Системы и назначение ее частей

Система состоит из функциональных и обеспечивающих подсистем.

Перечень подсистем и их назначение представлены в таблице ниже (Таблица 2).

Таблица 2 – Подсистемы РНИС ПК и их назначение

Наименование подсистемы	Назначение
Подсистема оператора РНИС ПК	Подсистема предназначена для обеспечения функционирования РНИС ПК и предоставления доступа к информации о передвижении ТС пользователям РНИС ПК, управления ролями и учётными записями пользователями РНИС ПК, настройки прав доступа пользователей и обеспечения функционирования РНИС ПК в целом, обеспечения информационного взаимодействия между подсистемами РНИС ПК, интеграции разнородных программно-аппаратных средств в единое информационное пространство и обеспечения взаимодействия РНИС ПК с внешними информационными системами и сервисами, формирования, хранения, актуализации и предоставления нормативно-справочной информации (НСИ), реестров, справочников и иной информации для использования в подсистемах РНИС ПК.
Подсистема мониторинга	Подсистема предназначена для мониторинга работоспособности РНИС ПК и диагностики

¹[Указываются полные и сокращенные официальные наименования информационных систем, с которыми взаимодействует Система. Наименования должны соответствовать наименованиям, указанным в нормативных правовых актах, решениях о создании информационных систем.]

Наименование подсистемы	Назначение
работоспособности и диагностики неисправностей РНИС ПК	неисправностей БНСО.
Аналитическая платформа РНИС ПК	Подсистема предназначена для предоставления аналитической информации о деятельности транспортного комплекса Пермского края
Подсистема мониторинга и управления пассажирскими перевозками на территории Пермского края	Подсистема предназначена для автоматизации процессов сбора, хранения и аналитической обработки информации, необходимой для оперативного управления пассажирским автотранспортом, планирования и учёта транспортной работы по перевозке пассажиров, обеспечения контроля передвижения и диспетчеризации ТС, в том числе создания план-нарядов, путевых листов, контроля соблюдения расписания и оперативного изменения план-нарядов, по формированию отчётов о выполнении транспортной работы предприятия края, и передача во внешние информационные ресурсы данных о движении транспортных средств.
Подсистема мониторинга и управления школьными автобусами (организованными перевозками детей школьными автобусами) на территории Пермского края	Подсистема (на аналитическом уровне) предназначена для автоматизации процессов сбора, хранения и аналитической обработки информации, необходимой для контроля объёмов работы школьных автобусов, контроля выполнения перевозчиками параметров и показателей транспортной работы в соответствии с условиями государственных и муниципальных контрактов и свидетельств на школьные перевозки. Подсистема (на прикладном уровне) предназначена для автоматизации процессов сбора, хранения и аналитической обработки информации, необходимой для оперативного управления школьными автобусами (организованными перевозками детей школьными автобусами), планирования и учёта транспортной работы, обеспечения контроля передвижения и диспетчеризации ТС, в том числе создания план-нарядов, путевых листов, контроля соблюдения расписания и оперативного изменения план-нарядов, по формированию отчётов о выполнении транспортной работы предприятия.

Наименование подсистемы	Назначение
Подсистема мониторинга перевозок специальных, опасных, крупногабаритных и тяжеловесных грузов автомобильным транспортом на территории Пермского края	Подсистема предназначена для автоматизации процессов планирования и оперативного управления перевозками специальных, опасных, крупногабаритных и тяжеловесных грузов автомобильным транспортом, контроль работы ТС, формирование отчётов о выполнении работы (посещении маршрутов и геозон), включая просмотр истории передвижения ТС.
Подсистема мониторинга автомобильных транспортных средств организаций жилищно-коммунального хозяйства на территории Пермского края	Подсистема предназначена для автоматизации процессов планирования и оперативного управления коммунальной техникой, в том числе создания путевых листов, контроль работы механизмов транспортных средств организаций ЖКХ, предоставление доступа к реестру заявок на проведение плановых и экстренных работ и выполнения заявок, формирование отчётов о выполнении работы (посещении маршрутов и геозон), контроля транспортных средств организаций ЖКХ, осуществления мониторинга за передвижением транспортных средств организаций ЖКХ, включая просмотр истории передвижения ТС, формирования отчётов о работе ТС.
Подсистема мониторинга и управления дорожной техникой на территории Пермского края	Подсистема предназначена для автоматизации процессов планирования и оперативного управления дорожной техникой, в том числе создания путевых листов, контроль работы механизмов дорожной техники, предоставление доступа к реестру заявок на проведение плановых и экстренных работ и выполнения заявок, формирование отчётов о выполнении работы (посещении маршрутов и геозон), контроля дорожной техники, осуществления мониторинга за передвижением дорожной техники, включая просмотр истории передвижения ТС, формирования отчётов о работе ТС.
Подсистема мониторинга и управления транспортными средствами прочих АТП	Подсистема предназначена для мониторинга транспорта прочих автотранспортных предприятий и предоставления отчётов о работе ТС.

Наименование подсистемы	Назначение
Подсистема мониторинга транспортных средств, осуществляющих вывоз ТКО на территории Пермского края	Подсистема предназначена для автоматизации процессов планирования и оперативного управления транспортными средствами, осуществляющих вывоз ТКО, в том числе осуществления мониторинга за передвижением транспортных средств, включая просмотр истории передвижения ТС, формирования отчётов о работе ТС.
Подсистема мониторинга транспортных средств, осуществляющих вывоз медицинских отходов	Подсистема предназначена для контроля и оперативного управления транспортными средствами, осуществляющих вывоз медицинских отходов. Контроль объемов вывозимых отходов с использованием мобильного приложения водителя, оперативная сверка данных по количеству вывезенных и количеству утилизированных отходов. Контроль за оборотом контейнерного парка путем идентификации маркировки контейнера, осуществления мониторинга за передвижением транспортных средств, включая просмотр истории передвижения ТС, формирования отчётов о работе ТС.
Подсистема мониторинга и управления транспортными средствами органов государственной власти на территории Пермского края	Подсистема предназначена для мониторинга транспорта ОГВ ПК и предоставления отчётов о работе ТС.
Подсистема мониторинга и управления транспортными средствами эвакуации	Подсистема предназначена для автоматизации процессов сбора, хранения и аналитической обработки информации, необходимой для оперативного управления эвакуаторами. Предназначена для приема, хранения, исполнения поступающих заявок на эвакуацию транспорта. Равномерного распределения работ между подрядными организациями и контроля качества выполнения работ, включая просмотр истории передвижения ТС, формирования отчётов о

Наименование подсистемы	Назначение
	работе ТС.
Подсистема информационного обеспечения потребителей услуг транспортного комплекса (в том числе перевозок пассажиров и грузов автомобильным транспортом) на территории Пермского края (Интернет-портал)	Интернет-портал предназначен для информирования населения о работе транспортного комплекса региона и предоставления информации по подключению к РНИС ПК, включая: • публикацию новостей транспортного комплекса; • отображение транспортных средств, выполняющих перевозки пассажиров и багажа; • построение пользовательских маршрутов используя региональную маршрутную сеть; • информирование о расписаниях; • предоставление формы обратной связи; • предоставление информации по подключению к РНИС ПК.
Подсистема «Единая телематическая платформа» (ЕТП)	Подсистема предназначена для сбора, обработки и предоставления во все смежные подсистемы РНИС ПК навигационных данных в режиме реального времени и ретрансляции навигационной информации в ВИС по протоколу EGTS.
Подсистема информационно-справочного обеспечения транспортного комплекса Пермского края	Подсистема предназначена для получения нормативно-справочной информации из информационной системы Единое хранилище данных Пермского края (ЕХД ПК) для формирования справочников в РНИС ПК (маршруты, остановочные пункты и т.д.), а также для предоставления нормативно-справочной информации из РНИС ПК во внешние ведомственные информационные системы (ВИС).
Подсистема обеспечения информационной безопасности	Подсистема обеспечения информационной безопасности обеспечивает предотвращение несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации, используемой в РНИС ПК.

3.7 Программно-аппаратное обеспечение Системы

Система размещена на серверах с использованием инфраструктуры Заказчика (Таблица 3):

Таблица 3 – Аппаратное и программное обеспечение Системы

Имя ресурса	Количество			Операционная система и программное обеспечение
	CPU (core)	RAM, Gb	Локальные диски, Gb	
База данных Основной (промышленный) контур	8	28	550	ОС – Альт СП; ПО - ClickHouse, node-exporter.
База данных Основной (промышленный) контур	8	20	1050	ОС – Альт СП; ПО - ClickHouse, node-exporter.
База данных Основной (промышленный) контур	8	20	1050	ОС – Альт СП; ПО - ClickHouse, node-exporter.
База данных Основной (промышленный) контур	8	20	1000	ОС – Альт СП; ПО - ClickHouse, node-exporter.
База данных Основной (промышленный) контур	2	4	50	ОС – Альт СП; ПО - ClickHouse, node-exporter.
База данных Основной (промышленный) контур	2	4	50	ОС – Альт СП; ПО - ClickHouse, node-exporter.
База данных Основной (промышленный) контур	2	4	50	ОС – Альт СП; ПО - ClickHouse, node-exporter.
База данных Основной (промышленный) контур	4	16	550	ОС – Альт СП; ПО - MongoDB, node-exporter.
База данных Основной (промышленный) контур	4	16	550	ОС – Альт СП; ПО - MongoDB, node-exporter.

Оркестратор контейнеров Основной (промышленный) контур	4	2	150	ОС – Альт СП; ПО - Kubernetes, node-exporter.
База данных Основной (промышленный) контур	2	2	150	ОС – Альт СП; ПО - Redis, node-exporter.
База данных Основной (промышленный) контур	2	2	150	ОС – Альт СП; ПО - Redis, node-exporter.
Сетевое хранилище Основной (промышленный) контур	1	2	350	ОС – Альт СП; ПО - node-exporter.
Сетевое хранилище Основной (промышленный) контур	1	2	350	ОС – Альт СП; ПО - node-exporter.
База данных Основной (промышленный) контур	20	2	2050	ОС – Альт СП; ПО - PostgreSQL, Kubernetes, node-exporter.
База данных Основной (промышленный) контур	20	2	2050	ОС – Альт СП; ПО - PostgreSQL, Kubernetes, node-exporter.
мониторинг Основной (промышленный) контур	6	2	350	ОС – Альт СП; ПО - Kubernetes, node-exporter, Prometheus, Grafana
База данных Основной (промышленный) контур	4	2	150	ОС – Альт СП; ПО - Kubernetes, node-exporter.
Веб-приложение Основной (промышленный) контур	16	2	350	ОС – Альт СП; ПО - Kubernetes, etcd, node-exporter, Nginx
Веб-приложение Основной (промышленный) контур	16	2	350	ОС – Альт СП; ПО - Kubernetes, etcd, node-exporter, Nginx
Веб-приложение Основной (промышленный)	4	2	350	ОС – Альт СП; ПО - Kubernetes, etcd, node-exporter, Nginx

контур				
Веб-приложение Основной (промышленный) контур	4	2	350	ОС – Альт СП; ПО - Kubernetes, etcd, node- exporter, Nginx
Веб-приложение Основной (промышленный) контур	8	2	350	ОС – Альт СП; ПО - Kubernetes, node- exporter.
Веб-приложение Основной (промышленный) контур	8	2	350	ОС – Альт СП; ПО - Kubernetes, node- exporter.
Веб-приложение Основной (промышленный) контур	12	2	350	ОС – Альт СП; ПО - Kubernetes, node- exporter.
Веб-приложение Основной (промышленный) контур	12	2	350	ОС – Альт СП; ПО - Kubernetes, node- exporter.
Веб-приложение Основной (промышленный) контур	4	2	150	ОС – Альт СП; ПО - Kubernetes, node- exporter.
Брокер сообщений Основной (промышленный) контур	6	2	150	ОС – Альт СП; ПО - RabbitMQ, Kubernetes, node-exporter.
Брокер сообщений Основной (промышленный) контур	6	2	550	ОС – Альт СП; ПО - Kubernetes, Apache Kafka, node-exporter.

3.8 Сведения о ранее исполненных контрактах

Система была создана в рамках ГК № 29/ОК-2021 от 29 декабря 2021 года, извещением от «29» октября 2021 г. № 0156200009921000929.

Развитие Системы проводилось в рамках ГК № 71/ЭА-2024 от 25 ноября 2024 года, извещением от 31.10.2024г. № 0356500001424007166.

Сведения о документации на Систему, разработанной в рамках создания и развития Системы, представлены ниже (Таблица 4).

Таблица 4 – Документация, разработанная на Систему

№ п/п	Наименование документа	Обозначение (код) документа
1	Частное техническое задание	1157746045192.425000.012.ЧТЗ-ЛУ
2	Пояснительная записка к техническому проекту	1157746045192.425000.012.П2
3	Общее описание системы	RU.1157746045192.425000.012.ПД
4	Описание информационного обеспечения	1157746045192.425000.012.П5
5	Руководство программиста	RU.1157746045192.62.01.29-02 33 12
6	Руководство оператора	RU.1157746045192.62.01.29-02 34 12
7	Руководство системного программиста	RU.1157746045192.62.01.29-02 32 12
8	Описание архитектуры системы	ГИС_РНИС_ПК.4/ЭА-2026.3.ОА.2

После заключения ГК Заказчик предоставляет Подрядчику указанные в таблице 4 документы в течение 5 (пяти) рабочих дней с даты получения соответствующего запроса от Подрядчика.

4 Требования к Системе

Система должна представлять собой открытую информационную систему, интегрируемую с другими информационными системами.

Развитие Системы должно происходить с учетом модульного принципа, допускающего отдельную разработку, установку, обновление и техническое обслуживание отдельных модулей.

При выполнении работ должно быть обеспечено преимущественное использование свободного программного обеспечения (далее – ПО). В случае невозможности использования свободного ПО Подрядчик обязан обосновать и согласовать данный факт с Заказчиком.

Система должна быть централизованной, т.е. все данные должны располагаться в централизованном хранилище.

Система должна отвечать критериям релевантности и целесообразности, что выражается в возможности использовать Систему с минимальным привлечением дополнительных затрат ресурсов.

Детализация требований к выполняемым работам должна быть выполнена при разработке частного технического задания.

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

Информационный обмен между компонентами Системы должен осуществляться через единое информационное пространство, посредством внутренних программных интерфейсов на базе протоколов HTTP (в том числе SOAP и REST) и RMI.

Информационный обмен между компонентами Системы должен осуществляться без вмешательства пользователя и без повторного ручного ввода информации

4.2 Требования к характеристикам взаимосвязей Системы с иными информационными системами

В рамках выполнения работ по-настоящему ТЗ Подрядчиком, требования по обеспечению возможности информационного взаимодействия со внешними информационными системами не предъявляются.

4.3 Требования к функциям (задачам), реализуемым в рамках выполнения работ

Перечень подсистем и их назначение представлены в п.3.6.

В рамках функций, выполняемых Системой, необходимо:

1. Оптимизировать работоспособность программного обеспечения Системы;
2. Разработать подсистему «Информационная система обеспечения мониторинга отходов строительства и сноса».
3. Проведение мероприятий по защите информации, и анализу исходных кодов на уязвимости и аттестации Системы (в соответствии с пунктом 6.6).

После проведенного обследования функциональности Системы Подрядчиком (совместно с ответственными сотрудниками Заказчика), Подрядчик разрабатывает ЧТЗ, на детализирующее требования, предъявленные Заказчиком. При этом ЧТЗ не должно дублировать положения настоящего ТЗ — в случае такой необходимости приводятся ссылки на соответствующие разделы ТЗ.

4.3.1 Требования к оптимизации работоспособности программного обеспечения Системы

В рамках проведения работ по оптимизации работоспособности Системы, Подрядчик должен выполнить:

Анализ текущих показателей времени отклика функций Системы и выявления проблемных зон, с последующим формированием реестра и предоставлением реестра Заказчику.

Оптимизацию работы программного обеспечения, кода, баз данных с целью уменьшения времени отклика \ выполнения функций системы для обеспечения быстродействия, увеличить производительность системы, всех функций Системы, отображения контента и выполнения пользовательских всех запросов за время, не превышающее 15 секунд.

4.3.2 Требования к разработке подсистемы «Информационная система обеспечения мониторинга отходов строительства и сноса»

4.3.2.1 Наименование подсистемы

Подсистема «Информационная система обеспечения мониторинга отходов строительства и сноса» (далее – Подсистема, ОСиС).

4.3.2.2 Цель и задачи подсистемы:

Целями создания подсистемы являются: обеспечение учёта и контроля транспортирования ОСиС, образуемых и ввозимых на территорию Пермского края; автоматизация процессов выдачи разрешений на транспортирование ОСиС; мониторинг движения ОСиС от момента образования до утилизации или размещения; формирование отчётности и аналитических данных для органов государственной власти и участников оборота ОСиС.

Задачами подсистемы являются: автоматизация выдачи разрешений на транспортирование ОСиС в электронном виде; учёт объектов образования ОСиС (объектов строительства, реконструкции, сноса и благоустройства); учёт объектов приема ОСиС (объектов обработки, утилизации, обезвреживания и размещения); мониторинг транспортирования с использованием ГЛОНАСС/GPS; и бортовым навигационно-связным оборудованием (БНСО); формирование статистических и аналитических отчётов по движению ОСиС.

4.3.2.3 Функциональные требования к подсистеме:

Подсистема «ОСиС» должна представлять собой автоматизированную информационную систему, обеспечивающую сбор, обработку, хранение и предоставление информации в области обращения с отходами строительства, реконструкции, капитального ремонта, сноса объектов капитального строительства и благоустройства территорий на территории Пермского края

Подсистема должна обеспечивать регистрацию участников (отходопроизводителей, отходоперевозчиков, отходополучателей) с ведением соответствующих реестров; регистрацию объектов образования ОСиС и

объектов приема ОСиС; регистрацию транспортных средств, используемых для перевозки ОСиС; автоматизированное формирование и закрытие разрешений на транспортирование ОСиС; мониторинг перемещения транспортных средств на карте в реальном времени; учёт объёма и веса ОСиС при выезде с объекта образования и въезде на объект приема; формирование отчётов по движению ОСиС, разрешениям и участникам; приём данных с БНСО.

Подсистема должна обеспечивать отображение на географической карте объектов образования и приема ОСиС, маршрутов движения транспортных средств, статусов разрешений и рейсов. Учёт и отчётность должны включать: отчёт о выданных разрешениях (ежемесячно \ по запросу), отчёт о перемещённых ОСиС (ежемесячно \ по запросу), отчёт об объектах образования и приема (ежемесячно \ по запросу), аналитический отчёт по видам ОСиС (ежемесячно \ по запросу), отчёт о нарушениях (ежемесячно \ по запросу) и иные виды отчетности.

4.3.2.4 Роли пользователей и разграничение доступа

Подсистема должна обеспечивать авторизацию и аутентификацию пользователей с поддержкой РСАА, ЕСИА и разграничением прав доступа по ролям; журналирование всех действий пользователей и администраторов.

В подсистеме должны быть предусмотрены следующие роли пользователей: администратор системы (полный доступ, управление пользователями, настройка системы, регистрация транспортных средств); уполномоченный орган (выдача разрешений, проверка документов, контроль, координация использования системы); отходопроизводитель (регистрация объектов, подача заявок на разрешения, предоставление договоров); отходоперевозчик (выполнение рейсов, передача данных \ документов, мониторинг); отходополучатель (регистрация объектов приема, подтверждение приёма ОСиС) и иные.

Для каждого участника в подсистеме должны храниться: полное и сокращённое наименование организации, организационно-правовая форма, ИНН, ОГРН, контактные данные, сведения о наличии лицензий на деятельность по обращению с отходами I-IV классов опасности, а также информация о регистрации в качестве индивидуального предпринимателя (для физических лиц). Подсистема должна обеспечивать возможность актуализации данных участниками, а также автоматическое уведомление участников о необходимости подтверждения или обновления сведений в установленные сроки.

Подсистема должна предоставлять каждому участнику информационного взаимодействия персональный личный кабинет с разграничением прав доступа в зависимости от роли пользователя. Личный кабинет должен обеспечивать: подачу заявок на получение разрешений на транспортирование ОСиС; просмотр статусов поданных заявок и выданных разрешений; регистрацию объектов образования и приема ОСиС; предоставление сведений о движении ОСиС и договорах на оказание услуг по обращению с ОСиС; формирование и выгрузку отчётов; получение уведомлений о статусе разрешений, нарушений и изменениях в системе; возможность заключения договоров на транспортирование ОСиС, на оказание услуг по обращению с ОСиС. Личный кабинет должен быть адаптирован для использования на персональных компьютерах, планшетах и мобильных устройства

4.3.2.5 Регистрация и учет объектов образования ОСиС

Подсистема должна обеспечивать регистрацию объектов образования ОСиС, на которых образуются отходы в результате строительства, реконструкции, капитального ремонта, сноса объектов капитального строительства или благоустройства территорий. Для каждого объекта образования ОСиС в подсистеме должна фиксироваться следующая информация: адрес объекта, кадастровый номер земельного участка, геозону,

вид разрешённого использования, сведения о застройщике, генеральном подрядчике (подрядчике в иерархическом виде), техническом заказчике, проектная документация, календарный план строительства или график производства работ, ведомость образования отходов с разделением по видам и группам однородных ОСиС и классам опасности, объём в кубических метрах, вес в тоннах и период образования, а также сведения о договорах на оказание услуг по обращению с ОСиС и иные. Подсистема должна обеспечивать возможность привязки к объекту образования регистрации транспортных средств, осуществляющих вывоз ОСиС, и формирования разрешений на транспортирование ОСиС.

4.3.2.6 Регистрация и учет объектов приема ОСиС

Подсистема должна обеспечивать регистрацию объектов приема ОСиС, на которых осуществляется обработка, утилизация, обезвреживание и размещение отходов строительства и сноса. Для каждого объекта приема ОСиС в подсистеме должна фиксироваться следующая информация: адрес объекта, кадастровый номер земельного участка, геозону, вид деятельности по обращению с ОСиС, наличие заключения о соответствии объекта требованиям законодательства Российской Федерации в области обращения с отходами и охраны окружающей среды, наличие лицензии на осуществление деятельности по сбору, транспортированию, обработке, утилизации, обезвреживанию, размещению отходов I-IV классов опасности, сведения о применяемых технологиях по утилизации ОСиС, остаточная мощность объекта приема для гарантированного приёма ОСиС. Подсистема должна обеспечивать ведение Реестра объектов приема ОСиС, формируемого уполномоченным органом, с отражением актуальной остаточной мощности каждого объекта, а также возможность поиска объектов по видам принимаемых ОСиС, их классам опасности и объёму свободных мощностей.

4.3.2.7 Регистрация и учет транспортных средств

Подсистема должна обеспечивать регистрацию транспортных средств, предназначенных для транспортирования ОСиС. Для каждого транспортного средства в подсистеме должна фиксироваться следующая информация: государственный регистрационный знак, марка и модель транспортного средства, грузоподъемность, вместимость кузова в кубических метрах, сведения о наличии аппаратуры спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS, сведения о наличии бортового навигационно-связного оборудования (БНСО). Подсистема должна обеспечивать привязку транспортных средств к отходоперевозчику и возможность отслеживания местоположения транспортного средства в реальном времени, а также хранение истории перемещений.

Предусмотреть возможность добавления и\или дублирования в подсистему «Отходы строительства и сноса» иных транспортных средств, которые уже подключены к РНИС ПК, но находятся в иной подсистеме

4.3.2.8 Требования к автоматизации выдачи разрешений на транспортирование ОСиС

Подсистема должна обеспечивать полный цикл автоматизированного оформления разрешений на транспортирование ОСиС, начиная с подачи заявки отходопроизводителем и заканчивая выдачей электронного разрешения для отходопроизводителя. Заявка на получение разрешения должна подаваться в личном кабинете в форме электронного документа. В заявке должны быть указаны: адрес объекта образования ОСиС, сведения об отходопроизводителе, отходоперевозчике и отходополучателе, государственные ГРЗ, их грузоподъемность и вместимость кузова, вид или группа однородных ОСиС и объем перемещаемых ОСиС, адрес объекта приема (переработки) ОСиС, реквизиты договоров на оказание услуг по обращению с ОСиС. Подсистема должна автоматически проверять наличие представленных документов (загрузил \ не загрузил), наличие заключенных договоров (загрузил \ не загрузил), соответствие объекта приема требованиям

и его остаточную мощность. Уполномоченный орган проверяет заявку и принимает решение: согласовать, отклонить или вернуть на доработку с указанием причин. При положительном результате проверки (уполномоченным органом) подсистема формирует электронное разрешение на транспортирование ОСиС, разрешение содержит серию, номер, дату выдачи, срок действия, ГРЗ ТС, объем, и иную информацию. Срок действия разрешения устанавливается автоматически на основании календарного графика производства работ, но не превышает срок действия разрешения на строительство или срок проведения работ. Подсистема должна обеспечивать ведение реестра выданных разрешений, автоматическое уведомление участников о приближении срока окончания действия разрешения и блокировку разрешения вывоза ОСиС при отсутствии действующего разрешения.

4.3.2.9 Требования к закрытию разрешений на транспортирование ОСиС

Подсистема должна обеспечивать автоматизированное закрытие разрешений на транспортирование ОСиС после завершения перевозки всего заявленного объема ОСиС или по истечении срока действия разрешения. Закрытие разрешения осуществляется на основании заявки отходопроизводителя, поданной в личном кабинете не позднее десяти рабочих дней после даты окончания срока действия разрешения. При закрытии разрешения подсистема должна проверять полноту данных о фактически перемещённых ОСиС, включая объёмы, зафиксированные на контрольно-измерительных пунктах, и подтверждение отходополучателя о приёме ОСиС. В случае отсутствия заявки на закрытие в установленный срок подсистема должна автоматически информировать уполномоченный орган. Закрытое разрешение должно сохраняться в архиве с возможностью просмотра и формирования отчётов.

4.3.2.10 Требования к мониторингу перемещения ОСиС

Подсистема должна обеспечивать непрерывный мониторинг перемещения транспортных средств, осуществляющих транспортирование ОСиС, на основе данных, поступающих с аппаратуры спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS, установленной на транспортных средствах бортового навигационно-связного оборудования (БНСО). Подсистема должна отображать в реальном времени на географической карте местоположение каждого зарегистрированного транспортного средства, его маршрут движения, статус выполнения рейса, а также параметры движения (скорость, координаты, время). В случае отклонения от маршрута, несанкционированной остановки или выгрузки ОСиС вне объекта приема, подсистема должна формировать сигнал тревоги и автоматически уведомлять уполномоченный орган и отходопроизводителя.

4.3.2.11 Требования к учету объемов фиксации данных с контрольно измерительных пунктов

Подсистема должна принимать данные о: государственный регистрационный знак транспортного средства, объём и/или вес ОСиС в кузове транспортного средства, дату и время проезда, фото изображение транспортного средства и перевозимого груза. Подсистема должна автоматически сравнивать объём ОСиС, введённый отход образователем \ отход перевозчиком \ отход производителя при выезде с объекта образования, с объёмом, веденным отход получателем \ отход переработчиком на объект приема, и в случае расхождения формировать уведомление для отхода производителя и уполномоченного органа. Данные должны сохраняться в архиве с возможностью просмотра и выгрузки отчётов. Логические требования к подсистеме.

4.3.2.12 Требования к информационному взаимодействию с аппаратурой спутниковой навигации

Подсистема должна обеспечивать приём и обработку данных с аппаратуры спутниковой навигации ГЛОНАСС или ГЛОНАСС/GPS, установленной на транспортных средствах, осуществляющих транспортирование ОСиС. Данные должны передаваться в подсистему в автоматическом режиме с периодичностью, обеспечивающей мониторинг в реальном времени. Передаваемые данные должны включать: координаты транспортного средства, скорость движения, направление движения, дату и время, а также идентификационный номер транспортного средства. Подсистема должна обеспечивать хранение указанных данных в течение всего срока действия разрешения на транспортирование ОСиС и возможность их использования для формирования отчётов и исследований.

4.3.2.13 Ведение реестра разрешений на транспортирование ОСиС

Подсистема должна обеспечивать ведение реестра разрешений на транспортирование ОСиС, в котором должны содержаться сведения о всех выданных, переоформленных и закрытых разрешениях на территории Пермского края. Реестр должен включать: дату выдачи, срок действия, серию и номер разрешения, адрес объекта образования, наименования и ИНН отходопроизводителя, отходоперевозчика и отходополучателя, виды и объём ОСиС, адрес объекта приема. Реестр должен обеспечивать поиск, фильтрацию и формирование отчётности по запросам уполномоченного органа, информационного оператора и иных заинтересованных лиц

4.3.2.14 Формирование статистической и аналитической отчетности

Подсистема должна обеспечивать формирование статистической и аналитической отчётности по движению ОСиС на территории Пермского края. Отчётность должна включать:

Отчёт о выданных разрешениях формируется для учёта и контроля выдачи разрешений на транспортирование ОСиС. В отчёте указывается период, количество выданных разрешений, серия и номер каждого разрешения, дата выдачи и срок действия, наименование и ИНН отходопроизводителя, отходоперевозчика и отходополучателя, адрес объекта образования и объекта приёма, виды и объёмы ОСиС, а также статус разрешения.

Отчёт о закрытых разрешениях предназначен для контроля завершения перевозок по разрешениям. В отчёте указывается период, количество закрытых разрешений, номер каждого разрешения, дата закрытия, фактически перемещённый объём, расхождение с заявленным объёмом, наличие подтверждения отходополучателя и сведения о нарушениях.

Отчёт о разрешениях, не закрытых в срок служит для выявления нарушений сроков закрытия. В отчёте отражается номер разрешения, срок его действия, дата истечения с учётом десяти рабочих дней, отходопроизводитель, причина отсутствия заявки на закрытие и принятые меры.

Отчёт о разрешениях, срок действия которых истекает предназначен для предупреждения участников. В отчёте указывается номер разрешения, срок действия, количество дней до окончания, участники и рекомендуемые действия.

Отчёт о фактически перемещённых ОСиС формируется для учёта фактического движения отходов. В отчёте указывается период, объект образования, вид ОСиС, группа однородных отходов, класс опасности, объём в кубических метрах, вес в тоннах, отходоперевозчик, отходополучатель, дата вывоза и статус (завершён или нарушение).

Отчёт о движении ОСиС по объектам образования предназначен для контроля вывоза с конкретных объектов. В отчёте отражается объект образования, заявленный объём, фактически вывезенный объём, остаток, процент выполнения, количество рейсов и сведения о нарушениях.

Отчёт о движении ОСиС по объектам приёма служит для контроля приёмки отходов. В отчёте указывается объект приёма, вид деятельности, принятый объём по видам ОСиС, остаточная мощность, процент загрузки, отходоперевозчики и сведения о нарушениях.

Отчёт о расхождениях объёмов предназначен для выявления несоответствий между выездом и въездом. В отчёте указывается государственный регистрационный знак транспортного средства, номер разрешения, объект образования, объект приёма, объём при выезде, объём при въезде, расхождение в кубических метрах и процентах.

Отчёт об объектах образования ОСиС формируется для учёта объектов образования. В отчёте указывается наименование объекта, адрес, кадастровый номер, застройщик, подрядчик, вид работ (строительство, снос, реконструкция, благоустройство), период работ, заявленный объём ОСиС, фактически вывезенный объём, статус объекта и сведения о нарушениях.

Отчёт об объектах приёма ОСиС предназначен для учёта объектов приёма и их мощностей. В отчёте отражается наименование объекта, адрес, кадастровый номер, вид деятельности, номер и срок действия лицензии, применяемые технологии, проектная мощность, остаточная мощность, процент загрузки, количество принятых ОСиС и сведения о нарушениях.

Отчёт о загрузке объектов приёма служит для анализа загруженности полигонов. В отчёте указывается объект приёма, проектная мощность, остаточная мощность, процент загрузки, динамика за период и прогноз заполнения.

Аналитический отчёт по видам ОСиС формируется для анализа структуры отходов. В отчёте указывается вид ОСиС, группа однородных отходов, класс опасности, объём в кубических метрах, вес в тоннах, доля в общем объёме в процентах, направления утилизации и динамика.

Аналитический отчёт по классам опасности предназначен для анализа распределения отходов по классам. В отчёте отражается класс опасности, объём, доля, объекты образования, объекты приёма.

Аналитический отчёт по направлениям утилизации служит для анализа способов обращения с ОСиС. В отчёте указывается направление (обработка, утилизация, обезвреживание, размещение), объём, доля, объекты приёма.

Аналитический отчёт по участникам служит для анализа деятельности участников оборота ОСиС. В отчёте указывается участник (наименование, ИНН, роль), количество разрешений, объём перемещённых ОСиС, количество нарушений, рейтинг и динамика.

Отчёт о нарушениях правил обращения с ОСиС формируется для учёта и анализа нарушений. В отчёте указывается период, вид нарушения, дата и время, место, участник, государственный регистрационный знак транспортного средства, номер разрешения (при наличии), статус (новое, в работе, закрыто).

Отчёт о нарушениях по типам предназначен для анализа структуры нарушений. В отчёте отражается тип нарушения (отклонение от маршрута, несанкционированная остановка, отсутствие разрешения, превышение объёма), количество, доля, участники.

Отчёт о повторных нарушениях служит для выявления систематических нарушителей. В отчёте указывается участник, количество нарушений, даты нарушений, виды нарушений.

Отчёт о транспортных средствах формируется для учёта транспортных средств, используемых для перевозки ОСиС. В отчёте указывается государственный регистрационный знак, марка и модель, грузоподъёмность, вместимость кузова, отходоперевозчик, наличие ГЛОНАСС/GPS, наличие БНСО, количество рейсов и сведения о нарушениях.

Отчёт о рейсах транспортных средств предназначен для детального анализа рейсов. В отчёте отражается номер рейса, государственный регистрационный знак транспортного средства, отходоперевозчик, объект образования, объект приёма, дата и время выезда, дата и время въезда, объём, статус и сведения о нарушениях.

Сводный отчёт по региону формируется для получения общей картины по региону. В отчёте указывается общий объём образованных ОСиС, общий объём перемещённых ОСиС, общий объём размещённых ОСиС, количество объектов образования, количество объектов приёма, количество выданных разрешений, количество нарушений, рейтинг участников и динамика.

Отчёт о рейтинге участников служит для публикации рейтинга. В отчёте указывается участник, роль, рейтинг (от 0 до 5), категория (отличный, хороший, удовлетворительный, плохой), количество нарушений и динамика.

Отчёт по конкретному разрешению формируется для предоставления детальной информации по разрешению. Включает все данные разрешения, рейсы, объёмы, нарушения и статус закрытия.

Отчёт по конкретному объекту формируется для предоставления детальной информации по объекту. Включает все данные объекта, разрешения, рейсы, объёмы и нарушения.

Отчёт по конкретному участнику формируется для предоставления детальной информации по участнику. Включает все данные участника, объекты, разрешения, рейсы, нарушения и рейтинг.

Отчёт по конкретному транспортному средству формируется для предоставления детальной информации по транспортному средству. Включает все данные транспортного средства, рейсы, треки и нарушения.

Также отчеты должны быть доступными для просмотра и скачивания в личном кабинете пользователей с соответствующими правами доступа.

4.3.2.15 Требования к картографическому отображению и геоинформационным функциям

Подсистема должна обеспечивать отображение на географической карте объектов образования ОСиС, объектов приема ОСиС, маршрутов движения транспортных средств, осуществляющих транспортирование ОСиС, а также границ зон с особыми условиями использования территорий. Картографическая основа должна быть актуализированной, масштабируемой и поддерживать наложение слоев с различной информацией. Пользователи

подсистемы должны иметь возможность просматривать объекты на карте, фильтровать их по типам, статусам, видам ОСиС, а также получать справочную информацию по каждому объекту. Подсистема должна поддерживать построение маршрутов движения транспортных средств с учётом ограничений и запретов, а также визуализацию отклонений от маршрута.

Также предоставлять интерактивную географическую карту с возможностью наложения различных информационных слоёв: объекты образования ОСиС с цветовой индикацией статуса (активные, завершённые, проблемные); объекты приема ОСиС с отображением остаточной мощности и загрузки; активные разрешения и рейсы с маршрутами движения; зоны с ограничениями и запретами на транспортирование; статистика по объёмам ОСиС в разрезе муниципальных образований. Пользователи должны иметь возможность фильтровать объекты по типам, статусам, объёмам, периодам времени, а также получать всплывающие подсказки с ключевой информацией при наведении на объект.

4.3.2.16 Требования к формированию рейтинга участников информационного взаимодействия

Подсистема должна автоматически формировать рейтинг участников оборота ОСиС на основе объективных показателей: соблюдение сроков и правил транспортирования, полнота и своевременность предоставления данных, количество нарушений и предписаний, рейтинг должен быть открытым для всех участников информационного взаимодействия и публиковаться в личных кабинетах с возможностью сортировки и фильтрации.

4.3.2.17 Требования к аналитическим дашбордам

Подсистема должна предоставлять набор интерактивных дашбордов для руководства Министерства и уполномоченного органа, отображающих ключевые показатели в режиме реального времени. Дашборды должны включать: общий объём ОСиС, образованных и перемещённых по периодам;

динамику выдачи и закрытия разрешений; распределение ОСиС по видам, группам и классам опасности; загрузку объектов приема и остаточные мощности; рейтинг участников и количество нарушений; географическое распределение потоков ОСиС по территории Пермского края. Дашборды должны настраиваться под конкретные задачи, поддерживать фильтрацию и детализацию до уровня отдельных объектов и рейсов, а также автоматически обновляться при поступлении новых данных.

4.4 Общие технические требования к Системе

4.4.1 Требования к функционированию системы

4.4.1.1 Требования к режимам функционирования Системы

Система должна функционировать в следующих режимах:

1. штатный режим, при котором обеспечивается выполнение задач в объеме функций, предусмотренных настоящим техническим заданием;
2. сервисный режим, необходимый для проведения обслуживания, реконфигурации и пополнения технических и программных средств Системы новыми компонентами;
3. аварийный режим работы.

В штатном режиме функционирования Система должна обеспечивать следующий режим работы: доступность функций Системы в режиме — 24 часа в день, 7 дней в неделю (24x7), с учетом перерывов на проведение работ по техническому и сервисному обслуживанию Системы. Круглосуточный режим работы системы не требует организации круглосуточной работы пользователей и допускает работу пользователей в соответствии со штатным расписанием.

В сервисном режиме Система должна обеспечивать возможность проведения следующих работ:

1. техническое обслуживание;
2. модернизацию аппаратно-программного комплекса;
3. устранение аварийных ситуаций.

Система переходит в аварийный режим при возникновении нештатной ситуации и невозможности штатной работы. В случае перехода Системы в

аварийный режим, обслуживающему персоналу необходимо перевести Систему в сервисный режим в соответствии с инструкциями, изложенными в руководстве Администратора системы.

Программное обеспечение Системы должно восстанавливать своё функционирование при корректном перезапуске аппаратных средств. Должна быть предусмотрена возможность организации автоматического и (или) ручного резервного копирования данных системы средствами системного и базового программного обеспечения (ОС, СУБД), входящего в состав программно-аппаратного комплекса РНИС ПК.

4.4.1.2 Перспективы развития, модернизации Системы

Система должна предусматривать реализацию возможности дальнейшего развития как СПО, так и КТС, возможности развития Системы в соответствии с изменениями в действующем законодательстве, потребностях Функционального заказчика.

Система должна допускать расширение, изменение функциональных возможностей за счет разработки, переработки \ модификации, адаптации или приобретения дополнительных функциональных компонент и приобретения дополнительных лицензий на ПО, СПО, а также изменения аппаратной части (используемых технических средств)

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

4.4.2.1 Требования к численности и квалификации персонала Системы

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

В состав персонала, необходимого для эксплуатации Системы, входят:

1. администратор Системы;
2. администратор баз данных.

Помимо наличия базовых навыков работы на персональном компьютере, к обслуживающему персоналу предъявляются следующие требования:

3. знание принципов построения систем управления базами данных;
4. наличие навыков работы с серверным и телекоммуникационным оборудованием;
5. наличие расширенных знаний в области поддержки пользователей;
6. знание основ администрирования операционных систем, серверов приложений и серверов баз данных.

Уровень квалификации обслуживающего персонала должен соответствовать требованиям производителей программного обеспечения и технических средств Системы, а также требованиям эксплуатационной документации.

4.4.2.2 Требования к квалификации пользователей Системы

Пользователи Системы должны обладать квалификацией, обеспечивающей:

1. базовые навыки работы на персональном компьютере с современными операционными системами (клавиатура, мышь, управление окнами и приложениями, файловая система);
2. базовые навыки использования интернет-браузера (настройка типовых конфигураций, установка подключений, доступ к web-сайтам, навигация, формы и другие типовые интерактивные элементы web-интерфейса);
3. знание основ информационной безопасности.

4.4.3 Показатели назначения

Система должна обеспечивать достижение следующих показателей назначения (Таблица 5) при соответствии технического и общесистемного программного обеспечения требованиям, установленным в настоящем документе.

Таблица 5 – Показатели назначения

№ п/п	Наименование показателя	Условие	Единица измерения
1	Суммарное время недоступности Системы и ее компонентов в течение года	не более 24	часы
2	Суммарное время недоступности функций по информационному обмену с СПО для Системы в течение года	не более 8	часы
3	Суммарное время частичной или полной	не более 4	часы

№ п/п	Наименование показателя	Условие	Единица измерения
	невозможность информационного взаимодействия с внешними Системами в течение года		
4	Снижение быстродействия СПО (время отклика СПО на операции в Системе	Не более 5	секунды
5	Максимальная продолжительность недоступности Системы или ее любого компонента	не более 4	часы
6	Минимальное время между периодами недоступности Системы или ее компонентов	не менее 90	дни
7	Количество зарегистрированных пользователей	не менее 8 000	пользователь
8	Количество зарегистрированных транспортных средств	не менее 8 000	транспортных средств
9	Количество зарегистрированных БНСО	не менее 8 000	БНСО
10	Максимальное число запросов, одновременно направляемых пользователями к пользовательским интерфейсам Системы, в секунду	не менее 2 000	запросов
11	Время отклика пользовательских интерфейсов Системы на любой запрос пользователя при максимальном числе запросов	не более 15	сек
12	Объемы хранимых данных в Системе	не менее 5	Тб
13	Число объектов учета в Системе	не менее 10 000 000	шт
14	Система должна обеспечивать сохранение производительности при ежемесячном приросте данных в хранилище	не менее 1000	Гб

4.4.4 Требования к надежности

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

Программное обеспечение Системы должно обладать надежностью, обеспечивающей работу пользователей в произвольном режиме и оперативное восстановление работоспособности при сбоях.

В целях обеспечения надежного функционирования программное обеспечение Системы должно предусматривать:

1. обеспечение отказоустойчивого доступа пользователей и недоступности функций по информационному обмену СПО с внешних информационных систем;
2. балансировщиков нагрузки, в части предоставления доступа пользователям и внешним информационным системам к функциям Системы;
3. автоматическое перенаправление запросов на рабочие узлы в случае отказа работоспособности;
4. автоматическое восстановление полной работоспособности серверной части после удачного перезапуска ОС при сбоях в работе аппаратной части, приводящих к перезагрузке ОС сервера Системы;
5. сохранение работоспособности программного обеспечения при некорректных действиях пользователей;
6. стабильность работы в многопользовательском режиме.

С целью обеспечения надежного функционирования и анализа при нештатных ситуациях в Системе должны быть предусмотрены следующие опции:

1. Круглосуточная работа функций логирования по информационному обмену СПО с внешних информационных систем в разрезе ТС с архивом хранения 30 суток;
2. Круглосуточная работа функций логирования работы СПО с архивом хранения 30 суток;
3. Автоматическое ежедневное резервное копирование базы данных в 4 экземплярах (ПО предоставляется Заказчиком);
4. возможность восстановления данных из резервной копии при нештатном завершении работы Системы;
5. контроль целостности данных.

Описание работы всех перечисленных механизмов должно быть внесено в эксплуатационную документацию на Систему.

Система должна сохранять работоспособность при корректном функционировании комплекса технических средств Системы.

При возникновении сбоев КТС, включая аварийное отключение электропитания, должно обеспечиваться автоматическое восстановление

работоспособности СПО Системы после устранения сбоев и корректного перезапуска КТС (за исключением случаев повреждения рабочих носителей информации с исполняемым программным кодом или хранилищами данных).

Критерии отказа Системы и (или) ее компонентов определяются:

1. средним временем наработки на отказ (время работы системы без сбоев) не менее 4320 часов;
2. средним временем восстановления работоспособности (после сбоев) не более 2 часов.

4.4.5 Требования к безопасности

Требования безопасности оборудования, электробезопасности, пожарной безопасности и общие требования к управлению охраной труда в соответствии с государственными стандартами Российской Федерации в области безопасности труда в части серверов Системы должны обеспечиваться Государственным Заказчиком в помещениях эксплуатации Системы.

Доступ к данным должен быть предоставлен только авторизованным пользователям с учётом их служебных полномочий, а также с учётом категории запрашиваемой информации.

Технические средства, обеспечивающие хранение информации, должны использовать современные технологии, позволяющие обеспечить повышенную надежность хранения данных и оперативную замену оборудования (распределённая избыточная запись/считывание данных, зеркалирование, независимые дисковые массивы, кластеризация).

Дополнительных требований не предъявляется.

4.4.6 Требования к эргономике и технической эстетике

Взаимодействие пользователей с Системой должно осуществляться посредством визуального графического интерфейса.

Интерфейс Системы не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение web-форм. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Интерфейс должен соответствовать современным эргономическим требованиям, типичным для

современных web-приложений, быть интуитивно понятным и обеспечивать простой и удобный доступ к основным функциям и операциям Системы.

Интерфейс должен быть рассчитан на использование как персональных рабочих станций, так и переносных компьютеров (ноутбуков) или планшетных компьютеров, а также на использование мобильных телефонов. Управление Системой должно осуществляться с помощью набора экранных меню, кнопок, значков и прочих графических элементов. Клавиатурный режим ввода должен использоваться при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений, зависящих от языка установленной операционной системы) должны быть на русском языке. Набор символов – кириллица. Цифровая информация должна отображаться арабскими цифрами.

Интерфейс Системы должен быть направлен на:

1. минимизацию производимых пользователем операций при переходе из одной подсистемы в другую, из одной страницы Системы в другую, от одной операции к другой (то есть должен быть эргономичным);
2. сокращение времени отклика Системы на действия пользователя (при выполнении длительных операций пользователь должен получать предупреждение о предстоящем времени ожидания, а в процессе выполнения операции видеть на экране динамику процесса).

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных параметров. В указанных случаях Система должна будет выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

4.4.7 Требования к защите информации от несанкционированного доступа

4.4.7.1 Требования к конфиденциальности

Информация, предоставляемая Подрядчику с целью выполнения работ, является конфиденциальной и не должна передаваться третьим лицам без предварительного письменного разрешения Заказчика и не иначе, как для исполнения обязательств в рамках ГК, приложением к которому является настоящее ТЗ.

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

Подрядчик обязан использовать доступ к информационным ресурсам Заказчика, Функционального заказчика только в целях выполнения работ, не копировать, не размножать и не распространять в любой форме любые материалы, содержащиеся на рабочих местах, серверах и прочих средствах хранения информации Заказчика, Функционального Заказчика.

Имена и пароли, используемые Подрядчиком атрибуты доступа и иная предоставленная Заказчиком для выполнения работ в рамках настоящего ТЗ информация:

1. должна передаваться с использованием способов, исключающих возможность несанкционированного доступа к информации третьих лиц;
2. не должна храниться в каком-либо электронном виде у Подрядчика (кроме случаев, когда это необходимо для выполнения работ);
3. должна быть уничтожена Подрядчиком по окончании выполнения работ.

Подрядчик должен ограничить круг лиц, привлекаемых к выполнению работ в рамках настоящего ТЗ, а также предоставлять минимально достаточный уровень доступа уполномоченным специалистам в зависимости от должностных обязанностей в рамках выполнения работ.

4.4.7.2 Общие требования по обеспечению информационной безопасности

Применяемые Подрядчиком в ходе выполнения работ меры обеспечения информационной безопасности должны быть достаточными для предотвращения рисков, связанных с возможным нарушением конфиденциальности, целостности и доступности информации, содержащейся в Системе.

Если по вине Подрядчика произошло нарушение конфиденциальности, целостности или доступности информации, содержащейся в Системе, то Подрядчик несет ответственность за такое нарушение в соответствии с законодательством Российской Федерации.

При выполнении работ в течение всего срока действия ГК доступ Подрядчика к ресурсам Заказчика должен осуществляться только по защищенному каналу связи и должен быть прекращен сразу после окончания выполнения работ.

Защищенный канал должен быть построен с использованием СКЗИ. СКЗИ (VipNet № 1321 АО «Инфотекс», <https://infotecs.ru>) приобретается Подрядчиком самостоятельно и за свой счет. В соответствии с п. 1 ч. 1 статьи 33 Федерального закона от 05.04.2013 №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» приобретение эквивалента не допустимо в связи с необходимостью обеспечения совместимости и взаимодействия с эксплуатируемой Заказчиком системой криптографической защиты информации и защищенной сетью VipNet.

По требованию Заказчика и с целью повышения защищенности ресурсов Системы порядок предоставления доступа к ресурсам Заказчика может быть усилен дополнительными мерами по защите информации с предварительным уведомлением Подрядчика не менее, чем за 7 календарных дней. Реализация дополнительных мер обеспечивается Заказчиком.

К АРМ Подрядчика, с которых осуществляется подключение к ресурсам Заказчика, размещенным в ЦОД ППК, должна быть:

- исключена возможность несанкционированного доступа третьих лиц;
- обеспечена антивирусная защита информации.

При разработке программного кода Подрядчик должен применять методы безопасного программирования, включающие:

- ручную и автоматизированную проверку кода на предмет недокументированных (не декларированных) возможностей;
- анализ исходного кода на наличие уязвимостей и их устранение;
- анализ используемых зависимостей (библиотек, пакетов, модулей) на наличие уязвимостей.

Заказчик оставляет за собой право провести собственную экспертизу исходного кода сертифицированным сканером исходного кода.

Система должна обеспечивать возможность защиты информации в Системе от потери и несанкционированного доступа.

Развертывание Системы в ЦОД ППК должно производиться на сертифицированных ОС. При этом должны применяться сертифицированные СУБД. Допускается применение СУБД, сертифицированных в составе ОС. Состав применяемых ОС и СУБД должен быть согласован с Заказчиком и предоставлен Заказчиком.

Публикация Системы должна быть реализована с использованием сертифицированного межсетевого экрана уровня приложений Заказчика, установленного в ЦОД ППК.

В Системе должна быть обеспечена отправка логов в SIEM Заказчика по стандарту syslog (перечень необходимой информации для отправки уточняется Заказчиком после заключения ГК). При развитии Системы должны быть соблюдены требования Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

При отнесении Региональной навигационно-информационной системы Пермского края (РНИС ПК) к объектам критической информационной инфраструктуры (ОКИИ) в соответствии с 187-ФЗ, Подрядчик и Заказчик обязаны выполнить следующие мероприятия:

- Подрядчику необходимо провести категорирование РНИС ПК согласно Постановлению Правительства Российской Федерации № 127 от 8 февраля 2018 г. «Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской

Федерации и их значений», с присвоением категории значимости (1, 2 или 3) или не присвоения ни одной из категорий.

- Подрядчику необходимо результаты проведения категорирования отразить в Акте категорирования. Исходя из разработанного акта категорирования Подрядчик заполняет форму сведений, утвержденную Приказом ФСТЭК России №236 от 22 декабря 2017 г. «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

- Заказчик направляет заполненную форму сведений в управление ФСТЭК России по Приволжскому федеральному округу.

- При изменении параметров системы категория подлежит пересмотру.

При отнесении Региональной навигационно-информационной системы Пермского края (РНИС ПК) к объектам критической информационной инфраструктуры (ОКИИ) в мероприятиях по аттестации необходимо учитывать требования, предъявляемые к ОКИИ.

4.4.7.3 Требования к актуализации модели угроз безопасности информации

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Модель угроз безопасности информации должна быть разработана в соответствии с «Методикой оценки угроз безопасности информации», утвержденной ФСТЭК России 5 февраля 2021 г.

Модель угроз безопасности информации Системы должна включать:

- 1) Общие положения.
- 2) Описание Системы (сегментов Системы) и особенностей ее функционирования:
 - Цели и задачи, решаемые Системой (сегментом Системы).

- Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных.
 - Номенклатура защищаемых данных, обрабатываемых в Системе (подсистеме) и функциональных задач, для решения которых они используются.
 - Назначение и структура объектов информатизации (сегментов) Системы.
 - Описание структурно-функциональных характеристик информационной системы (состав технических и программных средств Системы, сетевая инфраструктура).
 - Описание взаимосвязей с другими информационными системами (подсистемами) и телекоммуникационными сетями.
 - Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа.
 - Описание процессов обеспечения информационной безопасности.
 - Описание технологии обработки информации.
 - Информация о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных.
- 3) Возможные негативные последствия от реализации (возникновения) угроз безопасности информации:
- Описание рисков (ущербов) от нарушения или прекращения основных процессов.
 - Описание негативных последствий, приводящих к возникновению рисков (ущерба).
- 4) Источники угроз безопасности информации (модель нарушителя):
- Характеристика нарушителей и возможные цели реализации ими угроз безопасности информации.
 - Категории актуальных нарушителей.
 - Описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.

- 5) Способы реализации (возникновения) угроз безопасности информации:
 - Описание способов реализации (возникновения) угроз безопасности информации.
 - Описание интерфейсов объектов воздействия.
- 6) Актуальные угрозы безопасности информации, включая:
 - Перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей.
 - Описание возможных сценариев реализации угроз безопасности информации.
 - Выводы об актуальности угроз безопасности информации.
- 7) Перечень актуальных угроз информационной безопасности.
- 8) Выводы о необходимом к применению (или его отсутствии) классе СКЗИ.

При идентификации возможных угроз безопасности информации должен использоваться Банк данных угроз безопасности информации, сформированный ФСТЭК России (<http://bdu.fstec.ru/>), учитывая структурно-функциональные особенности Системы, возможные источники угроз.

4.4.8 Требования по сохранности информации при авариях

Для развиваемых или вновь создаваемых подсистем должно предусматриваться автоматическое восстановление обрабатываемой информации в следующих аварийных ситуациях:

1. программный сбой при операциях записи/чтения;
2. программные сбои при передаче пакетов информации в смежные системы;
3. разрыв связи с клиентской программой (терминальным устройством) в ходе редактирования/обновления информации.

В Системе должна предусматриваться возможность ручного восстановления обрабатываемой информации из резервной копии в следующих аварийных ситуациях:

4. физический выход из строя дисковых накопителей;

5. ошибочные действия обслуживающего персонала.

В Системе должно предусматриваться автоматическое восстановление работоспособности серверной части Системы в следующих ситуациях:

6. штатное и аварийное отключение электропитания серверной части;
7. штатная перезагрузка Системы и загрузка после отключения;
8. программный сбой общесистемного программного обеспечения, приведший к перезагрузке системы;
9. программный сбой после обновления программного обеспечения.

В Системе должно предусматриваться полуавтоматическое восстановление работоспособности серверной части Системы в следующих аварийных ситуациях:

10. физический выход из строя любого аппаратного компонента, кроме дисковых накопителей – после замены компонента и восстановления конфигурации общесистемного программного обеспечения;
11. аварийная перезагрузка системы, приведшая к нефатальному нарушению целостности файловой системы – после восстановления файловой системы.

4.4.9 Требования к патентной чистоте

Целью выполнения работ согласно ТЗ является развитие РНИС ПК (информационная система в значении, установленном статьей 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», включающая в себя в том числе охраняемые согласно части 4 Гражданского кодекса Российской Федерации программы для ЭВМ базы данных, иные результаты интеллектуальной деятельности).

Использование программного обеспечения должно осуществляться, в том числе, в соответствии с требованиями Гражданского кодекса РФ, Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В рамках работ в соответствии с ТЗ необходима разработка (переработка/модификация) специального программного обеспечения Системы. В соответствии с Гражданским кодексом Российской Федерации, Законом Пермского края от 25 декабря 2009 г. № 569-ПК «Об управлении и распоряжении

интеллектуальной собственностью Пермского края», право на получение патента и исключительные права на результат интеллектуальной деятельности, созданный при выполнении работ по государственному контракту, включая без ограничения специальное программное обеспечение, базы данных, документы и материалы, иные результаты интеллектуальной деятельности, созданные по настоящему ТЗ, а также при выполнении работ по настоящему ТЗ, подлежат передаче Заказчику в связи с тем, что указанные результаты интеллектуальной деятельности необходимы для предоставления государственных (муниципальных) услуг и(или) для осуществления государственных (муниципальных) функций.

Заказчик после заключения ГК в рабочем порядке предоставляет Подрядчику техническую и эксплуатационную документацию на Систему и иные документы, необходимые для выполнения работ в срок не позднее 5 рабочих дней с даты получения запроса от Подрядчика.

Результаты выполнения работ по настоящему ТЗ должны быть совместимы на уровне программного, технического, информационного и других видов обеспечения с результатами работ по созданию и развитию Системы, выполнявшимися в рамках предшествующих договоров на выполнение работ по созданию и развитию информационных систем.

Используемое в целях развития Системы программное обеспечение должно иметь соответствующие лицензии на его использование и быть свободным от обязательств перед третьими лицами.

Программы для ЭВМ, требующие каких-либо отчислений, закупаются Подрядчиком самостоятельно с учетом требований к исключительным и неисключительным правам, предусмотренным настоящим ТЗ (стоимость приобретения таких прав включена в цену государственного контракта).

В случае, если в процессе выполнения работ Подрядчик использует программы для электронных вычислительных машин, включая без ограничения системы управления базами данных, программные библиотеки, сервера приложений, и иные результаты интеллектуальной деятельности (далее – результаты интеллектуальной деятельности), разработанные третьими лицами, не подразумевающие свободного использования, либо в случае, если для использования результатов работ по ГК (эксплуатации Системы) требуются такие

результаты интеллектуальной деятельности, права (исключительные или неисключительные) на использование таких результатов интеллектуальной деятельности должны быть переданы Заказчику в объеме, необходимом для использования результатов работ по ТЗ всеми пользователями Системы в соответствии с требованиями законодательства РФ (стоимость передачи таких прав Заказчику включена в цену государственного контракта). Программные средства должны быть обеспечены гарантийным и постгарантийным обслуживанием фирмы-производителя (правообладателя).

Передаваемые права на результаты интеллектуальной деятельности третьих лиц, включая программы для ЭВМ, должны соответствовать требованиям к составу, количеству и характеристикам ПО, необходимого для доработки Системы, представленным в рамках настоящего ТЗ. Объем передаваемых прав должен обеспечивать возможность использования Системы на всей территории Пермского края всеми пользователями Системы. Срок действия прав – бессрочно, либо на срок действия исключительных прав. Состав прав должен допускать модификацию, модернизацию ПО с привлечением Заказчиком третьих лиц

При этом в составе ПО должны преимущественно использоваться программы для ЭВМ, подразумевающие свободное использование и обеспеченные поддержкой производителя (разработчика) и не накладывающие ограничений по использованию Системы. Программы для ЭВМ, не подразумевающие свободного использования, должны быть обеспечены гарантийным и постгарантийным обслуживанием фирмы-производителя (правообладателя), соответствующие права должны быть переданы Заказчику.

До начала работ Подрядчик должен уведомить Заказчика о результатах интеллектуальной деятельности, имеющих правовую охрану, принадлежащих Подрядчику, или третьим лицам, которые планируется использовать при выполнении работ в соответствии с ТЗ, а также об объеме имеющихся у Подрядчика прав на указанные результаты интеллектуальной деятельности и возможности предоставления Заказчику указанных прав.

В таком случае развитие Системы должно осуществляться исключительно с использованием программ для ЭВМ, соответствующих требованиям действующего законодательства Российской Федерации, устанавливающего национальный режим.

Риск нарушения прав третьих лиц на результаты интеллектуальной деятельности несет Подрядчик. В случае предъявления к Заказчику претензий со стороны правообладателей Подрядчик обязуется такие претензии урегулировать самостоятельно и/или возместить Заказчику убытки в этой связи.

Все созданные и использованные при исполнении ГК результаты интеллектуальной деятельности подлежат отражению в отчетных документах Подрядчика о результатах выполнения работ по ГК.

Программы для ЭВМ, а также иные результаты интеллектуальной деятельности, используемые в рамках выполнения работ по-настоящему ТЗ, должны иметь соответствующие лицензии на их использование и не должны нарушать прав третьих лиц. Средства, входящие в состав программного и технического обеспечения Системы, в случае приобретения их у сторонних фирм и предприятий, должны сопровождаться документацией, подтверждающей право этих организаций поставлять данную продукцию, и лицензионными соглашениями (в установленных законом случаях). Система должна функционировать в среде лицензионного серверного программного обеспечения.

Исключительные права на разработанное в результате работ по развитию Системы ПО, СПО, а также иные права, необходимые для нормальной эксплуатации Системы по ее непосредственному назначению, передаются Подрядчиком Заказчику путем подписания акта приема-передачи исключительных прав на результаты интеллектуальной деятельности по государственному контракту. Стоимость передаваемых прав входит в цену государственного контракта, приложением к которому является настоящее ТЗ.

Заказчик после заключения ГК предоставляет Подрядчику права использования ПО Системы, правообладателем которой является Пермский край в лице Заказчика, для использования в рамках исполнения ГК (далее – ПО Заказчика), безвозмездно на срок выполнения работ по ГК на условиях простой (неисключительной) лицензии в целях выполнения работ, предусмотренных ГК. Подрядчик имеет право использовать ПО Заказчика на территории Российской Федерации в рамках выполнения работ по ГК следующими способами: инсталляция, запуск, воспроизведение, модификация, переработка, доработка, адаптация. Подрядчик имеет право предоставить права использования ПО Заказчика

субподрядчикам для целей выполнения работ по ГК при письменном согласии Заказчика на такое предоставление прав использования. Стороны признают и соглашаются, что данные положения Технического задания признаются лицензионным договором.

4.4.10 Требования по стандартизации и унификации

В требования по стандартизации и унификации должны быть включены показатели, устанавливающие:

1. требуемую степень использования стандартных, унифицированных методов реализации функций (задач) системы, поставляемых программных средств, типовых математических методов и моделей, типовых проектных решений, унифицированных форм управленческих документов, общесоюзных классификаторов технико-экономической информации и классификаторов других категорий в соответствии с областью их применения,
2. требования к использованию типовых автоматизированных рабочих мест, компонентов и комплексов].

Экранные формы должны проектироваться с учетом требований унификации:

1. все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;
2. для обозначения одних и тех же операций должны использоваться одинаковые графические значки, кнопки и другие управляющие (навигационные) элементы;
3. должны быть унифицированы термины, используемые для описания идентичных понятий, операций и действий пользователя;
4. реакция системы на действия оператора (наведение указателя «мыши», переключение фокуса, нажатие кнопки) должна быть типовой для каждого действия над одними и теми же графическими элементами, независимо от их расположения на экране.

4.5 Требования к видам обеспечения

4.5.1 Требования к информационному обеспечению

4.5.2 Требования к лингвистическому обеспечению

Все экранные формы, выходные формы, инструкции по работе, вся документация должны быть выполнены на русском языке. Исключения могут составлять только системные сообщения, не подлежащие русификации. Набор символов – кириллица. Цифровая информация должна быть отражена арабскими цифрами.

4.5.3 Требования к программному обеспечению

В состав общесистемного программного обеспечения должны входить программные средства операционной системы, средства интеграции, системы управления базами данных и пр. Совокупность данных программных средств должна обеспечивать открытую архитектуру Системы.

Общесистемное программное обеспечение должно обеспечивать:

1. штатное функционирование комплекса технических средств Системы;
2. функционирование специального программного обеспечения;
3. взаимодействие с периферийными устройствами;
4. сетевое взаимодействие;
5. другие необходимые общесистемные функции.

Операционные системы, СУБД должны быть определены Подрядчиком по согласованию с Заказчиком и описаны в документе «Описание архитектуры системы».

Специальное программное обеспечение должно отвечать следующим требованиям:

1. высокая степень готовности для решения поставленных задач;
2. возможность работы программных продуктов в сетях общего пользования;
3. преимущественное использование свободного программного обеспечения;

4. совместимость программных продуктов в части используемых технических средств, системного программного обеспечения и общесистемной инфраструктуры в пределах требований к техническому обеспечению, а также их информационная совместимость в пределах требований к информационному обмену.

Требования к системному программному обеспечению должны быть определены на предварительном и технорабочем проектировании.

4.5.4 Требования к техническому обеспечению

Архитектура Системы должна быть разработана в соответствии с трехуровневой клиент-серверной архитектурой и состоять из следующих уровней:

1. уровень хранения данных;
2. уровень приложений;
3. презентационный уровень, обеспечивающий взаимодействие с клиентскими приложениями.

Технические средства, необходимые для размещения разрабатываемого решения, предоставляются Заказчиком.

Требования к техническому обеспечению должны быть уточнены при разработке частного технического задания на развитие Системы.

Подрядчик должен сформулировать предложение по размещению Системы, исходя из заданных параметров производительности, доступности и информационной безопасности. Предложение по размещению в части требуемых мощностей должно быть обосновано результатами нагрузочного тестирования и согласовано с Заказчиком.

4.5.5 Требования к организационному обеспечению

В ходе выполнения работ должно обеспечиваться постоянное взаимодействие между Подрядчиком и Заказчиком в части:

1. решения административных вопросов (организация встреч, предоставление допусков, рассмотрение и согласование документации и т.п.);

2. решения инженерно-технических вопросов (согласование технических аспектов реализации и администрирования Системы, определение наличия и размещения технических средств, коммуникаций и т.п.);
3. нормативно-методического и информационного обеспечения проектных работ (уточнение функциональных характеристик, предоставление дополнительных сведений).

Подрядчик по запросу Заказчика направляет специалиста(ов) на рабочие совещания и презентации. Запрос Заказчика на участие в совещании специалистов Подрядчика направляется не позднее 2 (двух) рабочих дней до срока проведения совещания/презентации. По согласованию с Заказчиком допускается проведение совещаний в онлайн-режиме.

5 Состав и содержание работ по развитию системы

5.1 Этапы выполнения работ

Этапы проведения работ по развитию Системы приведены ниже (Таблица 6).

Таблица 6 – Календарный план проведения работ по развитию Системы

№ этапа	Наименование и содержание выполняемых работ	Срок выполнения работ	Отчетная документация ¹⁾ и материалы
1.	Разработка ЧТЗ	Начало: с 11.01.2027 Окончание: 10.02.2027	- ЧТЗ, детализирующее требования; - Акт приема-передачи отчетной документации по этапу №1
2.	Разработка документации	Начало: с 11.02.2027 Окончание: 13.03.2027	- Технический проект Системы, включая: • Пояснительную записку к техническому проекту; • Описание архитектуры системы; • Описание автоматизируемых функций; • Описание информационного обеспечения системы; • Описание комплекса технических средств; • Описание программного обеспечения; • Ведомость технического проекта -Акт приема-передачи отчетной документации по этапу №2
3.	Разработка программного обеспечения, Разработка рабочей документации	Начало: с 14.03.2027 Окончание: 12.07.2027	- Рабочая документация в составе: • Ведомость эксплуатационных документов; • Актуализированное описание архитектуры (при внесении изменений); • Описание информационного массива; • Описание базы данных; • Руководство пользователя Системы;

№ этапа	Наименование и содержание выполняемых работ	Срок выполнения работ	Отчетная документация ¹ и материалы
			• Руководство функционального администратора; • Руководство системного администратора Системы; • Инструкция по развертыванию Системы; • Регламент гарантийного обслуживания; • Регламент эксплуатации системы; • План восстановления в случае аварии; • Паспорт; • Общее описание системы; • Регламент взаимодействия с внешними информационными системами (включая Паспорта информационного взаимодействия); - Исходные коды СПО и дистрибутивы ПО, СПО Системы; - Отчет по анализу исходного кода на наличие уязвимостей и их устранению - План-программа подготовки персонала (с приложением форм Отчета о подготовке персонала и Протокола подготовки персонала) - Акт приема-передачи отчетной документации по этапу №3
4.	Пусконаладочные работы, Проведение предварительных испытаний	Начало: с 13.07.2027 Окончание: 12.08.2027	- Программа и методика предварительных испытаний; - Акт о выполнении пуско-наладочных работ на тестовом стенде
5.	Опытная эксплуатация, (включая подготовку персонала системы)	Начало: с 13.08.2027 Окончание:	- Протокол предварительных испытаний; - Акт приемки Системы в опытную эксплуатацию - Доработанная документация и исходные коды/дистрибутив СПО Системы (при наличии замечаний по результатам предварительных испытаний) - Акт приема-передачи отчетной документации по этапу №4

№ этапа	Наименование и содержание выполняемых работ	Срок выполнения работ	Отчетная документация ¹ и материалы
		12.09.2027	- Отчет о проведении опытной эксплуатации (с приложением Журнала опытной эксплуатации); - Акт о завершении опытной эксплуатации и допуске к приемочным испытаниям - Акт приема-передачи отчетной документации по этапу №5
6.	Приемочные испытания	Начало: с 13.09.2027 Окончание: 27.09.2027	- Акт о выполнении пусконаладочных работ на промышленном стенде; - Программа и методика приемочных испытаний; - Программа и методика нагрузочных испытаний; - Протокол приемочных испытаний; - Протокол нагрузочных испытаний; - Акт о готовности Системы к вводу в эксплуатацию; - Доработанная документация и исходные коды/дистрибутив СПО Системы (при наличии замечаний по результатам опытной эксплуатации и приемочных испытаний); - Ведомость передаваемых файлов; - Акт приема-передачи исключительных прав на результаты интеллектуальной деятельности по государственному контракту; - Заполненные проекты заявок на государственную регистрацию прав заказчика на результаты интеллектуальной деятельности (по форме приложений №1-4 приказа Минэкономразвития России от 05.04.2016 № 211) на бумажном носителе, включая реферат, отвечающий требованиям приказа Минэкономразвития России от 05.04.2016 № 211; - Депонируемые материалы в электронной форме на машиночитаемом носителе в формате PDF/A, отвечающие требованиям приказа Минэкономразвития России от 05.04.2016 № 211; - Документы, подтверждающие отказ авторов (разработчиков) от исключительных прав на передаваемые объекты интеллектуальной собственности в пользу подрядчика; - Отчет по анализу исходного кода на наличие уязвимостей и их устранению (в случае внесения изменений в исходный код после опытной эксплуатации)

№ этапа	Наименование и содержание выполняемых работ	Срок выполнения работ	Отчетная документация ¹ и материалы
			и испытаний) - Акт приема-передачи отчетной документации по этапу №6
7.	Выполнение работ по защите информации	Начало: с 28.09.2027 Окончание: 12.10.2027	- Акт приема-передачи исключительных прав на результаты интеллектуальной деятельности по Заявке (в случае внесения изменений в Систему); - Заполненные проекты заявок на государственную регистрацию прав заказчика на результаты интеллектуальной деятельности (по форме приложений №1-4 приказа Минэкономразвития России от 05.04.2016 № 211) на бумажном носителе, включая реферат, отвечающий требованиям приказа Минэкономразвития России от 05.04.2016 № 211 (в случае внесения изменений в Систему); - Депонируемые материалы в электронной форме на машиночитаемом носителе в формате PDF/A, отвечающие требованиям приказа Минэкономразвития России от 05.04.2016 № 211 (в случае внесения изменений в Систему); - Документы, подтверждающие отказ авторов (разработчиков) от исключительных прав на передаваемые объекты интеллектуальной собственности в пользу подрядчика (в случае внесения изменений в Систему); - Ведомость передаваемых файлов; - Акт классификации системы - Акт определения уровня защищенности персональных данных системы; - Модель угроз информационной безопасности; - Модель нарушителя безопасности информации; - Частное техническое задание на систему защиты информации - Проектная документация на систему защиты информации: - ведомость технического проекта; - пояснительная записка к техническому проекту; - схема функциональной структуры; - схема структурная комплекса технических средств;

№ этапа	Наименование и содержание выполняемых работ	Срок выполнения работ	Отчетная документация ¹ и материалы
			- схема организационной структуры; - ведомость покупных изделий. - Эксплуатационная документация на систему защиты информации в составе: - Руководство администратора на систему защиты информации; - Руководство пользователя на систему защиты информации; - Инструкция по эксплуатации комплекса средств защиты информации и иных технических средств; - Технический паспорт; - Описание технологического процесса обработки информации - Акт приема-передачи неисключительных прав на СЗИ и/или СКЗИ (в случае внедрения системы защиты информации) - Акт установки СЗИ и/или СКЗИ (в случае внедрения системы защиты информации) - Программа и методики аттестационных испытаний - Протокол аттестационных испытаний (в случае изменения аттестованного объекта информатизации); - Заключение о соответствии Системы требованиям по защите информации - Отчет по анализу исходного кода на наличие уязвимостей и их устранению (при необходимости) - Аттестат соответствия требованиям информационной безопасности (в случае положительного заключения) - Акт приема-передачи отчетной документации по этапу №7

6 Порядок развития системы

В целях повышения эффективности и качества выполнения работ Заказчик вправе требовать от Подрядчика, а Подрядчик в свою очередь обязуется выполнять следующие требования Заказчика:

1. Загрузку проектных файлов (исходных кодов, файлов БД, конфигурационных файлов, библиотек и пр.) в СУРК Заказчика;
2. проверку исходных кодов в системе статического анализа кода Заказчика и устранение выявленных при этой проверке замечаний;
3. настройку скриптов для автоматизации процессов компиляции, создания дистрибутива (из исходных кодов, конфигурационных файлов, библиотек и пр.) и обновления приложений на серверах промышленного и тестового контуров Системы, средствами СУРК;
4. непосредственное участие представителей Подрядчика при выполнении предупредительно-плановой работы по выявлению необходимости осуществления в будущем изменений Системы в связи с готовящимися изменениями нормативно-правовых актов, изменений во внешних информационных системах, с которыми осуществлена интеграция Системы;
5. непосредственное участие представителей Подрядчика в работе по уточнению описанных требований и сбору/выявлению дополнительных требований к развитию Системы в объеме, достаточном для качественного выполнения задач;
6. непосредственное участие представителей Подрядчика во взаимодействии с представителями СТП внешних информационных систем по работам, касающимся информационного взаимодействия.

6.1 Требования к разработке документации

В рамках выполнения работ Подрядчик должен разработать частное техническое задание на развитие Системы, детализирующее требования настоящего ТЗ.

Порядок разработки, структура и содержание ЧТЗ должны соответствовать ГОСТ 34.602-2020 «Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы». ЧТЗ не должно дублировать положения настоящего ТЗ, а в случае такой необходимости должны

приводиться ссылки на соответствующие пункты ТЗ. В ЧТЗ Подрядчиком должны быть детализованы требования настоящего ТЗ до степени, позволяющей однозначно определить способ реализации каждого требования.

При описании процессов, структуры СПО, организации данных и функций СПО должны приводиться модели, разработанные с применением любых средств проектирования и в любой нотации, определенной Подрядчиком и согласованной с Заказчиком, но в рамках единой технологии моделирования.

ЧТЗ должно быть разработано Подрядчиком и согласовано с Заказчиком в сроки, указанные в п. 5.1 настоящего документа.

В рамках выполнения работ Подрядчик должен разработать документацию на Систему, указанную в п. 5.1 настоящего документа.

Документация технического проекта должна отражать характеристики СПО Системы, которое должны быть разработано согласно ТЗ.

Документ «Описание архитектуры системы» - При разработке документа должен использоваться язык моделирования архитектуры archimate.

6.2 Требования к разработке программного обеспечения и рабочей документации

Подрядчик должен выполнить работы по развитию Системы в объеме, указанном в разделе 5 настоящего документа, обеспечив его соответствие требованиям настоящего ТЗ и ЧТЗ.

Подрядчик должен выполнить работы по развитию Системы, а также настройку ОПО, используемого в рамках Системы.

Подрядчик в рамках выполнения работ должен обеспечить выполнение требований настоящего ТЗ без нарушения функционирования ранее разработанного функционала Системы.

В целях повышения эффективности и качества выполнения работ Заказчик имеет право требовать от Подрядчика, а Подрядчик в свою очередь обязуется выполнять следующие требования Заказчика:

1. загрузку проектных файлов (исходных кодов, конфигурационных файлов, библиотек и пр.) в СУРК;
2. непосредственное участие представителей Подрядчика при выполнении предупредительно-плановой работы по выявлению необходимости

осуществления в будущем изменений Системы в связи с готовящимися изменениями нормативно-правовых актов, изменений во внешних информационных системах, с которыми осуществлена интеграция Системы;

3. непосредственное участие представителей Подрядчика в работе по уточнению описанных требований и сбору/выявлению дополнительных требований к развитию Системы в объеме, достаточном для качественного выполнения задач;
4. непосредственное участие представителей Подрядчика во взаимодействии с представителями внешних информационных систем по работам, касающимся информационного взаимодействия.

По результатам разработки СПО Системы Подрядчик должен передать Заказчику исходный код и дистрибутив СПО Системы через СУРК. В состав дистрибутива должны входить предварительные конфигурационные настройки СПО Системы.

Передача исходных кодов, разработанных в ходе выполнения работ программ для электронных вычислительных машин (далее – программа для ЭВМ) и дистрибутивов должна сопровождаться передачей всех необходимых для сборки и запуска программы для ЭВМ библиотек зависимостей, инструкций и программных сценариев (скриптов) для проведения компиляции, создания дистрибутива и установки (развертывания) программы для ЭВМ.

Для проведения компиляции, создания дистрибутива и установки (развертывания) программы для ЭВМ должны использоваться свободно распространяемые компиляторы, интерпретаторы и иное программное обеспечение, необходимое для указанных целей, дистрибутивы которых должны быть переданы вместе с исходными кодами разработанных в ходе выполнения работ программ для ЭВМ.

В случае использования для проведения компиляции, создания дистрибутива и установки (развертывания) программы для ЭВМ компиляторов, интерпретаторов и иного программного обеспечения, права на использование, копирование и модификацию которых принадлежат третьим лицам, подрядчик за

свой счет передает Заказчику дистрибутивы и права на использование таких компиляторов, интерпретаторов и иного программного обеспечения.

Подрядчик в процессе сдачи-приемки работ по ГК должен провести демонстрацию процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ с использованием средств, указанных выше, а также в соответствии с инструкциями, приведенными в рабочей документации на Систему.

В рамках выполнения работ Подрядчик должен разработать рабочую документацию на Систему в составе, приведенном в п. 5.1 настоящего ТЗ. При этом содержание данной документации должно охватывать всю функциональность Системы, включая модернизированную в рамках выполнения работ функциональность.

«Документ «Описание архитектуры» должен соответствовать ГОСТ Р 57100-2025 Системная и программная инженерия. Описание архитектуры. При разработке документа должен использоваться язык моделирования архитектуры «archimate».

Документы «Руководство пользователя», «Руководство администратора» и другие документы, регламентирующие деятельность персонала, должны содержать описание выполнения операций (действий) персонала в технологическом процессе пользователя Системы, т.е. описание должно строиться на основе технологических задач персонала с использованием возможностей Системы и не должно сводиться к простому описанию (перечислению) функций Системы. При этом в указанных документах должна быть отражена работа всех функций по компонентам. Указанные документы должны содержать описание выполнения операций (действий) всех категорий пользователей с применением необходимых изображений экранных форм Системы.

6.3 Требования к проведению пусконаладочных работ и предварительных испытаний Системы

Предварительные испытания проводятся в соответствии с согласованной с Заказчиком «Программой и методикой предварительных испытаний». Проведение предварительных испытаний на технических средствах Подрядчика допускается только по согласованию с Заказчиком.

Работы по компиляции исходного кода, установки, обновлению и настройке ПО и СПО, производится Подрядчиком на инфраструктуре и в ПО Заказчика, путем использования СУРК предоставляемым Заказчиком.

Работы по установке и настройке СПО для проведения предварительных испытаний Системы осуществляет Подрядчик при взаимодействии со службой технической поддержки Системы, что должно фиксироваться в документе «Акт о выполнении пуско-наладочных работ на тестовом стенде», подписываемом Заказчиком и Подрядчиком.

Проведение пусконаладочных работ включает наладку программного обеспечения частей системы, загрузку информации в ее базу данных, комплексную наладку программного обеспечения системы, включая средства защиты информации.

«Программа и методика предварительных испытаний» должна включать тесты, позволяющие проверить:

1. соответствие ТЗ и ЧТЗ дистрибутива ПО, СПО и исходных кодов СПО Системы, предоставленных Подрядчиком;
2. все функции СПО Системы, предусмотренные ЧТЗ в рамках соответствующего этапа выполнения работ;
3. выполнение показателей назначения в части временных характеристик функционирования СПО Системы, установленных в п.4.4.3 настоящего ТЗ. Показатели назначения могут быть дополнены в рамках этапа «Разработка документации».

В ходе предварительных испытаний определяется полнота реализованных функций и документации на Систему.

Проверка полноты и корректности представленных исходного кода СПО и дистрибутива модернизированной Системы осуществляется на основании версий, переданных Заказчику через СУРК. Для этого специалистами Подрядчика в присутствии приёмочной комиссии производится сборка переданных дистрибутива ПО, СПО в соответствии с «Инструкцией по развертыванию».

Результаты предварительных испытаний фиксируются в «Протоколе предварительных испытаний», который подписывается всеми участниками испытаний. В «Протоколе предварительных испытаний» должны быть отражены

выявленные недостатки и сделан вывод о соответствии Системы требованиям настоящего ТЗ и ЧТЗ, а также о готовности Системы к проведению опытной эксплуатации.

В случае получения замечаний по итогам предварительных испытаний Системы Подрядчик должен провести работы по устранению полученных замечаний с высоким и средним уровнем критичности до запуска Системы в опытную эксплуатацию. Распределение замечаний по уровням критичности приведено в п.7.2.

При внесении изменений в СПО Системы по результатам предварительных испытаний Подрядчик должен внести соответствующие изменения и представить Заказчику исходные коды, дистрибутив СПО Системы, а также документацию (при необходимости), указанную в п.5.1 настоящего документа.

В случае отсутствия изменений в СПО Системы по результатам предварительных испытаний Подрядчик должен проинформировать Заказчика письмом, сообщив об отсутствии необходимости в корректировке исходных кодов СПО, дистрибутива ПО, СПО Системы.

6.4 Требования к проведению опытной эксплуатации

Опытная эксплуатация Системы проводится на технических средствах заказчика с целью проверки функционирования компонентов Системы в части реализации новой функциональности для выявления недостатков в работе Системы и их устранения, а также для обработки обращений пользователей по вопросам использования новой функциональности Системы.

Работы по установке и настройке ПО, СПО Системы для проведения опытной эксплуатации осуществляет Подрядчик.

Опытная эксплуатация Системы проводится в соответствии с разработанной и согласованной с Заказчиком «Программой опытной эксплуатации».

«Программа и методика опытной эксплуатации» должна включать требования к проведению опытной эксплуатации доработанной версии Системы и должна определять:

1. сроки проведения опытной эксплуатации;
2. состав объектов, на которых должна производиться опытная эксплуатация;

3. состав типов пользователей, участвующих в опытной эксплуатации Системы, и их количество;
4. условия и порядок функционирования Системы в рамках опытной эксплуатации;
5. порядок устранения замечаний к работе Системы, выявленных в процессе опытной эксплуатации;
6. иные требования к проведению опытной эксплуатации, предусмотренные настоящим ТЗ и ЧТЗ.

СПО Системы должно функционировать в объеме всех функций, предусмотренных ЧТЗ и реализованных в рамках выполнения работ.

Длительность опытной эксплуатации Системы определена в п. 5.1.

Состав пользователей, участвующих в опытной эксплуатации, фиксируются в «Программе и методике опытной эксплуатации».

Результаты обработки всех обращений пользователей Системы должны фиксироваться в «Журнале опытной эксплуатации».

«Журнал опытной эксплуатации» должен содержать следующие сведения:

1. регистрационный номер обращения;
2. способ поступления обращения (телефон, электронная почта);
3. контактные данные обратившегося пользователя (ФИО, организация/ведомство, должность);
4. дата и время поступления обращения;
5. описание содержания обращения;
6. дата и время окончательной отработки Подрядчиком обращения;
7. описание мер, принятых в связи с обращением.

Кроме того, в «Журнале опытной эксплуатации» должны фиксироваться факты обнаружения некорректной работы Системы, выявленные пользователями Системы, с указанием даты и времени события, описанием причин возникновения и мер, предпринятых для устранения.

СПО Системы с учетом выполненных доработок (дополнительных настроек) также передается Заказчику. По результатам выполнения работ Подрядчик должен передать Заказчику исходные коды и дистрибутив СПО Системы на оптическом

носителе с однократной записью. В состав дистрибутива должны входить предварительные конфигурационные настройки СПО Системы.

В случае если Заказчиком выдвинуто требование загрузки исходных кодов в репозиторий Заказчика, содержимое передаваемого носителя с однократной записью должно соответствовать репозиторию.

Работа завершается подписанием «Акта о завершении опытной эксплуатации Системы и допуске к приемочным испытаниям».

6.5 Требования к проведению пусконаладочных работ и приемочных испытаний

Приемочные испытания Системы проводятся на промышленном контуре, расположенном на технических средствах Заказчика в соответствии с согласованной с Заказчиком «Программой и методикой приемочных испытаний» путем выполнения предусмотренных в ней тестов.

«Программа и методика приемочных испытаний» должна включать тесты, позволяющие проверить выполнение всех положений ЧТЗ.

Проверка полноты и корректности представленных дистрибутива и исходного кода СПО Системы осуществляется аналогично п. 6.3 настоящего Технического задания.

Работы по установке и настройке СПО Системы для проведения приемочных испытаний осуществляет Подрядчик, что должно фиксироваться в документе «Акт о выполнении пуско-наладочных работ на промышленном стенде», подписываемом Заказчиком и Подрядчиком.

На испытания Подрядчиком должен быть представлен полный комплект документации, а также документы, подготовленные в рамках проведения опытной эксплуатации.

В программе и методике приемочных испытаний должна быть описана методика проведения нагрузочного тестирования по каждой из подсистем и порядок контроля данного тестирования.

Нагрузочное тестирование проводится на мощностях Заказчика в соответствии с разработанным документом «Программа и методика нагрузочных испытаний». Работы по установке и настройке СПО Системы для проведения

нагрузочных испытаний и приемочных испытаний осуществляет Подрядчик при взаимодействии со службой технической поддержки Системы.

Необходимо провести следующие виды нагрузочного тестирования:

1. тестирование производительности Системы;
2. стрессовое тестирование Системы.

Тестирование производительности Системы должно проводиться с постепенным увеличением нагрузки путем добавления новых пользователей через определенные интервалы времени.

Тестирование производительности Системы должно позволять определить:

3. время выполнения выбранных операций Системы при заданных (количество одновременно работающих пользователей) интенсивностях выполнения этих операций;
4. количество пользователей Системы, способных работать одновременно с заданными характеристиками отклика Системы;
5. границы приемлемой производительности при увеличении нагрузки на Систему (добавление новых пользователей);
6. производительность Системы при различных нагрузках (различное количество одновременно работающих пользователей).

Стрессовое тестирование Системы должно проводиться путем увеличения интенсивности операций выше пиковых значений (максимально разрешенных) или путем увеличения количества пользователей и количества вызовов веб-сервисов Системы до тех пор, пока нагрузка на Систему не станет выше максимально допустимых значений. После этого нагрузка на Систему должна быть снижена до средних значений с целью проверки способности Системы к возвращению из стрессового состояния в нормальное.

Подрядчик должен запустить процедуру нагрузочных испытаний в момент времени, согласованный с Заказчиком и Функциональным заказчиком.

Положительным результатом нагрузочных испытаний является выполнение показателей назначения в части функционирования Системы. В случае отрицательных результатов проводится доработка СПО/ОПО/Архитектуры системы для достижения целевых показателей указанных в п. 4.4.3.

Подрядчик должен сформулировать предложение по размещению Системы, исходя из заданных параметров производительности, доступности и информационной безопасности. Предложение по размещению в части требуемых мощностей должно быть обосновано результатами нагрузочного тестирования, изложено в Протоколе нагрузочных испытаний Системы.

При внесении изменений в СПО Системы по результатам приемочных испытаний Подрядчик должен внести соответствующие изменения и представить Заказчику исходные коды, дистрибутив СПО Системы, а также документацию, указанную в п.5.1 настоящего ТЗ.

Результаты приемочных испытаний, а также решение о готовности Системы к вводу в эксплуатацию фиксируются в «Протоколе проведения приемочных испытаний», который подписывается всеми участниками приемочной комиссии.

По результатам приемочных испытаний Заказчиком утверждается «Акт о готовности к вводу в эксплуатацию».

6.6 Требования к проведению работ по защите информации

В соответствии с п. 5.1 настоящего ТЗ состав работ по защите информации приведены в Таблице 7.

Таблица 7 – Перечень работ по защите информации.

№ п/п	Наименование работы по защите информации	Отчетная документация и материалы
1.	Определение класса защищенности, уровня защищенности персональных данных и оценки вреда	- Акт классификации информационной системы; - Акт определения уровня защищенности персональных данных системы; - Акт определения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»
2.	Актуализация модели угроз безопасности информации	- Модель угроз информационной безопасности; - Модель нарушителя безопасности информации;
3.	Актуализация частного технического задания на систему защиты	- Частное техническое задание на систему защиты информации

№ п/п	Наименование работы по защите информации	Отчетная документация и материалы
	информации	
4.	Актуализация проектно й документации на систему защиты информации	Проектная документация на систему защиты информации: - ведомость технического проекта; - пояснительная записка к техническому проекту; - схема функциональной структуры; - схема структурная комплекса технических средств; - схема организационной структуры; - ведомость покупных изделий.
5.	Актуализация эксплуатационной документации на систему защиты информации	Эксплуатационная документация на систему защиты информации в составе: - Руководство администратора на систему защиты информации; - Руководство пользователя на систему защиты информации; - Инструкция по эксплуатации комплекса средств защиты информации и иных технических средств; - Технический паспорт; - Описание технологического процесса обработки информации
6.	Предоставление прав использования СЗИ и/или СКЗИ	- Акт приема-передачи неисключительных прав на СЗИ и/или СКЗИ (в случае внедрения системы защиты информации)
7.	Установка и настройка СЗИ и/или СКЗИ	- Акт установки СЗИ и/или СКЗИ (в случае внедрения системы защиты информации)
8.	Проведение аттестационных испытаний информационной системы	- Программа и методики аттестационных испытаний (в случае изменения аттестованного объекта информатизации); - Протокол аттестационных испытаний (в случае изменения аттестованного объекта информатизации); - Заключение о соответствии Системы требованиям по защите информации (в случае изменения аттестованного объекта информатизации); - Отчет по анализу исходного кода на наличие уязвимостей и их устранению (при необходимости) - Аттестат соответствия требованиям информационной безопасности (в случае

№ п/п	Наименование работы по защите информации	Отчетная документация и материалы
		положительного заключения)

Подрядчик (или привлекаемый им субподрядчик) должен обладать следующими лицензиями, подтверждающими его квалификацию при выполнении работ:

- действующей лицензией ФСБ России, выданной уполномоченным органом государственной власти на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), включающей в себя пункты: 12, 21 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, утвержденного Постановлением Правительства РФ от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием

шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

- действующей лицензией ФСТЭК России на деятельность по технической защите конфиденциальной информации, выданной в соответствии с постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации», включающей следующие виды работ (услуг):

б) услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

г) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации: средств и систем информатизации;

д) работы и услуги по проектированию в защищенном исполнении: средств и систем информатизации;

е) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (программных (программно-технических) средств защиты информации).

6.6.1 Требования к определению класса защищенности, уровня защищенности персональных данных и оценки вреда

Определение класса защищенности Системы должно производиться в соответствии с требованиями Приказа ФСТЭК России от 18 февраля 2013 года № 117 «Об утверждении Порядка организации и обеспечения функционирования системы защиты информации государственной информационной системы, методов и способов защиты информации в государственной информационной системе»

Результаты классификации должны быть зафиксированы в документе «Акт классификации информационной системы».

Определение уровня защищенности персональных данных Системы должно производиться в соответствии с требованиями Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к

защите персональных данных при их обработке в информационных системах персональных данных».

Результаты определения уровня защищенности персональных данных должны быть зафиксированы в документе «Акт определения уровня защищенности персональных данных».

Определение оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» должно производиться в соответствии с требованиями приказа Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 октября 2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

Результаты определения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» должны быть зафиксированы в документе «Акт определения оценки вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных».

6.6.2 Требования к актуализации модели угроз

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Модель угроз безопасности информации должна быть разработана в соответствии с «Методикой оценки угроз безопасности информации», утвержденной ФСТЭК России 05 февраля 2021 г.

Модель угроз безопасности информации Системы должна включать:

1. Общие положения.
2. Описание Системы (сегментов Системы) и особенностей ее функционирования:
 - Цели и задачи, решаемые Системой (сегментом Системы).

- Класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных.
 - Номенклатура защищаемых данных, обрабатываемых в Системе (подсистеме) и функциональных задач, для решения которых они используются.
 - Назначение и структура объектов информатизации (сегментов) Системы.
 - Описание структурно-функциональных характеристик информационной системы (состав технических и программных средств Системы, сетевая инфраструктура).
 - Описание взаимосвязей с другими информационными системами (подсистемами) и телекоммуникационными сетями.
 - Описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа.
 - Описание процессов обеспечения информационной безопасности.
 - Описание технологии обработки информации.
 - Информация о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных.
3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации:
- Описание рисков (ущербов) от нарушения или прекращения основных процессов.
 - Описание негативных последствий, приводящих к возникновению рисков (ущерба).
4. Источники угроз безопасности информации (модель нарушителя):
- Характеристика нарушителей и возможные цели реализации ими угроз безопасности информации.
 - Категории актуальных нарушителей.
 - Описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей.
5. Способы реализации (возникновения) угроз безопасности информации:

- Описание способов реализации (возникновения) угроз безопасности информации.
- Описание интерфейсов объектов воздействия.

6. Актуальные угрозы безопасности информации, включая:

- Перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей.
- Описание возможных сценариев реализации угроз безопасности информации.
- Выводы об актуальности угроз безопасности информации.

7. Перечень актуальных угроз информационной безопасности.

8. Выводы о необходимом к применению (или его отсутствии) классе СКЗИ.

При идентификации возможных угроз безопасности информации должен использоваться Банк данных угроз безопасности информации, сформированный ФСТЭК России (<http://bdu.fstec.ru/>), учитывая структурно-функциональные особенности Системы, возможные источники угроз.

Модель нарушителя безопасности информации по методике ФСБ должна быть разработана в соответствии с Методическими рекомендациями по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности утвержденными руководством 8 Центра ФСБ России 31 марта 2015 года № 149/7/2/6-432.

Модель нарушителя безопасности информации по методике ФСБ должна быть оформлена отдельным документом.

Модель нарушителя безопасности информации по методике ФСБ должна включать:

- объекты, в которых размещены ресурсы информационной систем;
- физические меры защиты объектов, в которых размещены ресурсы информационной систем;
- меры по обеспечению контролируемой зоны;
- тип информационной системы;

- наличие или отсутствие информационного взаимодействия каждой подсистемы информационной системы или информационной системы в целом с другими информационными системами, а также наличие факта передачи персональных данных между ними;

- используемые в каждой подсистеме или в информационной системе в целом каналы (линии) связи, включая кабельные системы, и меры по ограничению несанкционированного доступа к защищаемой информации, передаваемой по этим каналам (линиям) связи, с указанием каналов (линий) связи, в которых невозможен несанкционированный доступ к передаваемой по ним защищаемой информации, и реализуемые для обеспечения этого качества меры;

- носители защищаемой информации, используемые в каждой подсистеме информационной системы или в информационной системе в целом (за исключением каналов (линий) связи).

Для информационной системы должна быть определена актуальность использования СКЗИ для обеспечения безопасности персональных данных.

6.6.3 Требования к актуализации частного технического задания на систему защиты информации

На основе перечня актуальных угроз безопасности информации должны быть определены требования по защите информации, подлежащие реализации в составе системы защиты информации информационной системы с учетом ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Требования к системе защиты информации Системы должны разрабатываться с учетом ГОСТ 34.602-2020 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» и, в том числе, содержать:

- цель и задачи обеспечения защиты информации;
- класс защищенности информационной системы;
- перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;
- перечень объектов защиты информационной системы;

- требования к мерам и средствам защиты информации, применяемым в информационной системе;
- этапы работ по созданию системы защиты информационной системы;
- перечень эксплуатационной и организационно-распорядительной документации;
- требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;
- функции Заказчика и оператора по обеспечению защиты информации на информационную систему;
- требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);
- требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

6.6.4 Требования к актуализации проектной документации на систему защиты информации

Проектная документация на систему защиты информации включает в себя следующие документы:

- ведомость технического проекта;
- пояснительная записка к техническому проекту;
- схема функциональной структуры;
- схема структурная комплекса технических средств;
- схема организационной структуры;
- ведомость покупных изделий.

Проектные решения по построению системы защиты информации должны быть выполнены с учетом ГОСТ Р 59795-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов» и должны отражать следующие предложения:

1. Типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (устройства, объекты файловой системы, запускаемые и исполняемые модули, объекты системы управления базами данных, объекты, создаваемые прикладным ПО, иные объекты доступа).
2. Методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам

доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в Системе.

3. Меры защиты информации, подлежащие реализации в системе защиты информации.
4. Виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации.
5. Структура системы защиты информации Системы, включая состав (количество) и места размещения ее элементов.
6. Выбор средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации, с учетом их стоимости, совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности Системы.
7. Требования к параметрам настройки ПО, включая ПО средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей Системы, приводящих к возникновению угроз безопасности информации.
8. Меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

Комплекс организационных и технических мер, направленных на нейтрализацию актуальных угроз безопасности, определенных с учетом специфики Системы и условий ее функционирования, должны предусматривать:

1. Идентификацию и аутентификацию субъектов доступа и объектов доступа.
2. Управление доступом субъектов доступа к объектам доступа.
3. Защиту машинных носителей информации.
4. Регистрацию событий безопасности.
5. Антивирусную защиту.
6. Обнаружение (предотвращение) вторжений.
7. Контроль (анализ) защищенности информации.
8. Целостность информационной системы и информации, хранимой посредством информационной системы, в части неправомерного уничтожения или модифицирования информации.
9. Доступность информации в части неправомерного блокирования информации.
10. Защиту технических средств.
11. Ограничение программной среды.
12. Защиту среды виртуализации (при использовании механизмов виртуализации).
13. Защиту информационной системы, ее средств, систем связи и передачи данных.

14. Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности ПДн (далее — Инциденты), и реагирование на них.

15. Управление конфигурацией информационной системы и защитой данных в рамках системы информационной безопасности.

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны предусматривать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

Меры по управлению доступом субъектов доступа к объектам доступа должны предусматривать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных для информационной системы правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе ПО или исключать возможность установки и (или) запуска, запрещенного к использованию в информационной системе ПО.

Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны предусматривать исключение возможности несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации путем проведения мероприятий по анализу защищенности и тестированию системы защиты информации информационной системы.

Меры по обеспечению целостности хранимой и обрабатываемой информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информации, а также возможность ее восстановления.

Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу к информации, обрабатываемой в информационной системе, в штатном режиме функционирования.

Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым ОС, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ Инцидентов в информационной системе, а также принятие мер по устранению и предупреждению Инцидентов.

Меры по управлению конфигурацией информационной должны осуществлять:

- поддержание конфигурации Системы и ее системы защиты информации (структуры системы защиты информации, состава, мест установки и параметров настройки средств защиты информации, ПО и технических средств) в соответствии с эксплуатационной документацией на систему

защиты информации (поддержание базовой конфигурации Системы и ее системы защиты информации);

- определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию Системы и ее системы защиты информации;
- внесение информации (данных) об изменениях в базовой конфигурации Системы и ее системы защиты информации в эксплуатационную документацию на систему защиты информации,

принятие решения о повторной аттестации информационной системы или проведении аттестационных испытаний по результатам управления конфигурацией.

6.6.5 Требования к актуализации эксплуатационной документации на систему защиты информации

Эксплуатационная документация на систему защиты информации информационной системы, кроме прочего, должна включать в себя:

- Руководство администратора на систему защиты информации;
- Руководство пользователя на систему защиты информации;
- Инструкцию по эксплуатации комплекса средств защиты информации и иных технических средств;
- Технический паспорт;
- Описание технологического процесса обработки информации.

Руководство администратора на систему защиты информации информационной системы должно содержать инструкции по установке, настройке, регламентным работам, а также формы журналов учета, связанных с эксплуатацией системы защиты информации информационной системы.

Руководство пользователя системы защиты информации информационной системы должно содержать инструкции, необходимые для работы со средствами защиты (в т.ч. криптографическими) при осуществлении доступа к информационной системе.

Инструкция по эксплуатации комплекса средств защиты информации и иных технических средств должна содержать всю информацию, необходимую для работы со средствами защиты (в т.ч. криптографическими) и иными техническими средствами при эксплуатации системы защиты информации информационной системы.

При разработке Технического паспорта необходимо руководствоваться требованиями и формой, представленными в приказе ФСТЭК России от 29 апреля

2021 г. № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

Описание технологического процесса обработки информации должно в полной мере описывать процесс обработки информации в информационной системе.

6.6.6 Требования к предоставлению прав использования СЗИ и/или СКЗИ

Необходимость предоставления прав использования СЗИ и/или СКЗИ определяется при разработке проектной и эксплуатационной документации.

В таком случае предоставление прав использования СЗИ и/или СКЗИ осуществляется по адресу, согласованному с Заказчиком, и должно быть оформлено актом приема-передачи неисключительных прав.

Права использования СЗИ и/или СКЗИ передаются Заказчику, в соответствии с п.4.4.8 настоящего ТЗ, с учетом лицензионной политики правообладателя СЗИ/СКЗИ.

6.6.7 Требования к установке и настройке СЗИ и/или СКЗИ

Необходимость установки и настройки СЗИ и/или СКЗИ определяется при разработке проектной и эксплуатационной документации.

Внедрение системы защиты информации информационной системы включает:

- Установку СЗИ и/или СКЗИ;
- Настройку, проверку функционирования СЗИ и/или СКЗИ.

Установка средств защиты информации и/или средств криптографической защиты информации должны быть оформлены соответствующими Актами установки СЗИ и/или СКЗИ (средств криптографической защиты информации).

Настройка, проверка функционирования СЗИ и/или СКЗИ должны быть оформлены Актами настройки, проверки функционирования средств защиты информации (средств криптографической защиты информации).

Для обеспечения защиты информации, содержащейся в информационной системе, должны применяться средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона

от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» и в соответствии с порядком, установленным ФСТЭК России и/или ФСБ России соответственно.

Требования к классу СКЗИ в информационной системе должны быть определены Подрядчиком с учетом требований приказа ФСБ России от 10 июля 2014 г. № 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».

6.6.8 Требования к проведению аттестационных испытаний информационной системы

Аттестационные испытания информационной системы должны включать проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых должно подтверждаться соответствие системы защиты информации требованиям по защите информации.

Допускается аттестация информационной системы на основе результатов аттестационных испытаний выделенного набора сегментов информационной системы, реализующих полную технологию обработки информации.

В качестве исходных данных, необходимых для проведения аттестации, должны использоваться модель угроз безопасности информации, акт классификации (определения уровня защищенности) информационной системы, техническое задание на создание/развитие информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации, проектная и эксплуатационная документация на систему защиты информации, организационно-распорядительные документы по защите информации.

Программа и методики оценки аттестационных испытаний должны содержать перечень работ, которые требуется провести для оценки и подтверждения выполнения предъявляемых требований по безопасности информации, перечень объектов аттестационных испытаний с указанием продолжительности работ и используемых при этом методов проверок и испытаний.

Программа аттестационных испытаний должна включать:

- проверку структуры, состава и условий эксплуатации системы защиты информации, обрабатываемой в информационной системе;
- проверку правильности классификации информационной системы (определения уровня защищенности);
- проверку достаточности представленных документов и соответствия их содержания установленным требованиям, наличия сертификатов соответствия требованиям безопасности информации;
- проверку уровня подготовки специалистов, обеспечивающих защиту информации, и распределения ответственности должностных лиц, эксплуатирующих информационную систему, за выполнение требований безопасности информации;
- проверку выполнения требований безопасности информации к помещению, в котором проводится обработка информации;
- проведение испытаний информационной системы на соответствие требованиям по защите информации от утечки по техническим каналам;
- проведение испытаний информационной системы на соответствие требованиям по защите от НСД;
- подготовку отчетной документации и оценку результатов испытаний аттестуемой информационной системы;
- проверку комплектности документов и соответствия их содержания установленным требованиям к системе защиты информации;
- проведение испытаний на соответствие требованиям к системе защиты информации, установленным в техническом задании и нормативных документах по защите информации;
- подготовку отчетной документации и оценку результатов аттестационных испытаний системы защиты информации;
- оформление материалов аттестационных испытаний (протоколов испытаний и заключения по результатам аттестационных испытаний);
- установление продолжительности работ по пунктам программы;
- проведение контроля соответствия системы защиты информации аттестованной информационной системы требованиям безопасности в процессе эксплуатации.

Методики аттестационных испытаний должны содержать подробное описание и порядок выполнения практических действий, осуществляемых при оценке количественных и качественных характеристик системы защиты информации, перечень требований, подлежащих проверке и условий, в которых проводится проверка, а также критерии, по которым делаются выводы о соответствии объекта проверки требованиям безопасности информации, установленных в техническом задании.

Методики испытаний должны включать:

- анализ полноты исходных данных, проверку их соответствия реальным условиям размещения, монтажа и эксплуатации технических средств информационной системы;
- исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки и передачи информации технических средств;
- проверку состояния организации работ и выполнения организационных и технических требований по защите информации, оценку правильности классификации (уровня защищенности), оценку полноты разработки организационно-распорядительной, проектной и эксплуатационной документации;
- проверку условий эксплуатации системы защиты информации;
- проверку выполнения функциональных требований к системе защиты информации;
- проверку соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации;
- проверку наличия действующих сертификатов ФСТЭК России или ФСБ России в пределах их компетенции на используемые средства защиты информации;
- проверку программной совместимости и корректности функционирования всего комплекса используемых средств вычислительной техники и с продукцией, используемой в целях защиты информации;
- проверку комплектности эксплуатационной документации на средства защиты информации;

- проверку реализации НСД доступа путем соответствующих настроек и пробного запуска средств защиты информации и наблюдения за выполнением их функций;
- проверку системы защиты информации от НСД, целостности применяемых средств защиты информации.

Программа и методики аттестационных испытаний должна быть согласована с Заказчиком до начала аттестационных испытаний.

Аттестация информационной системы должна проводиться в соответствии с программой и методиками аттестационных испытаний до начала обработки в информационной системе конфиденциальной информации. Для проведения аттестации применяются национальные стандарты, а также методические документы, разработанные и утвержденные 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 г. № 1085 (в т.ч. Приказ ФСТЭК России № 77 от 29 апреля 2021 г.).

Аттестационные испытания должны включать следующие мероприятия и работы:

- оценку соответствия технического паспорта ИС, акта классификации ИС, состава и содержания эксплуатационной документации на систему защиты информации объекта информатизации и документов по защите информации владельца объекта информатизации требованиям по защите информации;
- проверку наличия и согласования с ФСТЭК России в соответствии с пунктом 3 Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации, утвержденных Постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676, модели угроз безопасности информации, технического задания на создание (развитие, модернизацию) объекта информатизации (только для государственных информационных систем);
- обследование объекта информатизации на предмет оценки соответствия ИС и условий его эксплуатации требованиям по защите информации;

- проверку наличия документов, содержащих результаты анализа уязвимостей, проведенного на этапах предварительных или приемочных испытаний системы защиты информации объекта информатизации;
 - проверку наличия сведений о средствах защиты информации, установленных на объекте информатизации, в реестре сертифицированных средств защиты информации, ведение которого осуществляет ФСТЭК России в соответствии с «Положением о системе сертификации средств защиты информации», утвержденным приказом ФСТЭК России от 03 апреля 2018 г. № 55 (зарегистрирован Минюстом России 11 мая 2018 г., регистрационный № 51063);
 - проверку наличия работников, ответственных за обеспечение защиты информации в ходе эксплуатации ИС, в том числе за проведение оценки угроз безопасности информации, управление (администрирование) системой защиты информации (администраторов безопасности), управление конфигурацией объекта информатизации, реагирование на Инциденты, информирование и обучение персонала, контроль за обеспечением уровня защиты информации, а также проверку достаточности установленных для них обязанностей в соответствии с требованиями по защите информации;
 - оценку уровня знаний и умений работников, ответственных за обеспечение защиты информации, в соответствии с установленными для них обязанностями в эксплуатационной документации и документах по защите информации;
 - оценку соответствия принятых для ИС организационных мер требованиям по защите информации и их достаточности для защиты от актуальных для ИС угроз безопасности информации;
 - оценку соответствия принятых для ИС технических мер по защите информации от НСД (воздействия на информацию) требованиям по защите информации и их достаточности для защиты от актуальных для ИС угроз безопасности информации.
- При проведении аттестационных испытаний Подрядчиком должны применяться следующие методы, проверки и испытания:
- экспертно-документальный метод, предусматривающий проверку соответствия системы защиты информации объекта информатизации

установленным требованиям безопасности информации на основании экспертной оценки полноты и достаточности необходимых мер защиты информации в представленных документах, а также соответствия реальных условий эксплуатации требованиям к размещению, монтажу и эксплуатации технических средств;

- инструментальный метод с использованием контрольно-измерительной аппаратуры;
- проверка соответствия примененных параметров настройки элементов системы защиты информации требованиям безопасности информации;
- проверка системы защиты информации от НСД, целостности применяемых средств защиты информации от НСД;
- проверка программной совместимости и корректности функционирования всего комплекса используемых средств вычислительной техники с продукцией, используемых в целях защиты информации;
- испытания системы защиты информации от НСД путем осуществления попыток НСД к тестовой защищаемой информации.

Экспертно-документальный метод должен предусматривать проверку соответствия системы защиты информации, обрабатываемой в информационной системе, на основании экспертной оценки полноты и достаточности необходимых мер защиты информации в представленных документах, а также на основании соответствия реальных условий эксплуатации требованиям к размещению, монтажу и эксплуатации технических средств.

Измерения и оценка защищенности должны осуществляться с помощью инструментальных средств контроля эффективности защиты информации в соответствии с действующими нормативными и методическими документами по защите информации.

По результатам аттестации информационной системы должны оформляться протоколы аттестационных испытаний, заключение о соответствии Системы требованиям о защите информации (далее – Заключение).

По результатам испытаний, предусмотренных подпунктами «и» и «к» пункта 15 Порядка, органом по аттестации по результатам аттестационных испытаний оформляются протоколы аттестационных испытаний объекта информатизации (далее - протоколы), содержащие:

- наименование испытания в соответствии с программой и методикой испытаний;
- дату утверждения программы и методик аттестационных испытаний объекта информатизации;
- дату и место проведения аттестационных испытаний;
- критерии выполнения требований по защите информации, в отношении которых проводились испытания;
- условия и исходные данные для проведения испытаний;
- применяемые при проведении испытаний средства контроля эффективности защиты информации от несанкционированного доступа, а также контрольно-измерительное и испытательное оборудование;
- описание порядка испытаний по оценке критериев выполнения требований по защите информации;
- результаты испытаний по каждому оцениваемому критерию выполнения требований по защите информации.

Протоколы аттестационных испытаний подписываются экспертами органа по аттестации, проводившими аттестационные испытания объекта информатизации.

По результатам аттестационных испытаний, органом по аттестации должен оформить Заключение, которое должно включает в себя следующие сведения:

- наименование Системы и ее назначение, состав программно-технических, программных средств и средств защиты информации;
- класс защищенности Системы, категория значимости значимого объекта;
- фамилии, имена, отчества (при наличии), должности экспертов органа по аттестации, проводивших аттестацию Системы;
- дату утверждения программы и методик аттестационных испытаний Системы;
- срок проведения аттестационных испытаний;
- наименования и реквизиты документов ФСТЭК России, устанавливающих требования по защите информации, на соответствие которым проводилась аттестация объекта информатизации;

- результаты испытаний, предусмотренных пунктом 15 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным Приказом ФСТЭК России № 77 от 29 апреля 2021 г. (далее – Порядок), с описанием состава проведенных работ и испытаний в соответствии с программой и методикой испытаний, указанием сроков выполнения каждого испытания и экспертов органа по аттестации, ответственных за проведение каждого испытания, используемых экспертами при испытаниях средств, а также заключение о соответствии (несоответствии) требованиям по защите информации по каждой проведенной работе и испытанию;
- рекомендации по устранению несоответствий системы защиты информации Системы требованиям по защите информации (далее - недостатки) в случае их выявления при проведении аттестационных испытаний;
- вывод о возможности или невозможности выдачи аттестата соответствия или о необходимости доработки системы защиты информации Системы.

Заключение подписывается экспертами органа по аттестации, проводившими аттестацию Системы, и утверждается руководителем органа по аттестации.

Заключение и протоколы аттестационных испытаний в течение 5 рабочих дней после утверждения органом по аттестации направляются Заказчику.

В случае выявления в ходе аттестационных испытаний недостатков, которые можно устранить в процессе аттестации Системы, Подрядчик и/или Заказчик в соответствии компетенциями обеспечивает их устранение, а орган по аттестации оценивает качество такого устранения.

По результатам устранения недостатков орган по аттестации повторно оформляет заключение, в которое наряду со сведениями, указанными в пункте 18 Порядка, включаются сведения об устранении владельцем объекта информатизации всех выявленных недостатков, а также делается вывод о возможности выдачи аттестата соответствия требованиям по защите информации (далее - аттестат соответствия) на объект информатизации.

Аттестат соответствия должен быть выдан на весь срок эксплуатации Системы.

К моменту выдачи аттестата соответствия требованиям безопасности информации, в исходном коде информационной системе должны отсутствовать уязвимости критического, высокого и среднего уровня критичности.

Отсутствие уязвимостей подтверждается анализом исходного кода, который проводится при выполнении работ по развитию Системы. В случае внесения изменений в исходный код Системы, Подрядчиком проводится повторный анализ исходного кода с последующим предоставлением документа «Отчет по анализу исходного кода на наличие уязвимостей и их устранению».

Сведения об изменениях аттестованного объекта информатизации и проведенных при этом аттестационных испытаниях включаются в технический паспорт Системы.

7 Порядок контроля и приемки выполненных работ

7.1 Общие требования к приемке работ

Приемка результатов работ осуществляется в рамках выполнения работ в соответствии с разделом 5 настоящего ТЗ и календарным планом выполнения работ по ГК.

Приемка результатов выполнения работ на каждом этапе осуществляется путем проверки полноты предоставления документации, проведения компиляции, создания дистрибутива и установки (развертывания) программы для ЭВМ на технических средствах заказчика специалистами Заказчика и оформляется «документом о приемке работ»¹ по соответствующему этапу в ЕИС.

Результаты проведения испытаний должны быть зафиксированы в соответствующих протоколах испытаний.

Решение о принятии Системы в эксплуатацию принимается Заказчиком на основании «Акта о готовности к вводу в эксплуатацию».

Все создаваемые в рамках настоящего ТЗ программные изделия (результаты интеллектуальной деятельности) передаются Заказчику как в виде готовой Системы, так и в виде исходных кодов, представляемых в электронной форме через СУРК.

7.2 Виды, состав, объем и методы испытаний Системы и ее составных частей

В ходе выполнения работ по развитию Системы должны быть проведены следующие виды испытаний:

1. предварительные испытания;
2. опытная эксплуатация;
3. приемочные испытания (включая нагрузочные испытания).

При проведении предварительных/приемочных испытаний используются методики, определенные в согласованной с Заказчиком соответствующей «Программе и методике испытаний». «Программа и методика испытаний» должна содержать определение порядка контроля выполнения всех требований ЧТЗ и соответствующие методики контроля соответствия, при этом «Программа и

¹ Согласно ч.13 ст.94 Федерального закона от 05.04.2013 №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»

методика испытаний» в качестве приложений должна включать тесты (контрольные примеры).

Проверка соответствия требованиям к документированию производится в ходе испытаний Системы. Требования к объему документации приведены в разделе 5 настоящего ТЗ.

Соответствующие программы и методики испытаний должны быть разработаны Подрядчиком и согласованы с Заказчиком до проведения соответствующих испытаний.

Предварительные и приемочные испытания проводятся комиссией, формируемой Заказчиком на основании распорядительного документа, который должен определять состав комиссии по проведению испытаний (предварительных и приемочных), порядок ее работы. Заказчик имеет право привлекать к участию в испытаниях внешних экспертов.

Результаты проверок в ходе проведения испытаний в соответствии с «Программой и методикой испытаний» должны быть зафиксированы в соответствующих протоколах испытаний. Как недостатки реализации оформляются исключительно выявленные отклонения от настоящего ТЗ. Прочие замечания могут документироваться как рекомендованные доработки. Наличие рекомендованных доработок не влияет на процесс передачи Системы в эксплуатацию.

Условием для передачи Системы в опытную эксплуатацию является устранение всех замечаний с высоким и средним уровнем критичности. Распределение замечаний по уровням критичности приведено в таблице ниже (Таблица 8).

Таблица 8 – Распределение замечаний по уровням критичности

№ п/п	Уровень критичности	Описание
1.	Высокий	- полная недоступность СПО; - ошибки/сбои, которые приводят к полной неработоспособности всех функций СПО; - невозможность информационного обмена с СПО для информационной системы более 15 минут
2.	Средний	- ошибки/сбои, которые приводят к частичному нарушению работоспособности или недоступности функций СПО; - снижение быстродействия СПО (время отклика СПО на операции превышает 5 минут).

№ п/п	Уровень критичности	Описание
3.	Низкий	- отклонение в работе СПО, не влияющее на корректную работу функций Системы; - другие сбои и ошибки, затрагивающие основные функции СПО

В случае отклонения Системы от требований, предъявляемых на испытаниях, по решению приемочной комиссии сроки проведения испытаний могут быть перенесены/расширены Заказчиком до устранения выявленных замечаний в рамках срока выполнения работ этапа.

7.3 Порядок выполнения доработок и устранение допущенных Подрядчиком ошибок, которые выявлены в процессе испытаний и в период гарантийного обслуживания

Недостатки и ошибки в реализации Системы, выявленные в ходе проведения испытаний, должны быть устранены Подрядчиком в рамках выполнения работ. Порядок устранения замечаний и реализации рекомендаций комиссии должен быть определен в следующих документах:

1. Программа и методика предварительных испытаний;
2. Программа и методика опытной эксплуатации;
3. Программа и методика приемочных испытаний (включая программу нагрузочных испытаний).

Сроки устранения замечаний и рекомендаций, данных приемочной комиссией в ходе испытаний, определяются в документах, содержащих итоги проведения испытаний.

Недостатки и ошибки в реализации Системы, выявленные в период гарантийного обслуживания, устраняются Подрядчиком в рамках очередного обновления системы, или в рамках внеочередного экстренного обновления в случае, если обнаруженные ошибки препятствуют или ограничивают эксплуатацию Системы в штатном режиме.

Подрядчиком должны быть внесены соответствующие актуализирующие исправления в техническую и эксплуатационную документацию, связанные с устранением замечаний к работе Системы и предъявлены Заказчику на приемочные

испытания или до завершения срока гарантийного обслуживания для замечаний опытной эксплуатации или гарантийного обслуживания соответственно.

8 Сведения о гарантийном обслуживании Системы

Гарантийное обслуживание проводится в срок, определенный ГК, с момента завершения работ по ГК и подписания документа о приемке работ по последнему этапу выполнения работ по ГК.

Подрядчик должен гарантировать, что модифицированное программное обеспечение будет функционировать в соответствии со своим назначением не менее 12 месяцев с даты подписания документа о приемке работ по последнему этапу выполнения работ по ГК. При этом возможны незначительные отклонения его технических и потребительских характеристик, а также отдельные ошибки, не создающие препятствий для получения положительных результатов от эксплуатации Системы.

В течение гарантийного обслуживания Подрядчик обязуется в отношении уже выполненных работ выполнять работы по устранению выявляемых технических ошибок (дефектов), полученных от специалистов эксплуатирующей организации, в следующем объеме:

1. организация приема обращений по электронной почте о технических ошибках (дефектах) и нештатных ситуациях в работе Системы;
2. устранение обнаруженных в процессе эксплуатации дефектов в работе СПО Системы в срок не более 5 (пяти) рабочих дней (в случае необходимости данный срок может быть увеличен по согласованию с Заказчиком);
3. внесение изменений в техническую и рабочую документацию на СПО Системы на основании выявленных неточностей или обнаруженных недокументированных возможностей СПО Системы в срок не более 14 (четырнадцати) рабочих дней;
4. анализ информации о технических ошибках (дефектах) в работе Системы, выработка с ответственным сотрудником объекта автоматизации предложений по срокам и способам их преодоления, в срок не более 5 (пяти) рабочих дней;
5. консультирование представителей Заказчика в срок не более 5 (пяти) рабочих дней об особенностях реализации СПО Системы и возможности

и способах внесения предлагаемых изменений в новой версии СПО Системы.

Гарантия качества не распространяется на случаи повреждения Системы вследствие действий третьих лиц.

9 Требования к документированию

Документация на Систему и ее части (техническая и рабочая) должна содержать исчерпывающее описание принятых проектных решений в объеме, достаточном для ее дальнейшего развития и эксплуатации.

Разработанная документация на Систему должна удовлетворять требованиям комплекса стандартов на автоматизированные системы:

1. ГОСТ Р 59853-2021 – в части терминологии;
2. ГОСТ 34.201-2020 – в части наименования и обозначения документов;
3. ГОСТ Р 59793-2021 – в части определения стадий и этапов работ;
4. ГОСТ 34.602-2020 – в части состава, содержания и правил оформления «Частного технического задания»;
5. ГОСТ Р 59795-2021 – в части требований к содержанию документов;
6. ГОСТ Р 59792-2021 – в части определения видов испытаний.
7. ГОСТ Р 57100-2025 Системная и программная инженерия. Описание архитектуры

Документы на Систему должны оформляться в соответствии с требованиями ГОСТ Р 2.105-2019 на листах формата А4 по ГОСТ 2.301-68 без рамки, основной надписи и дополнительных граф к ней. Допускается для размещения рисунков и таблиц использование листов формата А3 с подшивкой по короткой стороне листа. Документы объемом более 25 листов должны содержать аннотацию и содержание.

Документы должны быть разработаны с учетом следующих требований:

- язык отчетных материалов – русский;
- отчетная документация передается Заказчику на бумажном носителе в 2 (двух) экземплярах и в электронном виде в 1 (одном) экземпляре (за исключением документа о приемке, формируемом в ЕИС);
- вспомогательная документация (не указанная в качестве непосредственного результата работ) передается только в электронном виде;
- отчетная документация в электронном виде должна быть представлена через СУРК;
- форматы представления информации в электронном виде:

- текстовые документы – форматы, позволяющие осуществить их просмотр средствами OpenOffice;
- схемы, рисунки и другие графические материалы – VSD (либо PDF);
- все материалы передаются с сопроводительными документами Подрядчика.

Если в состав документации включаются материалы, требующие больших форматов (схемы, чертежи, фотоматериалы и пр.), то по согласованию с Заказчиком допускается выполнение приложений к таким документам только на машинных носителях в форматах PDF, TIFF, JPEG и др. При этом основная часть документа выпускается в соответствии с требованиями, определенными выше.

Состав отчетной документации на Систему по каждому этапу выполнения работ определен в п. 5.1 настоящего ТЗ.

Подрядчик должен в обязательном порядке присваивать документам на Систему уникальные номера в соответствии с порядком, установленным в Приложении А к настоящему документу.

Приложение А

Правила присвоения номеров отчетной документации

Нумерация документам должна присваиваться в следующем формате:

КодСистемы.НомерГосКонтракта.Этап.КодДокумента.Версия

Пример:

АИСОГ.291-ОКЭФ/2020.2.П2.1

где,

АИСОГ – код системы

291-ОКЭФ/20 – номер госконтракта

2 – этап

П2 – код документа «Пояснительная записка к техническому проекту»

1 – версия (версия для документов является сквозной, т.е. при изменении номера контракта номер версии будет увеличиваться по нарастающей).

Таблица Б.1 – Перечень и коды документов¹⁾

Тип документа	Код документа
Ведомость эскизного проекта	ЭП*
Ведомость передаваемых файлов	ВФ
Пояснительная записка к эскизному проекту	П1
Схема организационной структуры	СО
Структурная схема комплекса технических средств	С1*
Схема функциональной структуры	С2*
Перечень заданий на разработку специализированных (новых) технических средств	В9
Схема автоматизации	С3*
Технические задания на разработку специализированных (новых) технических средств	-
Ведомость технического проекта	ТП*
Ведомость покупных изделий	ВП*
Перечень входных данных	В1
Перечень выходных данных	В2
Перечень заданий на разработку строительных, электротехнических, санитарно-технических и других разделов проекта, связанных с созданием системы	В3
Пояснительная записка к техническому проекту	П2
Описание автоматизируемых функций	П3
Описание архитектуры	ОА
Описание постановки задач (комплекса задач)	П4
Описание информационного обеспечения системы	П5
Описание организации информационной базы	П6
Описание систем классификации и кодирования	П7
Описание массива информации	П8

¹ Включая, но не ограничиваясь ГОСТ

Тип документа	Код документа
Описание комплекса технических средств	П9
Описание программного обеспечения	ПА
Описание алгоритма (проектной процедуры)	ПБ
Описание организационной структуры	ПВ
План расположения	С8
Ведомость оборудования и материалов	-
Локальный сметный расчет	Б2
Проектная оценка надежности системы	Б1
Шаблон документа	С9
Чертеж формы документа (видеокадра)	С9
Ведомость держателей подлинников	ДП*
Ведомость эксплуатационных документов	ЭД*
Спецификация оборудования	В4
Ведомость потребности в материалах	В5
Описание информационного массива	В6
Описание базы данных	В7
Локальная смета	Б3
Методика (технология) автоматизированного проектирования	И1
Технологическая инструкция	И2
Регламент информационного взаимодействия	
Регламент эксплуатации системы	
Регламент гарантийного обслуживания	
Руководство пользователя	И3
Руководство администратора	И5
Инструкция по развертыванию системы	
Инструкция по эксплуатации комплекса технических средств	ИЭ
Схема соединения внешних проводов	С4*
Схема подключения внешних проводов	С5*
Таблица соединений и подключений	С6
Схема деления системы (структурная)	Е1*
Чертеж общего вида	ВО*
Чертеж установки технических средств	СА
Схема принципиальная	СБ
Схема структурная комплекса технических средств	С1*
План восстановления в случае аварии	
План-программа подготовки персонала	
План расположения оборудования и проводов	С7
Описание технологического процесса обработки данных (включая телеобработку)	ПГ
Общее описание системы	ПД
Отчет о проведении опытной эксплуатации (с приложением журнала опытной эксплуатации)	
Программа и методика испытаний	ПМ*
Программа и методика опытной эксплуатации	
Формуляр	ФО*
Паспорт	ПС*
* Документы, код которых установлен в соответствии с требованиями стандартов Единой системы конструкторской документации (ЕСКД)	

Приложение Б

Форма документа «Ведомость передаваемых файлов»

№ п/п	№ CD ¹	Обозначение	Наименование	Имя файла	Объем, байт
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
38		б/н	Исходные коды и дистрибутив СПО Системы	Distrib.zip	

¹ Если документы сдаются через СУРК, то столбец не нужен.