

УТВЕРЖДАЮ:
Заместитель директора
СПб ГКУ «УИТС»

_____/О.В.Раева/
«__» _____ 2026 г.

ОПИСАНИЕ ОБЪЕКТА ЗАКУПКИ
Термины и определения

В настоящем документе применены следующие термины с соответствующими определениями:

Термин	Определение
1	2
Заказчик	Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи»
Задача	Элемент функциональной структуры Системы, представляющий собой процесс обработки информации с четко определенным множеством входной и выходной информации и имеющий самостоятельный технологический результат
Комплекс задач	Элемент функциональной структуры Системы, представляющий собой совокупность функционально взаимосвязанных задач
Мажорные изменения	Значительные изменения или добавление функционала в программном обеспечении Системы, в том числе приводящие к нарушению совместимости. Формат (тип) изменения определяется разработчиком
Минорные изменения	Незначительные изменения или добавление функционала в программном обеспечении Системы без нарушения совместимости. Формат (тип) изменения определяется разработчиком
Обладатель информации	Администрация Губернатора Санкт-Петербурга
Объект автоматизации	Организация (или организации), деятельность которых автоматизируется
Объект информатизации	Совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров
Оператор	Администрация Губернатора Санкт-Петербурга
Получатель	Администрация Губернатора Санкт-Петербурга
Промышленный контур	Программно-аппаратная среда, используемая в целях эксплуатации Системы
Предпродуктивный контур	Программно-аппаратная среда, используемая в целях организации установки, наладки, предварительных и приемочных испытаний,

Термин	Определение
1	2
	опытной эксплуатации Системы. Располагается на мощностях, предоставление которых организуется Заказчиком. Предпродуктивный контур является частью Промышленного контура Системы. Предпродуктивный контур по архитектуре и конфигурации должен соответствовать продуктивному контуру Системы, включая интеграции со внешними информационными системами (состоянию продуктивного контура Системы по результатам развития Системы в рамках настоящего контракта)
Продуктивный контур	Программно-аппаратная среда, используемая в целях промышленной эксплуатации Системы. Продуктивный контур является частью Промышленного контура Системы
Репозиторий	Репозиторий хранения исходных кодов государственных информационных систем Санкт-Петербурга
Система	Государственная информационная система Санкт-Петербурга «Единая система строительного комплекса Санкт-Петербурга»
Строгая аутентификация	Аутентификация с применением только метода многофакторной взаимной аутентификации и использованием криптографических протоколов аутентификации.
Ansible	Инструмент управления конфигурациями кода
CodeScoring	Инструмент для анализа кода на уязвимости
CI/CD	Совокупность практик и программных средств автоматизации процессов разработки программного обеспечения, обеспечивающих непрерывную интеграцию изменений кода, автоматизированное тестирование, сканирование на наличие уязвимостей, сборку и развертывание программного продукта в целевые среды эксплуатации с минимальным участием человека
Git	Распределённая система управления версиями Санкт-Петербургского государственного казенного учреждения «Служба сопровождения программных комплексов». Система обеспечивает хранение полной истории изменений (включая версии), ветвление, слияние кода и целостность данных
MP3	Формат файла для хранения аудиоинформации
MPEG-2	Группа стандартов цифрового кодирования видео-и аудиосигналов

Сокращения и обозначения

В настоящем документе применены следующие сокращения (обозначения):

Сокращение (обозначение)	Значение сокращения (обозначения)
1	2
АРМ	Автоматизированное рабочее место
БД	База данных
ВИС	Ведомственная информационная система
ВМ	Виртуальная машина
ГОСТ	Государственный стандарт
ЕГРЗ	Единый государственный реестр заключений
ЕГРИП	Единый государственный реестр индивидуальных предпринимателей
ЕГРН	Единый государственный реестр недвижимости
ЕГРЮЛ	Единый государственный реестр юридических лиц
ЕИСЖС	Единая информационная система жилищного строительства
ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
ЕСОВ ТОРИС	Подсистема «Единая система однократного входа» автоматизированной системы «Технологическое ядро» государственной информационной системы Санкт-Петербурга «Территориальная отраслевая региональная информационная система»
ЕССК	Государственная информационная система Санкт-Петербурга «Единая система строительного комплекса Санкт-Петербурга»
ЗО КИИ	Значимый объект критической информационной инфраструктуры
ИЖС	Индивидуальное жилищное строительство
ИНН	Идентификационный номер налогоплательщика
ИОГВ	Исполнительный орган государственной власти Санкт-Петербурга
ИСПДн	Информационная система персональных данных
МАИС ЭГУ	Межведомственная автоматизированная информационная система предоставления в Санкт-Петербурге государственных и муниципальных услуг в электронном виде
МЧД	Машиночитаемая доверенность
НСД	Несанкционированный доступ
ОГРН	Основной государственный регистрационный номер
ОГРНИП	Основной государственный регистрационный номер индивидуального предпринимателя
ОЖР	Общий журнал работ
ОКПД2	Общероссийский классификатор продукции по видам экономической деятельности
ОКС	Объект капитального строительства
ОПО	Общее программное обеспечение
ОС	Операционная система
ПО	Программное обеспечение

Сокращение (обозначение)	Значение сокращения (обозначения)
1	2
РБПО	Разработка безопасного программного обеспечения
Реестр	Единый реестр российских программ для электронных вычислительных машин и баз данных или Единый реестр программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза за исключением Российской Федерации
Реестр ГИС	Государственная информационная система Санкт-Петербурга «Реестр государственных информационных систем Санкт-Петербурга»
Репозиторий	Репозиторий хранения исходных кодов государственных информационных систем Санкт-Петербурга
РНВ	Разрешение на ввод в эксплуатацию
РНС	Разрешение на строительство
Роспатент	Федеральная служба по интеллектуальной собственности
РПГУ	Региональный портал государственных услуг
РРЦОД	Распределенный региональный центр обработки данных исполнительных органов государственной власти Санкт-Петербурга
РСМЭВ	Региональная система межведомственного электронного взаимодействия
СГСН	Служба государственного строительного надзора и экспертизы Санкт-Петербурга
СЗИ	Подсистема Система защиты информации
СМЭВ	Единая система межведомственного электронного взаимодействия
СКЗИ	Средство криптографической защиты информации, шифровальное (криптографическое) средство
СПО	Специальное программное обеспечение
СрЗИ	Средство защиты информации
СУБД	Система управления базами данных
СФУП	Государственная информационная система Санкт-Петербурга «Система формирования и учета проектов»
ТИМ	Технологии информационного моделирования
УКЭП	Усиленная квалифицированная электронная подпись
ФГИС ЕГРН	Федеральная государственная информационная система Единый государственные реестр недвижимости
ФИО	Фамилия, имя, отчество
ФОИВ	Федеральные органы исполнительной власти
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ЦИМ ОКС	Цифровая информационная модель объекта капитального строительства
ЦОУ ИБ АПК БГ	Автоматизированная система «Центр оперативного управления информационной безопасностью» государственной информационной системы Санкт-Петербурга «Аппаратно-программный комплекс «Безопасный город»
ЭВМ	Электронно-вычислительная машина
ЭДО	Электронный документооборот
API	Application Programming Interface Программный интерфейс

Сокращение (обозначение)	Значение сокращения (обозначения)
1	2
	приложения
AVI	Audio Video Interleave – (англ.) Формат файлов содержащий видео- и аудиоданные, позволяющий синхронно воспроизводить видео со звуком
BIM	Building Information Model или Modeling (англ.) – информационная модель здания
BPMN	Business Process Model and Notation (англ.) – система условных обозначений (нотация) и их описания
CD/DVD	Compact Disc/ Digital Versatile Disc – (англ.) Оптический носитель информации в виде цифрового многоцелевого диска, предназначенного для хранения и считывания информации
DOCX (DOC)	Microsoft Office Document (англ.) Текстовый формат файлов для хранения электронных документов пакетов офисных приложений
DVD M-DISC	DVD M-DISC Digital Versatile Millennial Disc – (англ.) Оптический носитель информации в виде цифрового многоцелевого диска, предназначенного для длительного хранения и считывания информации
IFC	Industry Foundation Classes (англ.) – открытый стандарт для формата представления данных BIM
JPEG (JPG)	Joint Photographic Experts Group – (англ.) Растровый графический формат, применяемый для хранения фотоизображений и подобных им изображений
PDF	Portable Document Format – (англ.) Межплатформенный формат электронных документов
PDF/A	Portable Document Format / A – (англ.) Стандарт для долгосрочного архивного хранения электронных документов, базирующийся на описании стандарта PDF
RAM	Random Access Memory – (англ.) Оперативная память
RSID	Идентификатор электронного сервиса в РСМЭВ
SSL	Secure Sockets Layer Протокол безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером
UML	Unified Modeling Language (англ.) – система условных обозначений (нотация) и их описания
URL	Uniform Resource Locator (англ.) – адрес ресурса в сети Интернет
UUID (GUID)	Universally unique identifier (Globally Unique Identifier) (англ.) – уникальный электронный идентификатор
vCPU	Virtual Central Processing Unit – (англ.) Виртуальное центральное процессорное устройство
XLSX (XLS)	Microsoft Office Excel – (англ.) Формат файла, предназначенный для хранения электронных таблиц
XLST	eXtensible Stylesheet Language Transformations (англ.) – язык преобразования XML-документов

1. Перечень выполняемых работ

1.1. Перечень выполняемых работ приведен в Приложении № 1 к Описанию объекта закупки.

2. Требования к техническим, функциональным и эксплуатационным, качественным характеристикам объекта закупки

2.1. Технические, функциональные и эксплуатационные характеристики объекта закупки указаны в Приложении № 2 и Приложении № 3 к Описанию объекта закупки.

2.2. Общие сведения о Системе доступны в Реестре ГИС по ссылке <https://reestr-gis.gov.spb.ru/gis>. Выполнение работ по развитию Системы в 2026-2027 годах осуществляется на основе технических и программных решений, реализованных ранее в рамках работ по созданию и развитию Системы в 2016-2025 годах.

2.3. Уполномоченным лицом, предоставляющим вычислительные ресурсы Получателю для обработки информации, содержащейся в Системе, является Санкт-Петербургское государственное казенное учреждение «Санкт-Петербургский информационно-аналитический центр» – оператор Распределенного регионального центра обработки данных исполнительных органов государственной власти Санкт-Петербурга.

2.4. Организацией, осуществляющей сопровождение Системы, является Санкт-Петербургское государственное казенное учреждение «Служба сопровождения программных комплексов».

2.5. Свидетельство от 28.04.2026 № 2693/26/1/0 о регистрации государственной информационной системы Санкт-Петербурга «Единая система строительного комплекса Санкт-Петербурга» в государственной информационной системе Санкт-Петербурга «Реестр государственных информационных систем Санкт-Петербурга».

2.6. Аттестат соответствия требованиям безопасности информации государственной информационной системы Санкт-Петербурга «Единая система строительного комплекса Санкт-Петербурга» от 13.12.2018 № 32/12/18.

2.7. Распоряжение Администрации Губернатора Санкт-Петербурга от 07.02.2022 № 3-ра (ред. от 07.02.2022) «О вводе государственной информационной системы Санкт-Петербурга «Единая система строительного комплекса Санкт-Петербурга» в эксплуатацию».

3. Требования к качеству и безопасности работ

3.1. Выполняемые работы должны отвечать требованиям, указанным в Приложении № 2 к Описанию объекта закупки.

3.2. Документы и/или информация, необходимые Подрядчику для выполнения работ по Контракту, предоставляются Заказчиком на основании письменного запроса Подрядчика. Запрос о предоставлении документов и/или информации должен содержать обоснование необходимости предоставления таких документов и/или информации с указанием обязательств Подрядчика, исполнение которых невозможно без предоставления таких документов и/или информации. В случае необходимости получения документов и/или информации от Получателя, Подрядчик обязан направить в адрес Получателя запрос о предоставлении документов и/или информации, содержащий обоснование необходимости предоставления таких документов и/или информации с указанием обязательств Подрядчика, исполнение которых невозможно без предоставления таких документов и/или информации, с учетом положений пункта 4.1.35 Контракта.

Условия использования исходного кода Системы (в случае если такой исходный код передается Подрядчику для выполнения работ) установлены в пункте 12.2 Контракта.

3.3. Работы выполняются Подрядчиком в соответствии с международными стандартами, национальными стандартами и государственными стандартами в части требований к проектированию, стадиям создания, видам, комплектности и обозначению документов, видам испытаний при создании и (или) развитии (модернизации) государственных информационных систем и (или) иных информационных систем.

При проектировании способов и средств обработки данных, содержащихся в Системе, должно быть предусмотрено использование классификаторов в соответствии с Положением о системе классификаторов исполнительных органов государственной власти Санкт-Петербурга, утвержденным постановлением Правительства Санкт-Петербурга от 30.09.2005 № 1491. При использовании локальных классификаторов (классификаторов

ИОГВ) Подрядчик обязан обосновать невозможность использования общегородских классификаторов Санкт-Петербурга и/или общероссийских классификаторов.

Заказчик после заключения Контракта на основании запроса Подрядчика передает перечень имеющегося у Заказчика общего программного обеспечения. При выполнении работ Подрядчик обязан использовать программное обеспечение, включенное в указанный перечень, использование иного, не включенного в перечень общего программного обеспечения допускается только по согласованию с Заказчиком.

Результаты выполняемых работ и технические решения, разработанные и реализованные Подрядчиком при выполнении работ по созданию/развитию Системы, должны соответствовать требованиям к защите информации, приведенным в Приложении № 4 к Описанию объекта закупки.

3.4. При выполнении работ должны быть соблюдены требования нормативных правовых актов, международных стандартов, национальных стандартов, государственных стандартов, технических регламентов, документов по стандартизации и иных руководящих документов в сфере информации, информационных технологий и защиты информации, связи, приведенных в Таблице 1.

Таблица 1

Обозначение	Наименование
1	2
Федеральный закон от 27.12.2002 № 184-ФЗ	О техническом регулировании
Федеральный закон от 27.07.2006 № 149-ФЗ	Об информации, информационных технологиях и о защите информации
Федеральный закон от 27.07.2006 № 152-ФЗ	О персональных данных
Федеральный закон от 06.04.2011 № 63-ФЗ	Об электронной подписи
Федеральный закон от 29.06.2015 № 162-ФЗ	О стандартизации в Российской Федерации
Постановление Правительства Российской Федерации от 28.11.2011 № 977	О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
Постановление Правительства Российской Федерации от 09.02.2012 № 111	Об электронной подписи, используемой органами исполнительной власти и органами местного самоуправления при организации электронного взаимодействия между собой, о порядке ее использования, а также об установлении требований к обеспечению совместимости средств электронной подписи
Постановление Правительства Российской Федерации от 01.11.2012 № 1119	Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных
Постановление Правительства Российской Федерации от 10.07.2013 № 583	Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных (вместе с «Правилами отнесения информации к общедоступной информации, размещаемой государственными органами и органами местного самоуправления в информационно-телекоммуникационной сети «Интернет» в форме открытых данных», «Правилами

1	2
	определения периодичности размещения в информационно-телекоммуникационной сети «Интернет» в форме открытых данных общедоступной информации о деятельности государственных органов и органов местного самоуправления, сроков ее обновления, обеспечивающих своевременность реализации и защиты пользователями своих прав и законных интересов, а также иных требований к размещению указанной информации в форме открытых данных», «Правилами обязательного размещения органами государственной власти субъектов Российской Федерации и органами местного самоуправления общедоступной информации о деятельности органов государственной власти субъектов Российской Федерации и органов местного самоуправления, созданной указанными органами или поступившей к ним при осуществлении полномочий по предметам ведения Российской Федерации и полномочий Российской Федерации по предметам совместного ведения Российской Федерации и субъектов Российской Федерации, переданных для осуществления органам государственной власти субъектов Российской Федерации или органам местного самоуправления, в информационно-телекоммуникационной сети «Интернет» в форме открытых данных»)
Постановление Правительства Российской Федерации от 06.07.2015 № 676	О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации
Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152	Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну
Приказ Федеральной службы безопасности Российской Федерации от 09.02.2005 № 66	Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)
Приказ Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21	Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
Приказ Федеральной службы безопасности Российской Федерации от 10.07.2014 № 378	Об утверждении Состав 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

1	2
Приказ Министерства связи и массовых коммуникаций Российской Федерации от 19.08.2015 № 305	Об утверждении Методических рекомендаций по использованию свободного программного обеспечения в деятельности федеральных органов исполнительной власти, включая критерии определения государственных информационных систем, при создании которых необходимо использовать свободное программное обеспечение, в том числе государственных информационных систем, предназначенных для оказания государственных и муниципальных услуг в электронном виде
Приказ Министерства экономического развития Российской Федерации от 05.04.2016 № 211	Об утверждении Правил оформления заявки на государственную регистрацию программы для электронных вычислительных машин или базы данных, Правил составления документов, являющихся основанием для осуществления юридически значимых действий по государственной регистрации программы для электронных вычислительных машин или базы данных, и их форм, Порядка государственной регистрации программы для электронных вычислительных машин и базы данных, Перечня сведений о зарегистрированной программе для электронных вычислительных машин или базе данных, публикуемых в официальном бюллетене Федеральной службы по интеллектуальной собственности, Перечня сведений, указываемых в свидетельстве о государственной регистрации программы для электронных вычислительных машин или базы данных, формы свидетельства о государственной регистрации программы для электронных вычислительных машин, формы свидетельства о государственной регистрации базы данных
Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 22.09.2020 № 486	Об утверждении классификатора программ для электронных вычислительных машин и баз данных
Приказ Федеральной службы по техническому и экспортному контролю от 29.04.2021 № 77	Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну
Приказ Федерального архивного агентства от 28.12.2021 № 142	Об утверждении Перечня типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения
Приказ Федеральной службы по техническому и экспортному контролю от 04.07.2022 г. № 118	Требования по безопасности информации к средствам контейнеризации
Приказ Федеральной службы по техническому и экспортному контролю	Требования по безопасности информации к средствам виртуализации

1	2
от 27.10.2022 г. № 187	
Приказ Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 02.11.2022 № 929/ПР	Об утверждении требований к формату документов, используемых при осуществлении регионального государственного строительного надзора и составляемых в электронной форме
Приказ Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 02.12.2022 № 1026/ПР	Об утверждении формы и порядка ведения общего журнала, в котором ведется учет выполнения работ по строительству, реконструкции, капитальному ремонту объекта капитального строительства
Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.01.2023 № 21	Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации
Приказ Федеральной службы по техническому и экспортному контролю от 14.04.2023 г. № 64	Требования по безопасности информации к системам управления базами данных
Приказ Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 16.05.2023 № 344/ПР	Об утверждении состава и порядка ведения исполнительной документации при строительстве, реконструкции, капитальном ремонте объектов капитального строительства
Приказ Федеральной службы по техническому и экспортному контролю от 11.04.2025 № 117	Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений
Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 19.06.2025 № 140	Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных, за исключением случаев, указанных в пункте 9.1 части 1 статьи 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»
Приказ Министерства строительства и жилищно-	Об установлении составов сведений, содержащихся в реестре уведомлений о планируемом строительстве объектов индивидуального жилищного строительства и в реестре

1	2
коммунального хозяйства Российской Федерации от 21.04.2026 № 257/пр	уведомлений об окончании строительства объектов индивидуального жилищного строительства
Приказ Министерства строительства и жилищно-коммунального хозяйства Российской Федерации от 17.07.2026 № 457/пр	Об установлении типовой формы выписки из реестра разрешений на строительство объектов капитального строительства и типовой формы выписки из реестра разрешений на ввод объектов капитального строительства в эксплуатацию
Приказ Федеральной службы безопасности Российской Федерации от 22.08.2026 № 321	Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5.1 статьи 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» с использованием шифровальных (криптографических) средств»
Закон Санкт-Петербурга от 01.07.2009 № 371-70	О государственных информационных системах Санкт-Петербурга
Постановление Правительства Санкт-Петербурга от 18.11.2003 № 43	Постановление Правительства Санкт-Петербурга от 18.11.2003 № 43 «Об Администрации Губернатора Санкт-Петербурга»
Постановление Правительства Санкт-Петербурга от 30.09.2005 № 1491	Об утверждении Положения о системе классификаторов исполнительных органов государственной власти Санкт-Петербурга
Постановление Правительства Санкт-Петербурга от 27.04.2010 № 450	Постановление Правительства Санкт-Петербурга от 27.04.2010 № 450 «О Комитете по информатизации и связи»
Постановление Правительства Санкт-Петербурга от 16.08.2010 № 1101	О мерах по реализации Закона Санкт-Петербурга «О государственных информационных системах Санкт-Петербурга»
Постановление Правительства Санкт-Петербурга от 01.07.2011 № 884	Об организации деятельности исполнительных органов государственной власти Санкт-Петербурга по развитию, подключению и эксплуатации Единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга и создании государственной информационной системы Санкт-Петербурга «Учет ресурсов Единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга»

1	2
Постановление Правительства Санкт-Петербурга от 22.08.2016 № 706	Постановление Правительства Санкт-Петербурга от 22.08.2016 № 706 «О создании государственной информационной системы Санкт-Петербурга «Единая система строительного комплекса Санкт-Петербурга»
Постановление Правительства Санкт-Петербурга от 24.10.2016 № 928	О мерах по реализации постановления Правительства Российской Федерации от 06.07.2015 № 676
Распоряжение Администрации Санкт-Петербурга от 19.02.2002 № 227-ра	О создании единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга
Распоряжение Комитета по информатизации и связи от 12.07.2010 № 31-р	Об утверждении Административного регламента Комитета по информатизации и связи по исполнению государственной функции по обеспечению ведения Реестра государственных информационных систем Санкт-Петербурга
Распоряжение Комитета по информатизации и связи от 29.11.2010 № 48-р	О мерах по реализации постановления Правительства Санкт-Петербурга от 16.08.2010 № 1101 «О мерах по реализации Закона Санкт-Петербурга «О государственных информационных системах Санкт-Петербурга»
ГОСТ Р 2.102-2023	Национальный стандарт Российской Федерации. Единая система конструкторской документации. Виды и комплектность конструкторских документов
ГОСТ Р 2.104-2023	Национальный стандарт Российской Федерации. Единая система конструкторской документации. Основные надписи.
ГОСТ Р 2.105-2019	Национальный стандарт Российской Федерации. Единая система конструкторской документации. Общие требования к текстовым документам
ГОСТ Р 2.106-2019	Национальный стандарт Российской Федерации. Единая система конструкторской документации. Текстовые документы
ГОСТ Р 2.109-2023	Национальный стандарт Российской Федерации. Единая система конструкторской документации. Основные требования к чертежам
ГОСТ Р 2.601-2019	Национальный стандарт Российской Федерации. Единая система конструкторской документации. Эксплуатационные документы
ГОСТ Р 7.0.97-2025	Национальный стандарт Российской Федерации. Система стандартов по информации, библиотечному и издательскому делу.
ГОСТ 7.32-2017	Межгосударственный стандарт. Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления
ГОСТ 19.101-2024	Межгосударственный стандарт. Единая система программной документации. Виды программ и программных документов
ГОСТ 19.202-78 (СТ СЭВ 2090-80)	Межгосударственный стандарт. Единая система программной документации. Спецификация. Требования к содержанию и оформлению
ГОСТ 19.402-78 (СТ СЭВ 2092-80)	Межгосударственный стандарт. Единая система программной документации. Описание программы

1	2
ГОСТ 19.503-79 (СТ СЭВ 2094-80)	Межгосударственный стандарт. Единая система программной документации. Руководство системного программиста. Требования к содержанию и оформлению
ГОСТ 19.507-79 (СТ СЭВ 2091-80)	Межгосударственный стандарт. Единая система программной документации. Ведомость эксплуатационных документов
ГОСТ 21.110-2013	Межгосударственный стандарт. Система проектной документации для строительства. Спецификация оборудования, изделий и материалов
ГОСТ 34.201-2020	Межгосударственный стандарт. Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем
ГОСТ 34.602-2020	Межгосударственный стандарт. Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы
ГОСТ Р 34.10-2012	Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
ГОСТ Р 34.11-2012	Национальный стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования
ГОСТ Р ИСО/МЭК 13335-1-2006	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
ГОСТ Р ИСО/МЭК ТО 18044-2007	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности
ГОСТ Р ИСО/МЭК 27002-2021	Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности
ГОСТ Р ИСО/МЭК 27005-2010	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности
ГОСТ Р ИСО/МЭК 27033-1-2011	Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции
ГОСТ 28270-89 (ИСО 8211-85)	Межгосударственный стандарт. Системы обработки информации. Спецификация файла описания данных для обмена информацией
ГОСТ Р 50922-2006	Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения
ГОСТ Р 51275-2006	Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения
ГОСТ Р 51583-2014	Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем

1	2
	в защищенном исполнении. Общие положения
ГОСТ Р 51624-2000	Национальный стандарт Российской Федерации. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования
ГОСТ Р 53114-2008	Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения
ГОСТ Р 54869-2011	Национальный стандарт Российской Федерации. Проектный менеджмент. Требования к управлению проектом
ГОСТ Р 56545-2015	Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей
ГОСТ Р 56546-2015	Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем
ГОСТ Р 56938-2016	Национальный стандарт Российской Федерации. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения
ГОСТ Р 56939-2024	Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования
ГОСТ Р 58833-2020	Национальный стандарт Российской Федерации. Защита информации. Идентификация и аутентификация. Общие положения
ГОСТ Р 59547-2021	Национальный стандарт Российской Федерации. Защита информации. Мониторинг информационной безопасности. Общие положения
ГОСТ Р 59792-2021	Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем
ГОСТ Р 59793-2021	Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания
ГОСТ Р 59795-2021	Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов
ГОСТ Р 59853-2021	Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения
Р 50-34.126-92	Рекомендации. Информационная технология. Правила проведения работ при создании автоматизированных систем
	Методический документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утвержден ФСТЭК России 15.02.2008
	Методический документ. Методика оценки угроз безопасности

1	2
	информации. Утвержден ФСТЭК России 05.02.2021
	Методический документ. Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах. Утвержден ФСТЭК России 12.04.2026
	Методические рекомендации по использованию Единой системы идентификации и аутентификации https://digital.gov.ru/documents/metodicheskie-rekomendaczii-po-ispolzovaniyu-esia

3.5. Должна быть обеспечена безопасность работ для здоровья сотрудников Заказчика и Получателя, имущества потребителя и окружающей среды при обычных условиях использования, хранения, транспортировки и утилизации результатов работ, а также безопасность процесса выполнения работ.

3.6. При выполнении работ по Контракту должна быть обеспечена возможность сохранения и представления пользователям в программах для ЭВМ и базах данных Системы, в том числе созданных (модернизированных) в целях исполнения настоящего контракта, ранее накопленных в Системе данных.

3.7. В ходе выполнения работ должны быть соблюдены требования к защите информации и безопасной разработке программного обеспечения, содержащиеся в национальном стандарте Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования». Подрядчику запрещено передавать третьим лицам информацию, используемую для выполнения работ, сведения о характере выполняемых работ и информацию об информационно-телекоммуникационных системах, каналах связи, компьютерных сетях, средствах вычислительной техники, программных средствах (операционных системах, системах управления базами данных и другого общесистемного и программного обеспечения), системах связи, передачи данных, используемых для сбора, хранения, обработки и передачи информации ограниченного доступа, системах и средствах охранно-тревожной, пожарной сигнализации и видеонаблюдения на объектах исполнительных органов государственной власти Санкт-Петербурга, и также сведения о системах защиты информации (средства, методы и способы защиты информации, а также коды и процедуры доступа к информационным ресурсам исполнительных органов государственной власти Санкт-Петербурга).

3.8. Разрабатываемые (модернизируемые) программные средства Системы не должны допускать и содержать недекларированных возможностей и известных уязвимостей информационной безопасности. Заказчик вправе проверять наличие уязвимостей, использовать средства проверки уязвимостей по своему выбору, в том числе привлекать для проверки наличия уязвимостей третьих лиц.

3.9. Подрядчик обязан согласовать с Заказчиком необходимость использования при выполнении работ охраняемых результатов интеллектуальной деятельности, права на которые принадлежат третьим лицам, объем и порядок приобретения прав на их использование.

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

3.11. Подрядчик обязан обеспечить отсутствие нарушений исключительных, авторских и смежных прав третьих лиц при реализации технических, программных, организационных и иных решений, предусмотренных Описанием объекта закупки.

3.12. Подрядчик обязан обеспечить выполнение требований к порядку создания (развития) государственных и (или) иных информационных систем, предусмотренных пунктом 1 части 1 статьи 13 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», устанавливаемых к таким информационным системам указанным Федеральным законом и иными нормативными правовыми актами Российской Федерации.

3.13. Исключительные права на результаты интеллектуальной деятельности, в том числе, но не исключая: изобретения, полезные модели, промышленные образцы, программы для электронных вычислительных машин, базы данных, топологии интегральных микросхем, а также исключительные права на результаты работ, включая объекты авторских прав и потенциально патентоспособные технические решения, секреты производства (ноу-хау), созданные в рамках контракта, принадлежат городу федерального значения Санкт-Петербургу, от имени которого выступает Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи».

Право на получение патента и исключительное право на результат интеллектуальной деятельности, созданный при выполнении контракта, принадлежит городу федерального значения Санкт-Петербургу, от имени которого выступает Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи» в соответствии с подпунктом 1 пункта 4 статьи 1240.1 Гражданского кодекса Российской Федерации (результат интеллектуальной деятельности необходим для предоставления государственных услуг и осуществления государственных функций).

3.14. Право собственности на результаты работ, включая отчетные документы и материалы, полученные в ходе выполнения работ по контракту, принадлежат городу федерального значения Санкт-Петербургу, от имени которого выступает Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи», и считаются переданными с момента подписания Государственным заказчиком документа о приемке в электронной форме, формируемого посредством единой информационной системы в сфере закупок.

3.15. Передача исходных кодов, разработанных в ходе выполнения работ программ 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) и запуска программы для ЭВМ.

3.16. Условия, предусмотренные пунктом 3.15 Описания объекта закупки, применяются в том числе для сценариев (скриптов), разработанных в ходе выполнения мероприятий по сборке программного обеспечения при использовании CI/CD в Репозитории, согласно пункту 2.2.2 Приложения № 2 Описанию объекта закупки.

При использовании свободного программного обеспечения Подрядчик предоставляет полный перечень всех компонентов свободного программного обеспечения, которые не были использованы при разработке Системы, но были включены в ее состав или необходимы для ее эксплуатации, а также исчерпывающую информацию об условиях использования таких компонентов свободного программного обеспечения.

Номер версии документа в рамках ГК

Номер АС в рамках ГК

Номер подсистемы в рамках АС либо в рамках ГК (в случае отсутствия АС)

Порядковый номер алиаса в рамках подсистемы

Опционально, не обязательное значение

Все значения данной строки должны быть указаны без пробелов, пробел является разделяющим символом

Выбрать что применимо с учетом формы обучения

Для баз данных должен быть предоставлен листинг кода, представляющий собой скрипт, в результате запуска которого формируется база данных со всеми элементами структуры базы данных (в том числе, таблицы, индексы, процедуры (пакеты), директории, роли, группы пользователей, и иные элементы), позволяющая провести установку системы на виртуальной инфраструктуре.

3.17. Документация на Систему и ее части (техническая и рабочая) должна содержать исчерпывающее описание принятых проектных решений в объеме, достаточном для ее развития и эксплуатации.²

3.18. Техническая и рабочая документация должна содержать описание разработанных результатов работ, в том числе программ для ЭВМ, прикладных программных интерфейсов, алгоритмов и протоколов информационного взаимодействия, технических требований, спецификаций и форматов обмена данными для взаимодействия с другими информационными системами, в объеме, достаточном для их установки, настройки, эксплуатации, сопровождения и развития в дальнейшем без привлечения подрядчика (исполнителя).

3.19. Техническая и рабочая документация должна быть выполнена в соответствии с п. 2.1.2 Приложения № 2 Описания объекта закупки.

3.20. 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.

3.21. 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.

3.22. Дистрибутив программы для ЭВМ, предусмотренный пунктом 3.21 Описания объекта закупки должен быть предоставлен для каждой программы для ЭВМ в отдельности.

3.23. Подрядчик в ходе предварительных комплексных и приемочных испытаний должен провести демонстрацию процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ с использованием средств, указанных в пункте 3.15 Описания объекта закупки, в соответствии с требованиями к обеспечению безопасности сборочной среды (п. 3.4 Приложения № 4 к Описанию объекта закупки) и в соответствии с инструкциями, приведенными в рабочей документации на Систему.

3.24. Передача Заказчику комплекта документов, материалов и сведений, предусмотренных нормативными правовыми актами Российской Федерации в сфере информационных технологий, защиты информации, правовой защиты интересов государства в области интеллектуальной собственности, включая документы, подтверждающие отказ авторов (разработчиков) от исключительных прав на передаваемые объекты интеллектуальной собственности в пользу Подрядчика, с проектами заявок на государственную регистрацию в установленном порядке прав Заказчика на результаты интеллектуальной деятельности, в том числе, но не исключая: изобретения, полезные модели, промышленные образцы, программы для электронных вычислительных машин, базы данных, топологии интегральных микросхем, а также исключительные права на результаты работ, включая объекты авторских прав и потенциально патентоспособные технические решения, секреты производства (ноу-хау), созданные в рамках Контракта, осуществляется Подрядчиком в составе отчетной документации, предусмотренной условиями Контракта.

² Объем информации включенный в документацию на Систему и ее части должен быть достаточным для развертывания Системы, ее штатной эксплуатации, сопровождения, в том числе в документации должно содержаться описание необходимых для штатной эксплуатации периодических регламентных работ.

3.25. Подрядчик должен обеспечить хранение архивных документов об организации работ по проектированию, созданию, эксплуатации и модернизации автоматизированных систем и баз данных в соответствии с приказом Федерального архивного агентства от 28.12.2021 № 142 «Об утверждении Перечня типовых архивных документов, образующихся в научно-технической и производственной деятельности организаций, с указанием сроков хранения».

3.26. Подрядчик по результатам выполненных работ по контракту обязан предоставить отчетные документы в соответствии с контрактом и перечнем отчетных документов (Приложение № 5 к Описанию объекта закупки) с учетом рекомендуемых форм отчетных документов (Приложение № 6 к Описанию объекта закупки).

3.27. Во всех случаях, когда Подрядчику требуется доступ к Репозиторию, Подрядчик направляет в адрес Заказчика с сопроводительным письмом заполненную и подписанную уполномоченным лицом Подрядчика Анкету для предоставления доступа к Репозиторию (п. 6 Приложения № 6 к Описанию объекта закупки). После получения от Подрядчика Анкеты для предоставления доступа к Репозиторию, Заказчик обеспечивает предоставление доступа к Репозиторию.

3.28. В случае, если в результате выполнения работ по развитию Системы создается либо модифицируется структура базы данных, принятые и реализованные Подрядчиком технические решения должны обеспечивать возможность переноса данных (миграции данных, конвертации данных при необходимости), обрабатываемых в Системе, во вновь созданную (модифицированную) базу данных с учетом ее функционального назначения.

Если для переноса данных (миграции данных, конвертации данных при необходимости) и последующего аудита данных в новой конфигурации необходимо программное обеспечение, дистрибутивы такого программного обеспечения передаются Подрядчиком Заказчику вместе с исходными кодами разработанного в ходе исполнения Контракта программного обеспечения.

В случае использования для указанных целей программного обеспечения, права на которое принадлежат третьим лицам, Подрядчик за свой счёт передаёт Заказчику дистрибутивы и права на использования такого программного обеспечения.

4. Требования к гарантии качества работы, а также требования к гарантийному сроку и (или) объему предоставления гарантий их качества

4.1. Гарантийный срок на выполненные работы: со дня утверждения Заказчиком документа о приемке результатов выполненных работ по 1 этапу, сформированного в электронной форме посредством единой информационной системы в сфере закупок до 31.12.2028. Гарантийный срок продлевается на период, в течение которого Получатель, Заказчик не могли пользоваться результатами выполненных работ по Контракту ввиду просрочки исполнения Подрядчиком обязательств, предусмотренных Контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Подрядчиком обязательств, предусмотренных Контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Подрядчиком обязательств, предусмотренных Контрактом.

4.2. Объем предоставления гарантии качества работ: в полном объеме на все результаты работ в соответствии с данным Описанием объекта закупки.

4.3. Устранение замечаний при согласовании отчетных документов с федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, осуществляется Подрядчиком в рамках гарантийных обязательств.

4.4. Подрядчик в течение гарантийного срока на выполненные работы предоставляет Заказчику без дополнительной оплаты обновления безопасности на разработанное и/или доработанное при выполнении работ специальное программное обеспечение.

4.5. В случае выявления в течение гарантийного срока уязвимостей в системном и общем программном обеспечении Системы, Подрядчик без дополнительной оплаты по требованию Заказчика содействует организации, осуществляющей сопровождение Системы, в установке обновлений безопасности на применяемое в Системе общее и системное программное обеспечение, Подрядчик в том числе обеспечивает личное присутствие своего представителя в месте и во время указанное Заказчиком. Обновления безопасности проприетарного общего и системного программного обеспечения предоставляются Заказчиком.

5. Требования энергетической эффективности работ

Требования не установлены.

Перечень приложений к Описанию объекта закупки

1. Приложение № 1. Перечень выполняемых работ.
2. Приложение № 2. Технические характеристики объекта закупки.
3. Приложение № 3. Функциональные и эксплуатационные характеристики объекта закупки.
4. Приложение № 4. Требования по информационной безопасности.
5. Приложение № 5. Перечень отчетных документов.
6. Приложение № 6. Рекомендуемые формы отчетных документов.

**Начальник управления цифровой трансформации
СПб ГКУ «УИТС»**

В.А. Гаврилов

**ПЕРЕЧЕНЬ
выполняемых работ**

№ п/п	Наименование работы	ОКПД2	Объем работ	Единица измерения объема работ
1	2	3	4	5
1	Выполнение работ по 1 этапу «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы. Техническое задание и Технический проект»			
1.1	Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы	62.01.11.000	1	усл.ед.
1.2	Разработка Дополнения №10 к Техническому заданию/Технического задания на создание Системы ³	62.01.11.000	1	усл.ед.
1.3	Разработка проектных решений по Системе и оформление комплекта документации Технического проекта на Систему ⁴	62.01.11.000	1	усл.ед.
2	Выполнение работ по 2 этапу «Рабочая документация и ввод в действие»			
2.1	Рабочая документация			
2.1.1	Разработка (в том числе модификация) программных средств системы	62.01.11.000	1	усл.ед.
2.1.2	Разработка рабочей документации на Систему	62.01.11.000	1	усл.ед.
2.2	Ввод в действие			

³ Разрабатывается Дополнение №10 к Техническому заданию на создание Системы в виде актуализированного технического задания на всю Систему, включая подсистему «Система защиты информации».

⁴ Разрабатывается в виде актуализированного технического проекта на всю Систему, включая подсистему «Система защиты информации».

№ п/п	Наименование работы	ОКПД2	Объем работ	Единица измерения объема работ
1	2	3	4	5
2.2.1	Подготовка объекта автоматизации к вводу в действие Системы	62.01.11.000	1	усл.ед.
2.2.2	Проведение предварительных комплексных испытаний Системы ⁵	62.01.11.000	1	усл.ед.
2.2.3	Подготовка персонала ⁶	62.01.11.000	1	усл.ед.
2.2.4	Проведение опытной эксплуатации и приемочных испытаний Системы ⁷	62.01.11.000	1	усл.ед.

⁵ Проводятся для развиваемых/создаваемых частей Системы, в объеме групп взаимосвязанных частей Системы, задач и комплексов задач, включая подсистему «Система защиты информации».

⁶ Проводится для развиваемых/создаваемых частей Системы, в объеме групп взаимосвязанных частей Системы, задач и комплексов задач, включая подсистему «Система защиты информации».

⁷ Проводятся для развиваемых/создаваемых частей Системы, в объеме групп взаимосвязанных частей Системы, задач и комплексов задач, включая подсистему «Система защиты информации».

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ объекта закупки

1. Выполнение работ по 1 этапу «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы. Техническое задание и Технический проект»

1.1. В ходе работ 1 этапа при обследовании объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы Подрядчик должен провести:

оценку класса защищенности Системы и уровня защищенности персональных данных, содержащихся в Системе;

оценку угроз безопасности информации, содержащейся в Системе, реализация которых может привести к нарушению безопасности информации, содержащейся в Системе.

1.1.1. Оценка класса защищенности Системы и уровня защищенности персональных данных, содержащихся в Системе, должна осуществляться для всей Системы в целом.

1.1.2. Оценка угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в Системе, проводится в соответствии с Методикой оценки угроз безопасности информации, утвержденной ФСТЭК России 05.02.2021, и включает в себя в том числе:

сбор и анализ данных о назначении, структуре, составе Системы, физических, логических, функциональных и технологических взаимосвязях между сегментами Системы, с иными информационными системами и информационно-телекоммуникационными сетями, о режимах обработки информации в Системе и в ее отдельных сегментах, особенностях функционирования Системы в соответствии с пунктом 6 Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной ФСТЭК России 15.02.2008, а также в соответствии с п. 3.2 Приложения № 4 к Описанию объекта закупки;

уточнение перечня объектов защиты информации Системы;

уточнение актуальных угроз безопасности информации, связанных с НСД к защищаемой информации, с утечкой информации по техническим каналам и с несанкционированным воздействием на информацию;

формирование совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак;

определение на основе совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и с учетом типа актуальных угроз требуемого класса СКЗИ.

1.1.3. В целях надлежащего выполнения Подрядчиком работ по 1 этапу Заказчик по заявке Подрядчика и при наличии технической возможности обеспечивает формирование и передает Подрядчику отчет об обследовании Системы. Отчет об обследовании Системы формируется в соответствии с требованиями ГОСТ Р 56939-2024 в части Процесса 6, Процесса 7, Процесса 16 Приложения № 4 к Описанию объекта закупки, а также в соответствии с п. 3.2 Приложения № 4 к Описанию объекта закупки.

1.1.4. По итогам работ по обследованию объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы Подрядчик

разрабатывает и передает Заказчику акт классификации Системы, акт определения уровня защищенности персональных данных Системы и модель угроз безопасности информации Системы.

В рамках 1 этапа выполняются следующие работы:

разработка Дополнения № 10 к Техническому заданию на создание Системы⁸;

разработка проектных решений по Системе и оформлении комплекта документации Технического проекта на Систему.⁹

1.2. В ходе работ 1 этапа при разработке Дополнения №10 к Техническому заданию на создание Системы, Подрядчик на основе функциональных и эксплуатационных характеристик объекта закупки, указанных в Приложении № 3 к Описанию объекта закупки, а также изменений в законодательстве Российской Федерации и Санкт-Петербурга (на дату начала работ по 1 этапу) и результатов работ по обследованию объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы должен произвести уточнения (актуализацию):

общих сведений о Системе;

назначения и целей создания (развития) Системы, включая указание автоматизируемых полномочий;

характеристик объектов автоматизации;

требований к Системе;

требований к мерам защиты информации в разрабатываемом специальном программном обеспечении Системы в соответствии с Процессом 3 Приложения № 4 к Описанию объекта закупки и п. 2.2 Приложения № 4 к Описанию объекта закупки.

состава и содержания работ по созданию Системы;

порядка контроля и приемки Системы;

порядка мониторинга работы Системы, производительности Системы, утилизации ресурсов РРЦОД выделенных для размещения Системы;

требований к составу и содержанию работ по подготовке объекта автоматизации к вводу Системы в действие;

требований к сценарию перехода на новую версию Системы в соответствии с требованиями Процесса 13 Приложения № 4 к Описанию объекта закупки, включающие требования к расчету требуемого объема и мощностей предпродуктивного контура, репликации продуктивного контура, установке и настройке нового ОПО и СрЗИ, установке и настройке новой версии СПО, требования к переходу с предпродуктивного на продуктивный контур, требование к определению состава утилизируемых мощностей, требование к утилизации мощностей, требования к созданию тестовых данных либо к обезличиванию данных, обрабатываемых в Системе в целях создания тестовых данных¹⁰.

требований к документированию;

источников разработки.

Техническое задание на создание подсистемы «Система защиты информации» является неотъемлемой частью Дополнения №_10_ к Техническому заданию на создание Системы.

Дополнение №10 к Техническому заданию на создание Системы оформляется в виде актуализированного Технического задания на создание Системы в соответствии с требованиями международных стандартов, национальных стандартов, государственных стандартов, технических регламентов, документов по стандартизации и иных руководящих

⁸ Разрабатывается Дополнение №10 к Техническому заданию на создание Системы в виде актуализированного технического задания на всю Систему, включая подсистему «Система защиты информации».

⁹ Разрабатывается в виде актуализированного технического проекта на всю Систему, включая подсистему «Система защиты информации».

¹⁰ Использование в качестве тестовых данных обезличенных данных обрабатываемых в Системе является приоритетным, Подрядчик вправе предусмотреть использование в качестве тестовых данных массива создаваемых (синтетических данных) только по согласованию с Заказчиком.

документов в сфере информации, информационных технологий и защиты информации, связи, приведенных в Таблице 1 Описания объекта закупки.

1.3. В ходе работ 1 этапа при разработке проектных решений по Системе и оформлении комплекта документации Технического проекта на Систему Подрядчик должен обеспечить:

разработку (доработку) общих решений по Системе и ее частям, функционально-алгоритмической структуре системы, по функциям персонала и организационной структуре, по структуре технических средств, по алгоритмам решений задач и применяемым языкам, по организации и ведению информационной базы, системе классификации и кодирования информации, по программному обеспечению;

разработку общих решений по защите информации, содержащейся в Системе, по ее функциональной структуре, техническим и программным средствам подсистемы «Система защиты информации» Системы, в том числе по применению СКЗИ в Системе, функциям персонала, обслуживающего подсистему «Система защиты информации» Системы;

разработку алгоритмов решения задач по защите информации в Системе, параметров настройки технических и программных средств, обеспечивающих реализацию функциональных возможностей подсистемы «Система защиты информации» Системы.

Проектные решения должны соответствовать Техническому заданию на создание Системы.

При необходимости разработки и/или доработки интерфейса Системы, разрабатываемый (дорабатываемый) интерфейс должен соответствовать следующим требованиям:

- Интерфейс Системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм;
- Цветовое решение интерфейса должно быть выдержано в спокойных тонах, не вызывающих зрительного утомления;
- Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям Системы;
- Все надписи экранных форм, а также сообщения, выдаваемые пользователю (кроме системных сообщений), должны быть на русском языке;
- Экранные формы должны проектироваться с учетом требований к их унификации в рамках Системы, а именно: все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации; для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы; термины, используемые для обозначения типовых операций (добавление информационной сущности, редактирование поля данных), а также последовательности действий пользователя при их выполнении, должны быть унифицированы; внешнее поведение сходных элементов интерфейса (реакция на наведение указателя «мыши», переключение фокуса, нажатие кнопки) должны реализовываться одинаково для однотипных элементов.

При разработке проектных решений Подрядчик должен учитывать следующее условие:

АРМ, подключаемые к Системе способом, при котором требуется регистрация АРМ, а также его пользователей программно-аппаратными и (или) программными средствами в Системе (прописывается в контроллере домена, межсетевых экранах и телекоммуникационном оборудовании, иными способами), должны входить в состав Системы. В состав Системы не должны входить АРМ, которые подключаются к Системе через веб-интерфейс или с использованием веб-приложения (в том числе через API).

По результатам разработки проектных решений по Системе Подрядчик проводит разработку, оформление, согласование и утверждение документации Технического проекта на Систему в объеме, необходимом для описания полной совокупности проектных решений и достаточном для дальнейшего выполнения работ по развитию, сопровождению и эксплуатации Системы. В случае выявления необходимости поставки технических и программных средств, Подрядчик разрабатывает ведомость покупных изделий для комплектования Системы.

По результатам разработки проектных решений по Системе, Подрядчик определяет и обосновывает вид проведения аттестационных испытаний и составляет «Акт определения вида аттестационных испытаний», в соответствии с Приказом ФСТЭК России от 29.04.2021 № 77.

По результатам разработки проектных решений по Системе Подрядчик определяет и обосновывает технические требования к подключению автоматизированных рабочих мест пользователей Системы, содержащие требования к техническому, программному обеспечению автоматизированного рабочего места, требования к характеристикам каналов связи, требования к средствам защиты информации.

Подрядчик разрабатывает сценарий перехода на новую версию Системы, учитывающий требования п. 1.1.1 (Процесс 13) Приложения № 4 к Описанию объекта закупки и включающий в себя:

процесс расчета требуемого объема и расчет требуемых мощностей предпродуктивного контура;

процесс полной или частичной репликации продуктивного контура в предпродуктивный контур с сохранением сетевой связности в пределах предпродуктивного контура¹¹;

процесс установки и настройки нового ОПО и СрЗИ¹²;

процесс установки и настройки новой версии СПО;

процесс перехода с предпродуктивного на продуктивный контур;

процесс определения состава утилизируемых мощностей.

Разработанные процессы сценария перехода должны включать в себя:

процедуры и необходимые скрипты для создания тестовых данных для использования на предпродуктивном контуре;

процедуры и необходимые скрипты для переноса данных с продуктивного на предпродуктивный контур;

процедуры и необходимые скрипты для перемещения лицензий между продуктивным и предпродуктивным контуром;

процедуры и необходимые скрипты для переключения между продуктивным и предпродуктивным контуром;

процедуры и необходимые скрипты для утилизации мощностей.

Технический проект на Систему оформляется в виде актуализированного Технического проекта на всю Систему в соответствии с требованиями международных стандартов, национальных стандартов, государственных стандартов, технических регламентов, документов по стандартизации и иных руководящих документов в сфере информации, информационных технологий и защиты информации, связи, приведенных в Таблице 1 Описания объекта закупки.

При разработке специального программного обеспечения Системы должны быть обеспечены меры защиты информации в соответствии с Процессом 3 Приложения № 4 к Описанию объекта закупки.

2. Выполнение работ по 2 этапу «Рабочая документация и ввод в действие»

2.1. В рамках 2 этапа в части «Рабочая документация» выполняются следующие работы: разработка (в том числе модификация) программных средств системы; разработка рабочей документации на Систему, в том числе разработка эксплуатационной документации на Систему;

2.1.1. Разработка (в том числе модификация) программных средств системы.

Работы по разработке (в том числе модификации) программных средств системы должны выполняться в соответствии с Техническим проектом и должны содержать:

¹¹ Производится в случае технологической необходимости по согласованию с Заказчиком

¹² В случаях, предусматривающих изменение архитектуры Системы или полную, или частичную замену ОС, СУБД, систем контейнеризации, систем виртуализации.

программирование и отладку программ;
 контроль отсутствия в разработанных (модифицированных) программных средствах Системы известных уязвимостей информационной безопасности;
 подготовку и передачу программной документации и документации для государственной регистрации прав.

Подрядчик получает исходный код путем клонирования Системы из Репозитория Git.

Исходные коды разработанных (в том числе модифицированных) программных средств системы должны быть загружены в Репозиторий по итогам выполнения работ (предоставление доступа к Репозиторию обеспечивается Заказчиком). В дополнение к исходным кодам в репозиторий Git должны быть загружены дистрибутивы, скрипты, Руководство системного программиста.

Изменения и дополнения в структуре баз данных Системы должны осуществляться автоматизированным способом.

Подрядчик проводит предварительные автономные испытания технических и программных средств Системы с тестированием на устойчивость и производительность под предельной нагрузкой в соответствии с ГОСТ Р 59792-2021¹³.

Сборка и развертывание программных средств Системы должны осуществляться автоматизированным способом с учётом требований информационной безопасности в соответствии с Приложением № 4 к Описанию объекта закупки. В репозитории GitLab ССПК должно быть настроено задание CI/CD с именем Distribution, выполняющее полную сборку, формирование дистрибутива, генерацию манифест-файлов manifest.json и manifest_D.json и их подписание с использованием УКЭП с целью достижения полной повторяемости при развертывании окружения и СПО.

Мощности для разработки (в том числе модификации) программных средств системы, в том числе для проведения предварительных автономных испытаний технических и программных средств Системы с тестированием на устойчивость и производительность под предельной нагрузкой Заказчиком не предоставляются.

Лицензии на общее программное обеспечение и средства защиты информации, используемых для разработки (в том числе модификации) программных средств системы, Заказчиком не предоставляются.

2.1.2. Разработка рабочей документации на Систему, в том числе разработка эксплуатационной документации на Систему.

Рабочая документация на Систему, в том числе эксплуатационная документация на Систему, должны обеспечивать выполнение работ по вводу в действие Системы, ее сопровождению и эксплуатации, в том числе для поддержания эксплуатационных характеристик (качества) Системы, в соответствии с принятыми на основании Технического задания на создание Системы проектными решениями¹⁴.

2.2. В рамках 2 этапа в части «Ввод в действие» выполняются следующие работы:

подготовка объекта автоматизации к вводу в действие Системы;
 проведение предварительных комплексных испытаний Системы;
 подготовка персонала;
 проведение опытной эксплуатации Системы;
 проведение приемочных испытаний Системы;

2.2.1. Подготовка объекта автоматизации к вводу в действие Системы должна включать:

¹³ Проводятся на развиваемые/создаваемые части Системы, включая подсистему «Система защиты информации» Системы, в объеме развиваемых/создаваемых задач и комплексов задач, а также на задачи и комплексы задач (в том числе не входящие в развиваемые, создаваемые части Системы), функционально взаимосвязанные с развиваемыми/создаваемыми задачами и комплексами задач.

По требованию Заказчика предварительные автономные испытания могут также проводиться на не развиваемые части Системы, не развиваемые задачи, комплексы задач с учетом принятых и реализованных Подрядчиком технических решений

¹⁴ Включая подсистему «Система защиты информации»

проведение проверки объекта автоматизации с целью определения уровня его подготовленности к вводу в действие Системы.

На этапе проверки объекта автоматизации Подрядчик должен собрать сведения о его оснащенности средствами вычислительной техники, системами связи и дополнительными техническими средствами, необходимыми для проведения автономной наладки технических средств Системы, включая подсистему «Система защиты информации», в том числе СКЗИ Системы и установки и отладки программных средств Системы, включая подсистему «Система защиты информации», в том числе СКЗИ Системы, и проверить его соответствие проектным решениям, изложенным в документах Технического проекта.

Результаты подготовки объекта автоматизации к вводу в действие Системы отражаются Подрядчиком в отчете о подготовленности объектов автоматизации к вводу в действие Системы.

2.2.2. Проведение предварительных комплексных испытаний Системы.

Предварительные комплексные испытания проводятся на развиваемые/создаваемые в рамках Контракта части Системы, включая подсистему «Система защиты информации» Системы, в объеме развиваемых/создаваемых задач и комплексов задач, а также на задачи и комплексы задач (в том числе не входящие в развиваемые, создаваемые части Системы), функционально взаимосвязанные с развиваемыми/создаваемыми задачами и комплексами задач.

По требованию Заказчика предварительные комплексные испытания могут также проводиться на не развиваемые части Системы, не развиваемые задачи, комплексы задач с учетом принятых и реализованных Подрядчиком технических решений.

До начала предварительных комплексных испытаний Системы Подрядчик в соответствии с разработанным сценарием перехода на новую версию Системы :

- формирует предпродуктивный контур Системы.

- направляет Заказчику уведомление о необходимости подготовки предпродуктивного контура Системы, Заказчик обеспечивает выделение необходимых мощностей и полную или частичную репликацию продуктивного контура Системы в предпродуктивный контур Системы с сохранением сетевой связности в пределах предпродуктивного контура с соблюдением разработанных процедур. Предпродуктивный контур Системы не может содержать данные, обрабатываемые в Системе и подлежащие защите;

- направляет уполномоченных специалистов для проведения развертывания Системы на предпродуктивном контуре. Работы по подготовке предпродуктивного контура Системы выполняются в месте, указанном Заказчиком, возможность выполнения подготовки предпродуктивного контура Системы с применением средств удаленного доступа не предусмотрена;

- при необходимости производит, установку и настройку новых экземпляров ОПО и СрЗИ, установку и настройку разработанной версии СПО и утилизирует мощности с соблюдением предусмотренных сценарием процедур;

- осуществляет сборку программного обеспечения Системы с использованием CI/CD в Репозитории способом, обеспечивающим повторяемость при поступлении новых версий программного обеспечения Системы.

При этом CI/CD должно быть настроено Подрядчиком в соответствии с требованиями, описанными в руководстве по его использованию, которое предоставляется Заказчиком в адрес Подрядчика в течение 5 (пяти) рабочих дней с момента начала выполнения работ по 2 этапу Контракта.

Настройка развертывания программного обеспечения Системы должна проводиться в отношении промышленных и непромышленных сред с помощью Ansible либо иного программного обеспечения.

Настройка программного обеспечения Системы должна позволять версионировать скрипты развертывания и повторно вносить изменения в среды, не меняя ранее примененных изменений (идемпотентность).

В решении по автоматизации сборки и развертывания Подрядчиком должны быть учтены:

- процедуры по безопасной разработке программного обеспечения в соответствии с Приложением № 4 к Описанию объекта закупки;

- процедуры контроля вносимых изменений в программное обеспечение;

- процедуры управления изменениями в программном обеспечении (включая изменения в исходном коде, артефактах, конфигурациях);

- процедуры автоматизации процессов передачи изменений (с помощью функциональности CI/CD).

В рабочей документации на систему должна содержаться информация и материалы для проведения развертывания:

- конфигурационные файлы для сборки и развертывания кода по технологии CI/CD;

- описание каждого этапа пайплайна, включая команды и зависимости между этапами;

- информационные материалы, объясняющие логику работы пайплайна и настройки для запуска пайплайна;

- готовые Ansible-плейбуки, роли и inventory-файлы для предпродуктивного и продуктивного контуров отдельно;

- инструкция по применению зашифрованных секретов (ansible-vault) и их интеграции в GitLab CI;

- описание переменных, используемых в пайплайне CI/CD и Ansible, с указанием названия, назначения, значения по умолчанию и контекста использования;

- описание структуры веток в репозитории;

- описание политик управления артефактами (GitLab Container Registry, Nexus);

- пошаговые инструкции по развертыванию и настройке ИС, в том числе миграции ИС с предпродуктивного контура на продуктивный, включая значения конфигурационных параметров для интеграций продуктивного контура с иными ИС;

- описание процедур обновления ИС.

Перед началом предварительных комплексных испытаний Подрядчик:

- обновляет Систему в Репозитории Git;

- передает Заказчику исходный текст (код) и дистрибутив программы, листинг кода базы данных;

- осуществляет установку и наладку программных средств Системы, в части защиты информации в СПО или иных СрЗИ с целью тестирования на совместимость и стабильность при работе в предпродуктивном контуре, включая подсистему «Система защиты информации»;

- загрузку тестовой информации в базы данных, в том числе внедрение классификаторов информации и справочников.

В программе и методике предварительных комплексных испытаний Подрядчик предусматривает комплексные испытания нефункциональных требований Системы. Объектами комплексных испытаний нефункциональных требований являются процессы в соответствии с п. 1.1.1 (Процессы 10 – 13) Приложения № 4 к Описанию объекта закупки.

В программе и методике предварительных комплексных испытаний Подрядчик предусматривает комплексные испытания подсистемы СЗИ (в том числе СКЗИ). Объектами комплексных испытаний подсистемы СЗИ являются СПО разрабатываемой Системы в части защиты информации, совокупности СКЗИ и совокупности СрЗИ иных частей Системы.

На серверах с приложениями СПО в Предпродуктивном контуре в целях проверки на совместимость необходима обязательная установка средств антивирусной защиты интеграции с СЗИ РРЦОД в соответствии с требованиями Процесса 12 Приложения № 4 к Описанию объекта закупки.

В случае, если в результате выполнения работ по развитию Системы создается либо модифицируется структура базы данных, Подрядчик в программе и методике предварительных комплексных испытаний предусматривает тесты по миграции данных

(конвертации данных если для миграции данных необходима их конвертация), в том числе тесты по аудиту данных в итоговой конфигурации, результат выполнения которых позволяет продемонстрировать возможность осуществления миграции (конвертации если необходимо), обеспечивающей сохранение и представление в программах для ЭВМ и базах данных Системы накопленных в Системе данных.

В программе и методике предварительных комплексных испытаний Подрядчик указывает:

- перечень и комплектность объектов комплексных испытаний;
- очередность испытаний объектов комплексных испытаний (объем, условия, порядок и методы проведения испытаний и обработки результатов);
- материально-техническое обеспечение испытаний;
- критерии приемки объектов комплексных испытаний и Системы в целом по результатам испытаний;
- порядок, методики и условия проведения проверок функционирования и взаимодействия объектов комплексных испытаний и функционирования Системы в целом;
- обеспечение безопасности при проведении испытаний.

Комплексные тесты должны обеспечивать проверку выполнения функций Системы или объектов комплексных испытаний во всех режимах функционирования, установленных в техническом задании на Систему, в том числе проверку взаимодействия между частями Системы, обеспечивать проверку реакции системы на некорректную информацию и аварийные ситуации, обеспечивать проверку показателей Системы в целом и ее составных частей на соответствие требованиям технического задания на Систему.

В состав комплексных тестов допускается включать встроенные в СрЗИ тесты, проверки, отчеты, пакетные командные файлы, на основании которых можно сделать выводы о соответствии проверяемых объектов требованиям технического задания подсистемы СИ. Допускаются объединение данных тестов в наборы тестов и в пакетные командные файлы, листинг командных файлов приводится в программе и методиках испытаний.

К программе и методике предварительных испытаний Подрядчик прилагает график проведения комплексных испытаний (при необходимости).

В пояснительную записку к программе и методике предварительных комплексных испытаний Подрядчик включает:

- технические характеристики Предпродуктивного контура, в котором проводятся испытания;
- в случае применения эмуляторов интеграций Системы с иными информационными системами, описание механизма работы эмулятора, а также мотивированное обоснование невозможности настройки интеграции с промышленными или тестовыми контурами информационных систем, интеграцию с которыми необходимо продемонстрировать;
- обоснование достаточности используемых тестовых данных;
- в случае использования тестовых данных, подготовленных Подрядчиком самостоятельно, обоснование невозможности использования при подготовке тестовых данных, данных содержащихся в Системе, в том числе деперсонализированных данных, содержащихся в Системе.

Проведение предварительных комплексных испытаний Системы осуществляется в соответствии с требованиями международных стандартов, национальных стандартов, государственных стандартов, технических регламентов, документов по стандартизации и иных руководящих документов в сфере информации, информационных технологий и защиты информации, связи, приведенных в Таблице 1 Описания объекта закупки, разработанной программой и методикой предварительных комплексных испытаний, а также на основании документов, разработанных Подрядчиком по результатам выполнения работ по пункту 2.2.1 Приложения № 2 к Описанию объекта закупки, подтверждающих выполнение работ.

Проведение предварительных комплексных испытаний Системы Подрядчик

осуществляет при участии Заказчика и Получателя в Предпродуктивном контуре. В рамках проведения предварительных комплексных испытаний Системы Подрядчик должен собрать предложения Получателя по развитию Системы.

Результаты проведения предварительных комплексных испытаний Системы должны быть оформлены Подрядчиком в форме протокола предварительных комплексных испытаний. Результаты и анализ собранных предложений отражаются Подрядчиком в рекомендациях по развитию Системы.

По итогам проведения предварительных комплексных испытаний Системы Подрядчик должен устранить недостатки (в случае выявления) и внести изменения в документацию, в том числе эксплуатационную, в соответствии с протоколом проведения предварительных комплексных испытаний.

По итогам проведения предварительных комплексных испытаний Системы Заказчик и Получатель принимают решение о вводе Системы в опытную эксплуатацию, а Подрядчик оформляет акт приемки в опытную эксплуатацию.

По результатам проведения предварительных комплексных испытаний Системы Подрядчик передает Заказчику полные атрибуты административного доступа к Системе, в том числе к административной консоли Системы, базам данных Системы, дочерним виртуальным машинам, на которых развернута Система, СрЗИ и иные атрибуты административного доступа необходимые для развертывания, сопровождения, эксплуатации Системы, по акту приема-передачи в запечатанном конверте.

В процессе проведения предварительных комплексных испытаний Системы Подрядчик должен провести демонстрацию процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ с использованием средств, указанных в пункте 3.15 Описания объекта закупки, в соответствии с требованиями безопасности информации Приложения № 4 к Описанию объекта закупки, а также в соответствии с инструкциями, приведенными в рабочей документации на Систему в Предпродуктивном контуре. Подрядчик осуществляет видеозапись процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ в формате скринкаста, а именно видеозахвата экрана с параллельной записью голосовых комментариев. Видеозапись процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ передается Подрядчиком Заказчику по результатам проведения предварительных комплексных испытаний Системы.

2.2.3. Подготовка персонала.

В рамках подготовки персонала Подрядчик должен провести подготовку пользователей Системы к ее использованию, а в части СЗИ в соответствии с требованиями к эксплуатации Системы, и собрать предложения пользователей по развитию Системы.

В части защиты информации, содержащейся в Системе, Подрядчик проводит подготовку специалистов структурного подразделения или должностного лица (работника), ответственных за защиту информации в Системе, а также подготовку иного персонала (пользователей) Системы в части, касающейся защиты информации.

Условия подготовки персонала:

наличие плана подготовки персонала (по ролям);

обеспечение пользователей Системы, включенных в списки для подготовки персонала, инструктивно-методическими материалами (руководство системного программиста, руководство пользователя (по ролям), описание базы данных, руководство администратора безопасности Системы, инструкция по формированию и ведению баз данных);

Подрядчик формирует 1 (одну) учебную группу. Общее количество пользователей, прошедших подготовку, – не менее 10 пользователей.

Подготовка персонала проводится в формате видеоконференцсвязи

План подготовки персонала должен учитывать проведение подготовки персонала с учетом ролевых моделей пользователей.

Список слушателей предоставляется Получателем на основании письменного запроса Подрядчика.

Перед началом подготовки персонала Подрядчик обязан передать атрибуты доступа и инструктивно-методические материалы для прохождения подготовки, в соответствии со списком слушателей, всем участникам подготовки персонала путем направления на адрес электронной почты (e-mail), не менее, чем за один рабочий день до начала видеоконференцсвязи. В сообщении электронной почты (e-mail) Подрядчик указывает контактные данные (телефон, ФИО ответственного сотрудника) для обращения слушателей по вопросам подключения к системе видеоконференцсвязи.

Регистрация слушателей в системе видеоконференцсвязи должна осуществляться с использованием служебной электронной почты (e-mail) слушателя, а также с отражением ФИО и должности слушателя.

Результаты и анализ собранных предложений от персонала (пользователей) Системы отражаются Подрядчиком в рекомендациях по развитию Системы.

2.2.4. Проведение опытной эксплуатации и приемочных испытаний Системы.

Опытная эксплуатация Системы обеспечивается Подрядчиком и проводится Получателем при участии Заказчика не менее 15 (Пятнадцати) рабочих дней на Предпродуктивном контуре Системы. Предпродуктивный контур должен обеспечивать возможность проведения отладочных работ для работы информационных обменов с иными информационными системами, которые имеют отдельный контур для испытаний. Доступ к таким контурам обеспечивает Заказчик. Опытная эксплуатация проводится на развиваемые/создаваемые в рамках Контракта части Системы, включая подсистему «Система защиты информации» Системы, в объеме развиваемых/создаваемых задач и комплексов задач, а также на задачи и комплексы задач (в том числе не входящие в развиваемые, создаваемые части Системы), функционально взаимосвязанные с развиваемыми/создаваемыми задачами и комплексами задач.

По требованию Заказчика опытная эксплуатация может также проводиться на не развиваемые части Системы, не развиваемые задачи, комплексы задач с учетом принятых и реализованных Подрядчиком технических решений.

Отбор пользователей, принимающих участие в опытной эксплуатации осуществляется Получателем в соответствии с документом «Схема организационной структуры». Общее количество пользователей, принимающих участие в опытной эксплуатации, – не менее 8 пользователей.

Перед началом опытной эксплуатации Подрядчик обязан передать атрибуты доступа к предпродуктивному контуру пользователям Системы, принимающим участие в опытной эксплуатации, а также организовать линию поддержки пользователей Системы во время проведения опытной эксплуатации и передать сведения о времени работы и контактных данных линии поддержки пользователей Системы пользователям Системы, принимающим участие в опытной эксплуатации. Способы доступа пользователей Системы, принимающих участие в опытной эксплуатации к линии поддержки (телефон, мессенджеры, e-mail), определяются Подрядчиком по согласованию с Заказчиком и Получателем.

Ход проведения опытной эксплуатации Системы должен быть оформлен Подрядчиком в форме рабочего журнала проведения опытной эксплуатации. В рамках проведения опытной эксплуатации Системы Подрядчик должен собрать предложения Получателя по развитию Системы. Результаты и анализ собранных предложений отражаются Подрядчиком в рекомендациях по развитию Системы.

По итогам проведения опытной эксплуатации Системы Подрядчик должен провести анализ результатов опытной эксплуатации, доработку (при необходимости) программного обеспечения Системы, дополнительную наладку (при необходимости) технических средств и общего программного обеспечения Системы и внести изменения в документацию, в том числе эксплуатационную.

По итогам проведения опытной эксплуатации Системы Заказчик и Получатель

принимают решение о допуске Системы к приемочным испытаниям, а Подрядчик оформляет акт о завершении опытной эксплуатации.

На этапе подготовки к приемочным испытаниям необходимо произвести настройку ВМ Системы (в случае, если не производилась ранее) для подключения к подсистеме «Контроль, анализ и мониторинг информационной безопасности исполнительных органов государственной власти Санкт-Петербурга» ЦОУ ИБ АПК БГ, а также установить средства антивирусной защиты и настроить данные средства для подключения к СЗИ РРЦОД в соответствии требованиями Процесса 13 Приложения № 4 к Описанию объекта закупки.

В виртуальных машинах Подрядчик должен настроить индивидуальные технологические учетные записи для обеспечения работы подсистемы «Контроль, анализ и мониторинг информационной безопасности исполнительных органов государственной власти Санкт-Петербурга» ЦОУ ИБ АПК БГ с минимально необходимыми привилегиями в соответствии требованиями Процесса 13 Приложения № 4 к Описанию объекта закупки.

Проведение приемочных испытаний Системы Подрядчик осуществляет при участии Заказчика и Получателя в предпродуктивном контуре Системы.

Приемочные испытания проводятся на развиваемые/создаваемые в рамках Контракта части Системы, включая подсистему «Система защиты информации» Системы, в объеме развиваемых/создаваемых задач и комплексов задач, а также на задачи и комплексы задач (в том числе не входящие в развиваемые, создаваемые части Системы), функционально взаимосвязанные с развиваемыми/создаваемыми задачами и комплексами задач.

В случае если по результатам опытной эксплуатации Подрядчик выполнил доработку программного обеспечения Системы, в процессе проведения приемочных испытаний Системы Подрядчик должен провести повторную демонстрацию процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ с использованием средств, указанных в пункте 3.15 Описания объекта закупки, а также в соответствии с инструкциями, приведенными в рабочей документации на Систему в тестовом контуре. Подрядчик осуществляет видеозапись процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ в формате скринкаста¹⁵, а именно видеозахвата экрана с параллельной записью голосовых комментариев. Видеозапись процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ передается Подрядчиком Заказчику по результатам приемочных испытаний Системы.

В программе и методике приемочных испытаний Подрядчик предусматривает приемочные испытания нефункциональных требований Системы. Объектами приемочных испытаний нефункциональных требований являются процессы в соответствии с п. 1.1.1 Приложения № 4 к Описанию объекта закупки.

В программе и методике приемочных испытаний Подрядчик предусматривает испытания объектов подсистемы СЗИ, включая СКЗИ. Объектами приемочных испытаний подсистемы СЗИ являются СПО разрабатываемой Системы в части защиты информации, совокупности СКЗИ и совокупности СрЗИ иных частей Системы. Приемочные испытания проводятся по отношению ко всем экземплярам СрЗИ.

В программе и методике приемочных испытаний СЗИ Подрядчик указывает:

перечень и комплектность объектов приемочных испытаний (объектами комплексных испытаний подсистемы СЗИ являются СПО разрабатываемой Системы в части защиты информации, совокупности СКЗИ и совокупности СрЗИ иных частей Системы).

перечень требований, которым должны соответствовать объекты приемочных испытаний (со ссылкой на пункты технического задания Системы);

объем, условия, порядок и методы проведения испытаний и критерии оценки результатов;

¹⁵ Качество передаваемого Подрядчиком скринкаста должно позволять прочитать любой текст, имеющийся на экране

перечень и последовательность проверок, которым должна быть подвергнута Система в соответствии с требованиями технического задания на Систему (со ссылкой на пункты мер и мероприятий по защите Системы из технического проекта на Систему);

перечень конечных точек всех приложений ОПО и СПО, используемых в Системе, в том числе технологические (временные) конечные точки, а именно: полный URL, порт, протокол, тип (тестовый/ продуктивный) и прочее;

методы выполнения проверок на соответствие показателей Системы в целом и ее составных частей требованиям технического задания на Систему;

материально-техническое и метрологическое обеспечение испытаний;

критерии приемки Системы и ее частей;

порядок, методики и условия проведения проверок функционирования и взаимодействия частей Системы, функционирования Системы в целом, в соответствии с требованиями технического задания на Систему;

обеспечение безопасности при проведении испытаний.

По согласованию с Заказчиком проверка СрЗИ в подсистеме СЗИ в зависимости от их специфики может проводиться автономно или в составе других частей Системы. Объединение задач при проверке в комплексах целесообразно проводить с учетом общности используемой информации и внутренних связей.

В состав проверок допускается включать встроенные в СрЗИ тесты, проверки и отчеты, пакетные командные файлы на основании которых можно сделать выводы о соответствии проверяемых объектов требованиям технического задания подсистемы СЗИ. Допускается объединение данных проверок в наборы проверок и в пакетные командные файлы, листинг командных файлов приводится в программе и методиках испытаний.

Проверки функционирования и взаимодействия частей Системы, которые возможно произвести при проведении приемочных испытаний Системы, включаются в программу и методику приемочных испытаний.

В пояснительную записку к программе и методике приемочных испытаний Подрядчик включает:

- технические характеристики Предпродуктивного контура, в котором проводятся испытания;

- в случае применения эмуляторов интеграций Системы с иными информационными системами, описание механизма работы эмулятора, а также мотивированное обоснование невозможности настройки интеграции с промышленными или тестовыми контурами информационных систем, интеграцию с которыми необходимо продемонстрировать;

- обоснование достаточности используемых тестовых данных;

Результаты проведения приемочных испытаний Системы должны быть оформлены Подрядчиком в форме протокола приемочных испытаний.

По итогам проведения приемочных испытаний Системы Подрядчик должен провести анализ результатов приемочных испытаний, устранить недостатки (в случае выявления) и внести изменения в документацию, в том числе эксплуатационную, в соответствии с протоколом проведения приемочных испытаний.

По итогам проведения приемочных испытаний Системы Подрядчик оформляет акт приемки в постоянную эксплуатацию и разрабатывает проект правового акта о вводе Системы в постоянную эксплуатацию и рекомендации по развитию Системы.

Перечень мероприятий по обеспечению ввода Системы в эксплуатацию и срок начала эксплуатации Системы определяется Подрядчиком в проекте правового акта с учетом результатов работ по развитию Системы.

3. Общие требования

Состав, содержание и порядок оформления отчетных документов по каждому этапу, а также сроки их предоставления Получателю и Заказчику должны соответствовать требованиям, указанным в Приложениях №№ 5-6 к Описанию объекта закупки.

ФУНКЦИОНАЛЬНЫЕ И ЭКСПЛУАТАЦИОННЫЕ ХАРАКТЕРИСТИКИ объекта закупки

1. Требования к функциям и задачам, выполняемым Системой

1.1. Развитие подсистемы «Строительный портал»

1.1.1. Развитие функции «Предоставление информации, содержащейся в ЕССК»

1.1.1.1. Развитие комплекса задач «Электронное взаимодействие с субъектами строительства в рамках исполнения процедур регионального государственного строительного надзора»

1.1.1.1.1. Развитие задачи «Взаимодействие в рамках дела строительного надзора»

В рамках развития задачи «Взаимодействие в рамках дела строительного надзора» необходимо:

реализовать в ЕССК возможность получения из РПГУ иправки в ВИС СГСН документа «Уведомление об изменении проектной документации» в формате xml, по схеме Минстроя России, введенной в действие на момент заключения Государственного контракта в соответствии с приказом Минстроя России от 02.11.2022 № 929/пр «Об утверждении требований к формату документов, используемых при осуществлении регионального государственного строительного надзора и составляемых в электронной форме»;

реализовать в ЕССК возможность направления в РПГУ и получения из ВИС СГСН документа «Уведомление об отказе в приеме документов» в формате xml, по схеме Минстроя России, введенной в действие на момент заключения Государственного контракта в соответствии с приказом Минстроя России от 02.11.2022 № 929/пр «Об утверждении требований к формату документов, используемых при осуществлении регионального государственного строительного надзора и составляемых в электронной форме».

При размещении в ЕССК xml-файлов, указанных выше документов «Уведомление об изменении проектной документации» и «Уведомление об отказе в приеме документов» должна автоматически обеспечиваться:

проверка соответствия таких документов настроенным в ЕССК xml-схемам Минстроя России для таких документов;

обработка отрицательных результатов проверки соответствия таких документов настроенным в ЕССК xml-схемам Минстроя России.

Способ реализации возможности получения из РПГУ иправки в ВИС СГСН документа «Уведомление об изменении проектной документации», способ реализации возможности направления в РПГУ и получения из ВИС СГСН документа «Уведомление об отказе в приеме документов», а также обработка отрицательных результатов проверки соответствия таких документов настроенным в ЕССК xml-схемам Минстроя России должны быть уточнены на этапе «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы, Техническое задание и Технический проект».

Требования к развитию задачи могут быть уточнены на этапе «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы, Техническое задание и Технический проект».

1.1.1.1.2. Развитие задачи «Электронный журнал работ»

В рамках развития задачи «Электронный журнал работ» необходимо:

реализовать возможность автоматической генерации значений полей для элементов, содержащих UUID (GUID) идентификаторы по заданному для них в xml-схеме ОЖР

шаблонам, соответствующим xml-схеме ведения ОЖР, утвержденной приказом Минстроя России от 02.12.2022 № 1026/пр «Об утверждении формы и порядка ведения общего журнала, в котором ведется учет выполнения работ по строительству, реконструкции, капитальному ремонту объекта капитального строительства» и введенной в действие на момент заключения Государственного контракта в соответствии с приказом Минстроя России от 16.05.2023 № 344/пр «Об утверждении состава и порядка ведения исполнительной документации при строительстве, реконструкции, капитальном ремонте объектов капитального строительства»; реализовать возможность формирования печатных форм xml-файлов ОЖР, размещенных в ЕССК, которые соответствуют xml-схемам Минстроя России, входящим в состав ОЖР:

GeneralWorkJournal.xsd;
 generalWorkJournalTitlePage.xsd;
 Participants.xsd;
 BuildingParticipants.xsd;
 BuildingInfo.xsd;
 idDesignerSupervisionRepresentative.xsd;
 idConstructionControlRepresentative.xsd;
 WorkInfo.xsd;
 sk5111.xsd;
 gsn35.xsd.

Требования к развитию задачи могут быть уточнены на этапе «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы, Техническое задание и Технический проект».

1.1.1.2. Развитие комплекса задач «Реестровая модель»

1.1.1.2.1. Развитие задачи «Учет результатов предоставления государственных услуг (процедур) в реестровой модели»

В рамках развития задачи «Учет результатов предоставления государственных услуг (процедур) в реестровой модели» необходимо обеспечить:

формирование реестра сведений включаемых в реестр выданных разрешений на строительство объекта капитального строительства, формируемых, по результатам исполнения государственной услуги «Выдавать разрешения на строительство при осуществлении строительства и реконструкции объектов капитального строительства, на проведение работ по созданию искусственного земельного участка в случаях, установленных действующим законодательством» (реестровый номер 7800000010000000901), по данным из xml-файлов проектов реестровых записей СГСН по РНС, соответствующих в своем составе приказу Минстроя России от 17 июля 2026 года № 457/пр «Об установлении типовой формы выписки из реестра разрешений на строительство объектов капитального строительства и типовой формы выписки из реестра разрешений на ввод объектов капитального строительства в эксплуатацию»;

формирование реестра сведений, включаемых в реестр разрешений на ввод объектов капитального строительства в эксплуатацию, формируемых по результатам исполнения государственной услуги «Выдавать разрешения на ввод объектов капитального строительства и искусственных земельных участков в эксплуатацию в случаях, установленных действующим законодательством» (реестровый номер 7800000010000000927), по данным из xml-файлов проектов реестровых записей СГСН по РНВ, соответствующих в своем составе приказу Минстроя России от 17 июля 2026 года № 457/пр «Об установлении типовой формы выписки из реестра разрешений на строительство объектов капитального строительства и типовой формы выписки из реестра разрешений на ввод объектов капитального строительства в эксплуатацию»;

формирование реестра сведений, включаемых в реестр уведомлений о планируемом строительстве объектов индивидуального жилищного строительства, формируемых по результатам исполнения государственной услуги «Направление уведомлений, предусмотренных пунктом 2 части 7, пунктом 3 части 8 статьи 51.1 Градостроительного кодекса Российской Федерации, при осуществлении строительства, реконструкции объектов индивидуального жилищного строительства, садовых домов» (реестровый номер 7800000000167156640), по данным из xml-файлов проектов реестровых записей по ИЖС, соответствующих в своем составе приказу Минстроя России от 21 апреля 2026 года № 257/пр «Об установлении составов сведений, содержащихся в реестре уведомлений о планируемом строительстве объектов индивидуального жилищного строительства и в реестре уведомлений об окончании строительства объектов индивидуального жилищного строительства»;

формирование реестра сведений, включаемых в реестр уведомлений об окончании строительства объектов индивидуального жилищного строительства, формируемых по результатам исполнения государственной услуги «Направление уведомлений, предусмотренных пунктом 5 части 19 статьи 55 Градостроительного кодекса Российской Федерации, при осуществлении строительства, реконструкции объектов индивидуального жилищного строительства, садовых домов (реестровый номер 7800000000167156630), по данным из xml-файлов проектов реестровых записей по ИЖС, соответствующих в своем составе приказу Минстроя России от 21 апреля 2026 года № 257/пр «Об установлении составов сведений, содержащихся в реестре уведомлений о планируемом строительстве объектов индивидуального жилищного строительства и в реестре уведомлений об окончании строительства объектов индивидуального жилищного строительства».

Состав полей реестровых записей по РНС и РНВ может быть уточнен на этапе «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы, Техническое задание и Технический проект».

Требования к развитию задачи могут быть уточнены на этапе «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы, Техническое задание и Технический проект».

1.2. Развитие подсистемы «Документооборот»

Развитие функции «Хранение информации, содержащейся в ЕССК»

1.2.1.1. Развитие комплекса задач «Документы»

1.2.1.1.1. Развитие задачи «Строительная документация»

В рамках развития задачи «Строительная документация» необходимо:

обеспечить возможность приема документа «Раздел №1 проектной документации «Пояснительная записка» в формате xml по версии схемы 1.07, утвержденной Минстроем РФ, загружаемого в ЕССК в рамках подачи заявления по услуге «Проведение государственной экспертизы проектной документации и (или) результатов инженерных изысканий» (реестровый номер 7800000000160201973), внутри загружаемого заявителем архива документов.

Требования к развитию задачи могут быть уточнены на этапе «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы, Техническое задание и Технический проект».

1.3. Развитие подсистемы «Интеграция»

1.3.1. Развитие функции «Взаимодействие с государственными информационными системами Санкт-Петербурга и иными информационными системами»

1.3.1.1. Создание задачи «Взаимодействие со СМЭВ по протоколу S3»

В рамках создания задачи «Взаимодействие со СМЭВ по протоколу S3» необходимо обеспечить возможность взаимодействия ЕССК с файловым хранилищем СМЭВ по http based

S3-протоколу и осуществить перевод используемого в ЕССК взаимодействия с файловым хранилищем СМЭВЗ на указанный протокол, описание которого приводится в пункте 7.2

«Работа с вложениями по протоколу S3» Методических рекомендаций по работе с Единым электронным сервисом Единой системы межведомственного электронного взаимодействия версии 3.5.0.29 (Приложение № 4 к протоколу заочного голосования членов президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 13 августа 2026 г. № 31пр, одобренное президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 13 августа 2026 г. № 31пр).

В рамках создания задачи должны быть обеспечены следующие возможности:

получение по протоколу S3 из файлового хранилища СМЭВЗ вложений к сообщениям в СМЭВЗ;

передача по протоколу S3 из ЕССК в файловое хранилища СМЭВЗ вложений к сообщениям в СМЭВЗ;

регистрация в БД ЕССК данных об использовании методов S3 API;

хранение данных о взаимодействии с S3 API в течение периода времени, заданного пользователем с ролью «Администратор», начиная с момента регистрации этих данных.

При передаче по протоколу S3 из ЕССК в файловое хранилища СМЭВЗ вложений к сообщениям в СМЭВЗ должны выполняться проверки:

соблюдения лимита на размер для передаваемого вложения не более 1ГБ;

Требования к созданию задачи могут быть уточнены на этапе «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы, Техническое задание и Технический проект».

1.3.1.2. Развитие задачи «Идентификация и аутентификация пользователей»

В рамках развития задачи «Идентификация и аутентификация пользователей» возможность аутентификации и авторизации пользователей при взаимодействии с ЕСОВ ТОРИС должна быть доработана в соответствии с обновленными методическими рекомендациями по взаимодействию с ЕСОВ ТОРИС.

Возможность аутентификации и авторизации пользователей при взаимодействии с ЕСОВ должна быть переведена на взаимодействие по протоколу авторизации OAuth 2.0.

Требования к доработке возможности аутентификации и авторизации пользователей при взаимодействии с ЕСОВ ТОРИС должны быть уточнены на этапе «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы, Техническое задание и Технический проект».

1.4. Развитие подсистемы «Система защиты информации»

Для обеспечения безопасности информации Системы должны быть реализованы функции защиты информации, содержащейся в Системе, которые должны соответствовать требованиям к защите информации, приведенными в п. 1.1 – 2.3 Приложения № 4 к Описанию объекта закупки, исключая п. 1.1.1 Приложения № 4 к Описанию объекта закупки.

2. Требования к развитию Системы по видам обеспечения

2.1. Требования к техническому обеспечению

2.1.1. Серверное оборудование Системы должно представлять собой виртуальный ресурс, созданный на базе оборудования, размещенного в РРЦОД.

2.1.2. Требования к техническому обеспечению приведены в п. 1.1 - 2.3 Приложения № 4 к Описанию объекта закупки.

2.2. Требования к программному обеспечению

Требования к программному обеспечению приведены в п. 1.1 - 2.3 Приложения № 4 к Описанию объекта закупки.

Средства защиты информации (включая проприетарное программное обеспечение защиты информации), серверные операционные системы и системы управления базами данных закупаются вне рамок Контракта в порядке, установленном постановлением Правительства Санкт-Петербурга от 30.12.2013 № 1095 «О системе закупок товаров, работ, услуг для обеспечения нужд Санкт-Петербурга».

ТРЕБОВАНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Нормативные-правовые требования

Технические решения, разработанные и реализованные Подрядчиком при выполнении работ по развитию Системы, должны соответствовать требованиям о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденным приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий», и обеспечивать возможность успешной аттестации Системы на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, в соответствии с приказом Федеральной службы по техническому и экспертному контролю от 29.04.2021 № 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

Результаты выполняемых работ, разработанные и реализованные Подрядчиком при выполнении работ по развитию Системы, должны соответствовать требованиям к защите информации, приведенным в пп. 1.1-1.3 Приложения № 4 к Описанию объекта закупки.

1.1. Нормативные требования к ГИС ФСТЭК России

Для достижения целей защиты информации должны быть применены необходимые меры защиты информации, а также должны быть обеспечены необходимые мероприятия, предусмотренные Требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных Предприятий, государственных учреждений, утвержденных приказом ФСТЭК России от 11.04.2025 № 117.

Для защиты информации должны применяться сертифицированные средства защиты информации в соответствии с инструкциями (правилами) по их эксплуатации, установленными разработчиками в эксплуатационной документации. Применяемые средства защиты информации должны быть обеспечены со стороны их разработчиков поддержкой безопасности на территории Российской Федерации, включая выпуск и применение обновлений программного обеспечения, обеспечивающих устранение выявленных уязвимостей, дефектов и недостатков.

Применяемые сертифицированные средства защиты информации должны соответствовать:

для защиты информационных систем 1 класса защищенности – не ниже чем 4 классу защиты и уровню доверия

для защиты информационных систем 2 класса защищенности – не ниже чем 5 классу защиты и уровню доверия;

для защиты информационных систем 3 класса защищенности – 6 классу защиты и уровню доверия

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

Для всех объектов защиты Системы должны быть обеспечена реализация мероприятий

по защите информации в соответствии с Методическим документом «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах» утвержденным ФСТЭК России 12.04.2026. Мероприятия по реализации в информационных системах мер по их защите и содержащейся в них информации по отношению к объектам защиты Системы, за исключением объекта защиты СПО, должны включать:

- реализацию базовых мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности, устанавливаемых оператором (обладателем информации);
- адаптацию базовых мер защиты информационных систем и содержащейся в них информации применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям функционирования информационных систем;
- верификацию адаптированных базовых мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

Технические меры по защите информации должны приниматься на аппаратном, системном, прикладном уровнях, а также в информационно-телекоммуникационной инфраструктуре при ее наличии. На аппаратном и системном уровнях защита информации должна обеспечиваться посредством применения встроенных в аппаратное обеспечение и системное программное обеспечение средств защиты информации. На прикладном и сетевом (инфраструктурном) уровнях защита информации должна обеспечиваться применением встроенных в прикладное программное обеспечение средств защиты информации и (или) применением наложенных и сетевых средств защиты информации.¹⁶

Мероприятия и меры по защите информации, должны реализовываться с использованием методических документов ФСТЭК России, ФСБ России и методического документа разработанного Заказчиком¹⁷.

При обработке в Системе информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации, требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных Предприятий, государственных учреждений, утвержденных приказом ФСТЭК России от 11.04.2025 № 117, должны быть применены и реализованы следующие требования:

1.1.1. Требования по ГОСТ Р 56939-2024 Разработка безопасного программного обеспечения

В соответствии с требованиями и рекомендациями, содержащимися в национальном стандарте Российской Федерации ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования» (далее - ГОСТ Р 56939-2024), к Подрядчику применяются требования по разработке безопасного программного обеспечения в соответствии с ГОСТ Р 56939-2024. Процессы разработки безопасного программного обеспечения, изложенные в ГОСТ Р 56939-2024, подлежат обязательной реализации в рамках настоящего Контракта, за исключением рекомендуемых к реализации требований, в формулировках которых используются вспомогательные глаголы «рекомендуется»

¹⁶ Для АРМ входящих в состав Системы приоритетно должно использоваться программное обеспечение, имеющее встроенные средства защиты информации. В случае если на АРМ, входящих в состав Системы, организовано администрирование средств защиты информации Системы, и используемое на АРМ программное обеспечение не имеет встроенных средств защиты информации, допускается использование наложенных средств защиты информации

¹⁷ Методический документ опубликован на сайте Санкт-Петербургского государственного казенного учреждения «Управление информационных технологий и связи» в сети Интернет, по адресу <https://uits.spb.ru/md/>

и «может». Подлежат обязательными к реализации Подрядчиком следующие базовые процессы:

Планирование процессов разработки безопасного программного обеспечения (далее – Процесс 1). Устанавливаются дополнительные требования, приведенные в п. 3.1 Приложения № 4 к Описанию объекта закупки;

Обучение сотрудников (далее – Процесс 2);

Формирование и предъявление требований безопасности к программному обеспечению (далее – Процесс 3). Устанавливаются дополнительные требования, приведенные в п. 2.2 Приложения № 4 к Описанию объекта закупки;

Управление конфигурацией программного обеспечения (далее – Процесс 4);

Управление недостатками и запросами на изменение программного обеспечения (далее – Процесс 5);

Разработка, уточнение и анализ архитектуры программного обеспечения (далее – Процесс 6). Устанавливаются дополнительные требования, приведенные в п. 3.2 Приложения № 4 к Описанию объекта закупки;

Моделирование угроз и разработка описания поверхности атаки (далее – Процесс 7);

Формирование и поддержание в актуальном состоянии правил кодирования (далее – Процесс 8);

Экспертиза исходного кода (далее – Процесс 9);

Статический анализ исходного кода (далее – Процесс 10). Устанавливаются дополнительные требования, приведенные в п. 3.3 Приложения № 4 к Описанию объекта закупки;

Динамический анализ кода программы (далее – Процесс 11);

Использование безопасной системы сборки программного обеспечения (далее – Процесс 12);

Обеспечение безопасности сборочной среды программного обеспечения (далее – Процесс 13). Устанавливаются дополнительные требования, приведенные в п. 3.4 Приложения № 4 к Описанию объекта закупки;

Управление доступом и контроль целостности кода при разработке программного обеспечения (далее – Процесс 14);

Обеспечение безопасности используемых секретов (далее – Процесс 15). Устанавливаются дополнительные требования, приведенные в п. 3.5 Приложения № 4 к Описанию объекта закупки;

Использование инструментов композиционного анализа (далее – Процесс 16);

Проверка кода на предмет внедрения вредоносного программного обеспечения через цепочки поставок (далее – Процесс 17);

Функциональное тестирование (далее – Процесс 18);

Нефункциональное тестирование (далее – Процесс 19). Устанавливаются дополнительные требования, приведенные в п. 3.6 Приложения № 4 к Описанию объекта закупки;

Обеспечение безопасности при выпуске готовой к эксплуатации версии программного обеспечения (далее – Процесс 20);

Безопасная поставка программного обеспечения пользователям (далее – Процесс 21);

Обеспечение поддержки программного обеспечения при эксплуатации пользователями (далее – Процесс 22);

Реагирование на информацию об уязвимостях (далее – Процесс 23);

Поиск уязвимостей в программном обеспечении при эксплуатации (далее – Процесс 24);

Процессы должны быть выражены в регламентах, которые должны содержать требования к реализации процесса разработки с учетом требований, изложенных в Приложении № 2 к Описанию объекта закупки. Выполнение реализаций требований подтверждается артефактами. Артефакты реализаций требований должны быть выражены в документах, отчетах, файлах, журналах, результатах работы инструментов, процессов,

сохраненных в электронном виде, на основании которых возможно подтвердить реализацию соответствующих требований.

В ходе реализации процессов разработки безопасного ПО должны быть реализованы меры по защите информации, относящейся к этим процессам, а именно: разграничение доступа к результатам исследований и тестирования, обеспечение защищенного хранения соответствующей информации и антивирусная защита.

Меры защиты информации для процессов разработки безопасного ПО должны быть включены в регламенты реализации соответствующих процессов разработки безопасного ПО.

Наборы артефактов, соответствующие определенным процессам, предоставляются в качестве отчетных документов, определенных в Приложении № 5 к Описанию объекта закупки.

Первичный отчет РБПО должен содержать наборы артефактов требований процессов, как по базовым, так и по соответствующим им расширенным процессам, по пунктам: Процесс 1, Процесс 2, Процесс 5, Процесс 8, Процесс 13, Процесс 14, Процесс 15.

Основной отчет РБПО должен содержать наборы артефактов требований процессов, как по базовым, так и по соответствующим им расширенным процессам, по пунктам: Процесс 3, Процесс 4, Процесс 6, Процесс 7, Процесс 9, Процесс 10, Процесс 11, Процесс 12, Процесс 16, Процесс 17, Процесс 18, Процесс 19.

Завершающий отчет РБПО должен содержать наборы артефактов требований процессов, как по базовым, так и по соответствующим им расширенным процессам, по пунктам: Процесс 20, Процесс 21, Процесс 22, Процесс 23, Процесс 24.

Отчеты РБПО предоставляются Подрядчиком с учетом требований, установленных в п. 3.5 Приложения № 4 к Описанию объекта закупки.

1.1.2. Требования по ГОСТ Р 59547-2021 «Мониторинг информационной безопасности»

В соответствии с требованиями и рекомендациями, содержащимися в национальном стандарте Российской Федерации ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения» (далее – ГОСТ Р 59547-2021), подлежат обязательной реализации мероприятия по мониторингу информационной безопасности в соответствии с разделами 4 и 5 ГОСТ Р 59547-2021.

Источниками данных мониторинга информационной безопасности в Системе определяются: средства защиты информации, общее программное и разрабатываемое специальное программное обеспечение, программно-технические средства, информационные сервисы, среда функционирования информационных (автоматизированных) систем, оператор информационных (автоматизированных) систем в части контроля действий, иные источники данных (в том числе внешние доступные источники данных).

1.1.3. Требования по ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем»

В соответствии с требованиями и рекомендациями, содержащимися в национальном стандарте Российской Федерации ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей» (далее – ГОСТ Р 56545-2015), предъявляются следующие требования к описанию уязвимостей:

Структура описания уязвимости должна обеспечивать достаточность информации для идентификации уязвимости и выполнения работ по анализу уязвимостей. Для однозначной идентификации уязвимости описание должно включать следующие элементы: идентификатор уязвимости, наименование уязвимости, класс уязвимости, наименование программного обеспечения и его версия.

Для обеспечения возможности выполнения работ по анализу уязвимостей, описание должно включать следующие элементы: идентификатор типа недостатка, тип недостатка, место возникновения (проявления) уязвимости, способ (правило) обнаружения уязвимости, возможные меры по устранению уязвимости.

При выполнении анализа уязвимостей необходимо руководствоваться методическим документом от 30.06.2025 ФСТЭК России «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств».

1.1.4. Требования по ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация»

В соответствии с требованиями и рекомендациями, содержащимися в национальном стандарте Российской Федерации ГОСТ Р 58833-2020 «Защита информации. Идентификация и аутентификация. Общие требования» (далее – ГОСТ Р 58833-2020), при реализации функций безопасности в создаваемом (дорабатываемом, модернизируемом) специальном программном обеспечении Системы необходимо обеспечить:

- первичную идентификацию, включающую подготовку, формирование и регистрацию информации о субъекте (объекте) доступа, а также присвоение субъекту (объекту) доступа идентификатора доступа и его регистрацию в перечне присвоенных идентификаторов;
- хранение и поддержание актуального состояния (обновление) идентификационной и аутентификационной информации субъекта (объекта) доступа;
- вторичную идентификацию, которая обеспечивает опознавание субъекта доступа, запросившего доступ к объекту доступа, по предъявленному идентификатору;
- аутентификацию, включающую проверку подлинности субъекта (объекта) доступа и принадлежности ему предъявленных идентификатора и аутентификационной информации.

Удаленный доступ пользователей к информационным системам в целях выполнения своих обязанностей (функций) должен осуществляться с использованием сетей связи, расположенных на территории Российской Федерации, посредством применения средств защиты канала передачи данных.

1.2. Нормативные требования к ИСПДн ФСТЭК России

При обработке в Системе информации, содержащей персональные данные, должны применяться (быть реализованы) меры защиты персональных данных определяемые в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119, а также «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18.02.2013 № 21.

1.3. Нормативные требования ФСБ России к СКЗИ

В случае использования для защиты информации, содержащейся в Системе, шифровальных (криптографических) средств защиты информации должны применяться требования о защите информации, установленные ФСБ России в соответствии с частью 5 статьи 16 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», а именно:

Требования к Составу и содержанию 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, утвержденные приказом ФСБ от 10.07.2014 № 378;

Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, а также при использовании технических средств и программ для электронных вычислительных машин и баз данных в соответствии с частью 5.1 статьи 13 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об

информации, информационных технологиях и о защите информации» с использованием шифровальных (криптографических) средств, утвержденные приказом ФСБ от 22.08.2026 № 321;

Требования к средствам электронной подписи и Требования к средствам удостоверяющего центра, утвержденные приказом ФСБ России от 27.12.2011 № 796.

2. Требования к объектам защиты Системы

2.1. Требования к средствам защиты информации

2.1.1. Применяемые в Системе серверные операционные системы должны иметь действующий сертификат ФСТЭК России в соответствии с классом защищенности Системы и/или уровнем защищенности Системы и соответствовать Требованиям безопасности информации к операционным системам, утвержденный приказом ФСТЭК России от 19.08.2016 № 119ДСП (Информационное сообщение от 18.10.2016 № 240/24/4893).

2.1.2. Применяемые в Системе системы управления базами данных должны быть сертифицированы в составе сертифицированной ФСТЭК России на соответствие требованиям безопасности информации операционной системы. В случае невозможности применения СУБД сертифицированной в составе сертифицированной ФСТЭК России на соответствие требованиям безопасности информации операционной системы, СУБД применяемые в Системе должны иметь действующий сертификат ФСТЭК России в соответствии с классом защищенности Системы и соответствовать Требованиям по безопасности информации к системам управления базами данных, утверждённые приказом ФСТЭК России от 14.04.2023 № 64ДСП.

2.1.3. Применяемые в Системе системы контейнеризации должны быть сертифицированы в составе сертифицированной операционной системы на соответствие требованиям безопасности информации ФСТЭК России. В случае невозможности применения системы контейнеризации, сертифицированной в составе сертифицированной операционной системы, допускается применение системы контейнеризации, сертифицированной ФСТЭК России и соответствующие Требованиям по безопасности информации к средствам контейнеризации, утверждённые приказом ФСТЭК России от 04.07.2022 № 118ДСП.

2.1.4. Применяемые в Системе системы виртуализации должны быть сертифицированы в составе сертифицированной операционной системы на соответствие требованиям безопасности информации ФСТЭК России. В случае невозможности применения системы виртуализации, сертифицированной в составе сертифицированной операционной системы, допускается применение системы виртуализации, сертифицированной ФСТЭК России и соответствовать требованиям по безопасности информации к средствам виртуализации, утверждённые приказом ФСТЭК России от 27.10.2022 № 187ДСП.

2.1.5. Применяемые в Системе средства технической защиты информации и средства обеспечения безопасности информационных технологий быть сертифицированы ФСТЭК России и обеспечения безопасности информационных технологий, утвержденные приказом ФСТЭК России от 02.06.2020 № 76ДСП.

2.1.6. Применяемые в Системе межсетевые экраны уровня сети должны иметь сертификат ФСТЭК и соответствовать Требованиям по безопасности информации к многофункциональным межсетевым экранам уровня сети (выписка)", утвержденным приказом ФСТЭК России от 07.03.2023 № 44.

2.1.7. Параметры настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, должны соответствовать требованиям к устранению возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.

2.1.8. Средства защиты информации, применяемые в Системе (включая СКЗИ), должны быть совместимы с другими компонентами Системы, а также с СЗИ (СКЗИ), установленными в РРЦОД. При проведении испытаний на серверах с приложениями СПО в целях проверки на совместимость необходима обязательная установка средств антивирусной защиты и интеграций с СЗИ РРЦОД.

Доступ для администрирования Системы, предоставляется с использованием АРМ, входящих в состав Системы и с использованием сети передачи данных, защищенных с использованием шифровальных (криптографических) средств

Размещение веб-сайтов и веб-порталов (включая API) Системы осуществляется с учетом использования имеющихся на серверных мощностях межсетевых экранов уровня веб-приложений.

Серверная и клиентская части API (в том числе API мобильного приложения) должны обеспечивать организационные и технические меры, соответствующие требованиям по обеспечению безопасности государственных информационных систем. При реализации API должны использоваться защищенные протоколы доступа к API и предприняты иные необходимые меры для предотвращения состояния «Отказ в обслуживании» серверной части API Системы.

Для контроля доступа к API должно быть предусмотрено обязательное использование процедур аутентификации и авторизации, за исключением случаев, когда набор данных, передаваемый по API эквивалентен анонимному доступу пользователя Системы.

2.2. Требования к специальному программному обеспечению

Для объекта защиты – СПО должна быть обеспечена реализация мероприятий по защите информации в соответствии с разделом 3 Методического документа «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах» утвержденным ФСТЭК России 12.04.2026.

При разработке специального программного обеспечения Системы должны быть обеспечены меры защиты информации, состав которых определяется на основании категории значимости, класса защищенности либо уровня защищенности Системы. Меры защиты информации при разработке безопасного программного обеспечения должны быть реализованы в соответствии с разделами 4 и 5 ГОСТ Р 56939-2024.

При разработке специального программного обеспечения Системы, функционирование которого предполагается на базе информационно-телекоммуникационной инфраструктуры РРЦОД, должны быть учтены меры защиты информации, реализованные в информационно-телекоммуникационной инфраструктуре РРЦОД.

Содержание базовых мер защиты информации для соответствующего класса защищенности информационной системы приведено в Таблице 1 Приложения № 4 к Описанию объекта закупки. Определение специальных мер защиты в СПО для их реализации в должны включать:

- реализацию базовых мер защиты информационных систем и содержащейся в них информации соответствующих классов защищенности;
- адаптацию базовых мер защиты информационных систем и содержащейся в них информации применительно к архитектуре информационных систем, применяемым информационным технологиям, особенностям функционирования информационных систем;
- верификацию адаптированных базовых мер защиты информационных систем и содержащейся в них информации в соответствии с актуальными угрозами и возможностями нарушителей, их дополнение и (или) усиление.

Состав мер защиты информации подлежит уточнению Подрядчиком в ходе работ 2 этапа.

Меры защиты информации в специальном программном обеспечении

Таблица 1

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Класс защищенности* информационной Системы			Уровень защищенности* Системы			
		3	2	1	4	3	2	1
1. Идентификация и аутентификация (ИАФ)								
ИАФ.1	Идентификация пользователей	+	+	+				
			1	1				
ИАФ.2	Идентификация устройств							
ИАФ.3	Аутентификация пользователей	+	+	+				
				1				
ИАФ.4	Аутентификация устройств							
2. Управление доступом (УПД)								
УПД.1	Реализация модели управления доступом	+	+	+				
			1, 2	1, 2				
УПД.2	Разграничение и контроль прав доступа	+	+	+				
			1	1, 2				
УПД.3	Управление учетными записями	+	+	+				
			1	1, 2				
УПД.4	Ограничение неуспешных и нерегламентированных попыток доступа в информационную систему	+	+	+				
			1, 2	1, 2				
УПД.5	Предупреждение пользователя при его доступе к информационной системе							
УПД.6	Оповещение пользователя о предыдущем входе в информационную систему							
УПД.7	Ограничение числа параллельных сеансов доступа		+	+				
				1a				
УПД.8	Блокирование сеанса доступа пользователя при неактивности	+	+	+				
УПД.9	Контроль действий субъектов доступа до идентификации и аутентификации	+	+	+				
3. Регистрация событий безопасности (РСБ)								
РСБ.1	Определение событий безопасности и данных о них, подлежащих регистрации	+	+	+				
		1	1	1, 3				
РСБ.2	Анализ событий безопасности и реагирование на них	+	+	+				
РСБ.3	Генерация временных меток при регистрации событий безопасности	+	+	+				
РСБ.4	Требования к сбору, хранению и защите данных о событиях безопасности	+	+	+				
РСБ.5	Реагирование на сбои при регистрации событий безопасности	+	+	+				
	4. Защита веб-технологий (ЗВТ)							
ЗВТ.1	Защита пользовательских данных	+	+	+				
ЗВТ.2	Управление доступом пользователей	+	+	+				
			1	1				
ЗВТ.3	Контроль и фильтрация трафика веб-приложений	+	+	+				
				1				
ЗВТ.4	Регистрация событий безопасности в веб-приложениях и реагирование на них	+	+	+				
ЗВТ.5	Проверка файлов, передаваемых веб-приложениями, на вредоносное программное обеспечение	+	+	+				

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Класс защищенности* информационной Системы			Уровень защищенности* Системы			
		3	2	1	4	3	2	1
5. Защита программных интерфейсов взаимодействия приложений (API) (ЗПИ)								
ЗПИ.1	Защита данных API	+	+	+				
			1	1				
ЗПИ.2	Управление доступом пользователей и приложений	+	+	+				
ЗПИ.3	Проверка на соответствие спецификации API	+	+	+				
				1				
6. Антивирусная защита (AB3)								
AB3.1	Антивирусная защита устройств	+	+	+				
7. Защита от компьютерных атак, направленных на отказ в обслуживании (ЗОО)								
ЗОО.1	Защита от компьютерных атак, направленных на отказ в обслуживании, при доступе внешних пользователей к прикладным сервисам, предоставляемым информационной системой	+	+	+				
ЗОО.3	Мониторинг состояния сервисов и интерфейсов	+	+	+				
ЗОО.5	Ограничение нагрузки	+	+	+				
8. Защита персональных данных								
ПДН.1	Обеспечение информационной системы автоматизированными средствами, регистрирующими запросы пользователей информационной системы на получение персональных данных, а также факты предоставления персональных данных по этим запросам в электронном журнале сообщений (состав данных: сотрудник, запросивший данные, дата время, факт получения) в “Журнале сообщений ПДн”. В ОРД должны быть определены отдельные права доступа к этим журналам, данные права должны быть реализованы средствами СПО. Доступ к журналам должен быть реализован непосредственно из интерфейса СПО в соответствии с назначенными правами доступа.						+	+
ПДН.2	Обеспечение информационной системы автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного “Журнала сообщений ПДн” средствами СПО в профилях или ролях Пользователя. Доступ к изменению данного профиля или роли должен быть реализован непосредственно из интерфейса СПО в соответствии с назначенными правами доступа.						+	+
ПДН.3	Обеспечение информационной системы автоматизированными средствами, позволяющими автоматически регистрировать в электронном "Журнале безопасности ПДн" изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе.							+
ПДН.4	Отражение в электронном "Журнале безопасности ПДн" полномочий сотрудников оператора персональных данных по доступу к персональным данным, содержащимся в информационной системе. Указанные полномочия должны соответствовать должностным обязанностям сотрудников оператора.							+
ПДН.5	Формирование, использование и хранение аутентификационной информации пользователей должно производиться исключительно с использованием хеш-функций по ГОСТ Р 34.11-2012				+	+	+	+

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Класс защищенности* информационной Системы			Уровень защищенности* Системы			
		3	2	1	4	3	2	1
ПДН.6	Обеспечение блокировки, уточнения и уничтожения персональных данных средствами СПО				+	+	+	+
9. Меры защиты в ГИС Санкт-Петербурга								
СПБ.1	Доступ в административную панель разрабатываемого СПО должен быть реализован исключительно из защищенной компьютерной сети ЗКС.	+	+	+				
СПБ.2	Реализация одной точка входа в административную панель для всех подсистем или всех АС разрабатываемого СПО.	+	+	+				
СПБ.3	Для всех подсистем или АС разрабатываемого СПО должна быть реализована единая аутентификация, авторизация, управление правами доступа и регистрации событий безопасности пользователей или процессов..	+	+	+				
СПБ.4	Регистрация событий безопасности в СПО должна быть реализована в формате логов централизованной системы сбора событий безопасности (совместимо с форматом системы централизованного сбора и обработки событий безопасности ЦОУ ИБ АПК-БГ)	+	+	+				
СПБ.5	Все настройки СПО в части безопасности должны быть доступны для оперативного редактирования непосредственно из интерфейса СПО с ограничениями, исключающими ослабление политик безопасности.	+	+	+				
СПБ.6	Доступ внешних аутентифицированных пользователей должен быть реализован исключительно через двухфакторную аутентификацию (рекомендуется использование ЕСИА).	+	+	+				
СПБ.7	Доступ внутренних не привилегированных пользователей должен быть реализован исключительно через двухфакторную аутентификацию (рекомендуется использование ЕСИА либо иную информационную систему).	+	+	+				
СПБ.8	Доступ внутренних привилегированных пользователей (администраторов, администраторов безопасности) должен быть реализован через многофакторную аутентификацию с использованием российских криптографических алгоритмов без использования ЕСИА	+	+	+				
СПБ.9	Для аутентификации всех процессов в разрабатываем СПО должны использоваться уникальные специальные учётные записи с минимально необходимым уровнем привилегий. Процессы должны иметь минимально необходимые привилегии	+	+	+				
СПБ.10	Разрабатываемое СПО никогда не должно показывать токены сессии в параметрах URL	+	+	+				
СПБ.11	Разрабатываемое СПО не должно регистрировать аутентификационную информацию или платежные реквизиты. Токены сессии должны храниться в журналах только в необратимой хешированной форме в соответствии с мерами ПДН.5	+	+	+				
СПБ.12	Разрабатываемое СПО не должно принимать большие файлы, которые могут заполнить хранилище или вызвать отказ в обслуживании	+	+	+				
СПБ.13	Разрабатываемое СПО проверяет сжатые файлы (например, zip, gz, docx, odt) на соответствие максимально допустимому несжатому размеру и максимальному количеству файлов, прежде чем распаковывать файл.	+	+	+				
СПБ.14	Установлена квота на размер файла и максимальное количество файлов на	+	+	+				

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Класс защищенности* информационной Системы			Уровень защищенности* Системы			
		3	2	1	4	3	2	1
	пользователя, чтобы гарантировать, что один пользователь не сможет заполнить хранилище							

*«+» - мера защиты информации включена в базовый набор мер для соответствующего класса защищенности информационной системы и должны выполняться требования к реализации данной меры защиты информации.

«цифра» или «цифра» «буква» - должны выполняться требования к усилению данной меры защиты информации, указанные в подразделе «Требования к усилению». Цифры и буквы, не включенные в таблицу и указанные под рубриками «требования к усилению» применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности.

Меры защиты информации, не обозначенные знаком «+», применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер защиты информации в информационной системе соответствующего класса защищенности.

Примечание к Таблице 1 «Меры защиты информации в специальном программном обеспечении»:

Специальные меры защиты в разрабатываемом специальном программном обеспечении применяются в соответствии с текущим классом защищенности Системы в соответствии с приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий» и в соответствии с текущим уровнем защищенности Системы в соответствии с приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». По отношению к мерам ПДН.1-ПДП.4 меры защиты определяются в соответствии с разделами IV и V приказа ФСБ от 10.07.2014 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»

Получение обновлений СПО должно производиться из источников, содержащих механизмы проверки подлинности и целостности обновлений.

В отношении обновлений библиотек СПО:

В процессе развития при использовании библиотек в СПО необходимо обновлять мажорную и минорную версию путем перехода на самую старшую мажорную и самую старшую минорную версию библиотеки;

При эксплуатации переход на более старшую мажорную и минорную версию не производится, за исключением случаев, когда обновление безопасности требует такого перехода.

Проектирование и реализация мер защиты информации при разработке в СПО Системы осуществляется в соответствии с Методическим документом, разработанным Заказчиком¹⁸.

В случае, если Система является ЗОКИИ и/или ИСПДн в части СПО, то применяется совокупность требований мер защиты, перечисленных в Таблице 1 Приложения № 4 к Описанию объекта закупки и мер защиты по соответствующим требованиям к данным типам Систем. В случае, если Система является ЗОКИИ и/или ИСПДн, но не является ГИС, то применяется совокупность требований мер защиты, перечисленных в Таблице 1 Приложения № 4 к Описанию объекта закупки мер защиты по соответствующим требованиям к данным типам Систем.

2.3. Требования к общему программному обеспечению

В операционных системах источником применяемого общего программного обеспечения, включая системы управления базами данных, системы контейнеризации, системы виртуализации, должен являться основной репозиторий, содержащий программные компоненты и пакеты, прошедшие сертификационные испытания, входящий в поставочный комплект сертифицированной операционной системы, реализующий все функциональные возможности и функции безопасности без использования пакетов из других репозиториев (замкнут по времени исполнения) и содержащий пакеты поддержки оборудования и драйверы для распространенных устройств и устройств на длительной поддержке.

Допускается установка общего программного обеспечения из дополнительных (расширенных) репозиториев и иных доверенных источников, с условием исключения возможности изменения программных компонентов, реализующих сертифицированные функции безопасности операционной системы, а также исключения возможности изменения программных компонентов, поддерживающие выполнение функции безопасности в соответствии с эксплуатационной документацией операционной системы.

В ходе проектирования Системы должен проводиться анализ доступных отечественных программных, программно-аппаратных и технических средств, а также предусмотрена возможность их применения в информационных системах в соответствии с Методическими рекомендациями по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации, утвержденными приказом Минцифры России от 18.01.2023 № 21.

В технической документации Системы состав общего программного обеспечения указывается в следующем формате (далее указано как пример): «Docker 25.0 и выше (из репозитория ОС «Astra Linux Special Edition 1.7 «Воронеж»)), где первое число – это мажорный номер версии, используемой на данный момент, второе число – номер минорной версии.

Устанавливаются требования по обеспечению доступа к веб-ресурсам Системы для внешних пользователей, в том числе с использованием отечественных SSL/TLS алгоритмов

¹⁸ Методический документ опубликован на сайте Санкт-Петербургского государственного казенного учреждения «Управление информационных технологий и связи» в сети Интернет, по адресу <https://uits.spb.ru/md/>

шифрования по ГОСТ Р 34.11-2012.

Тестирование обновлений необходимо производить до их применения в контурах промышленной эксплуатации информационных систем в соответствии с Методикой тестирования обновлений программных, программно-аппаратных средств, утвержденной ФСТЭК России.

Должна быть обеспечена возможность отмены обновлений программного обеспечения, в том числе возможность восстановления программного обеспечения из резервной копии.

Для тестирования обновлений должна быть применена тестовая зона информационной системы («песочница»).

Для применения обновлений программных, программно-аппаратных средств в информационной инфраструктуре, на которой размещается Система, должен быть развернут и функционировать выделенный сервер обновлений, предназначенный для их распространения и установки в информационных системах. Загрузка и установка в реальном режиме времени (on-line) обновлений программных, программно-аппаратных средств не допускается.

В отношении обновлений программных пакетов ОПО:

В процессе развития при использовании сертифицированного ОПО необходимо обновлять мажорную версию путем перехода на самую старшую стабильную сертифицированную мажорную версию. Во время исполнения контракта допускается минорное поднятие версии сертифицированного программного обеспечения;

В рамках гарантийных обязательств переход на более старшую сертифицированную мажорную версию не производится, за исключением случаев, когда обновление безопасности требует такого перехода;

В рамках гарантийных обязательств переход на более старшую сертифицированную минорную версию не производится, за исключением случаев, когда обновление безопасности требует такого перехода.

В операционных системах, системах контейнеризации должны быть произведены необходимые настройки для обеспечения:

использования доверенных источников и репозиториев. В случае размещения Системы в РРЦОД необходимо использовать доверенные репозитории РРЦОД, размещенного по адресу: <http://nexus.adc.vpn:8081>;

наличия учетных записей привилегированного доступа в соответствии с требованиями по обеспечению защиты информации при предоставлении пользователям привилегированного доступа ФСТЭК России, в том числе для обеспечения работы подсистемы «Контроль, анализ и мониторинг информационной безопасности исполнительных органов государственной власти Санкт-Петербурга» ЦОУ ИБ АПК БГ и СЗИ РРЦОД с минимально необходимыми привилегиями;

исключения «замораживания» библиотек для СПО при сборке;

исключения возможность использования сторонних сервисов (Docker Registry, DockerHub и ему подобных);

На виртуальных машинах с приложениями СПО в целях проверки на совместимость при проведении приемочных и предварительных комплексных испытаний необходима обязательная установка средств защиты информации, в том числе средств интеграции антивирусной защиты с системой защиты информации РРЦОД.

3. Расширенные требования к процессам

3.1. Расширенные требования к планированию процессов разработки безопасного программного обеспечения

Устанавливаются расширенные требования к планированию процессов разработки безопасного программного обеспечения с целью определения ответственности Подрядчика за защиту информации при реализации удаленного доступа работников подрядной организации к информационной инфраструктуре Заказчика и/или Оператора:

Предоставить список работников подрядной организации, планирующих осуществлять

удаленный доступ к информационной инфраструктуре Заказчика и/или Оператора. В случае изменения состава указанных работников, Подрядчик должен уведомить Заказчика о фактах таких изменений в течении 1 календарного рабочего дня.

Определить перечень информации и информационных ресурсов, расположенных в информационной инфраструктуре Заказчика и/или Оператора, к которым будет предоставляться удаленный доступ работникам подрядной организации, а также каналы связи, используемые для этих целей, при необходимости производить актуализацию данных списков в течении 1 календарного рабочего дня.

Подрядчик должен предоставить Заказчику политики информационной безопасности подрядной организации, результаты внутренних (внешних) аудитов информационной безопасности, результаты тестирования на проникновение инфраструктуры, план реагирования на компьютерные инциденты, а также регламент действий работников подрядной организации в случае нештатных ситуаций.

Подрядчик должен предоставить Заказчику контакты ответственных лиц по обеспечению информационной безопасности у Подрядчика, каналы для оперативного взаимодействия (резервные каналы взаимодействия), а также порядок такого взаимодействия.

Подрядчик во время исполнения Контракта обязан уведомлять Заказчика о наступлении в его инфраструктуре компьютерных инцидентов

Подрядчик должен реализовать следующие базовые минимально необходимые меры по информационной безопасности в собственной инфраструктуре:

- двухфакторная аутентификация пользователей;
- антивирусная защита автоматизированных рабочих мест и серверов;
- защищенное удаленное подключение с использованием средств криптографической защиты информации;
- защита почтовых сервисов от фишинга;
- защищенный обмен файлами и информацией через файловое хранилище;
- реализация парольной политики (длина пароля должна быть не менее 15 символов, пароль должен содержать буквы верхнего и нижнего регистра (А-Я, А-Z, а-я, а-z), специальные символы (!, », №, %, , /), в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов, словесные выражения)). Пароли от учетной записи подрядной организации и учетной записи органа (организации) должны отличаться.

Учетные записи работников Подрядчика для доступа в информационную систему должны иметь минимально необходимые права доступа, позволяющие выполнять их должностные обязанности. При увольнении или завершении выполнения работ по заключенному с подрядной организацией договору (государственному Контракту) учетные записи работников подрядной организации должны быть удалены.

Подрядчик должен обеспечить проверку и фиксацию местоположения удаленного доступа работников подрядной организации, с указанием адреса (например, IP-адрес, страна) и формата такого подключения (например, локально или удаленно).

Информационная инфраструктура, технические средства, программное обеспечение и обрабатываемая информация Подрядчика, включая сети связи, должны располагаться на территории Российской Федерации.

Подрядчик должен организовать запись всех действий пользователей при осуществлении удаленного подключения к инфраструктуре Заказчика и/или Оператора. Срок хранения журналов событий не менее 1 года. В случае возникновения инцидента Подрядчик обязан предоставлять указанные журналы Заказчику и Оператору.

Подрядчик должен обеспечить ограничение подключений к инфраструктуре Заказчика и/или Оператора работников Подрядчика вне рабочего времени. В случае необходимости такие подключения должны быть согласованы с Заказчиком и/или Оператором в период исполнения Контракта.

Подрядчик обязан производить периодические проверки на предмет возникновения

нештатных ситуаций или инцидентов информационной безопасности путем имитации указанных событий (проведение тренировок) в соответствии с действующим НПА.

Подрядчику запрещено использование программного обеспечения для удаленного управления автоматизированным рабочим местом (например, TeamViewer, AnyDesk, AmmyAdmin, AeroAdmin, Radmin, LiteManager, Удаленный рабочий стол Chrome, Microsoft Remote Assistance, Microsoft Remote Desktop и им подобным).

Для доступа к информационной инфраструктуре Заказчика и/или Подрядчика должны использоваться средства вычислительной техники, которые не используются в личных целях и к которым применяются корпоративные меры по информационной безопасности.

В случае привлечения для исполнения Контракта субподрядной организации Субподрядчики должны обеспечить реализацию мероприятий, предусмотренных абзацами выше.

3.2. Расширенные требования по аудиту информационной безопасности

Устанавливаются расширенные требования к разработке, уточнению и анализу архитектуры программного обеспечения в части аудита (обследования) информационной безопасности. Данные требования устанавливаются с целью контроля состава программно-технических средств, виртуального аппаратного обеспечения, программного обеспечения и средств защиты информации, мероприятий контроля (анализа) защищенности информации и контроля установок обновлений безопасности ПО, включая ПО средств ЗИ. Данные требования должны быть реализованы следующим образом:

сбор информации о составе ТС, входящих в состав Системы;

сбор информации о фактическом составе общего программного обеспечения и программных средств защиты информации, перечень образов и контейнеров в виртуальных и физических серверах, включая состав общего программного обеспечения и программных средств защиты информации в образах и контейнерах, наименований и версий операционной системы, перечень активных (разрешенных) репозиторий, перечней активных пользователей с указанием ролей и прав, информации об активных сетевых интерфейсах и пр.;

выявление (поиск) уязвимостей ОПО;

выявление (поиск) уязвимостей СПО.

Отчеты (артефакты) аудита должны формироваться с использованием или специализированного программного обеспечения, в исключительном случае с использованием скриптов оболочки в продуктивном контуре либо предпродуктивном контуре и содержать информацию:

В части состава ТС, входящих в состав Системы: наименование, ip-адрес, доменное имя (в случае наличия) для всех технических средств Системы;

В части состава общего программного обеспечения и программных средств защиты информации: наименование программного пакета или компонента, в том числе в контейнерах и образах, версию, наименование лицензии, сведения о пользователях и их правах, сведения об обновлениях безопасности, сведения об наименовании и версии дистрибутива, сведения об сетевых интерфейсах, наименовании хоста;

В части уязвимостей ОПО в соответствии с требованиями Процесса 3.

В части уязвимостей СПО в соответствии с требованиями Процесса 3.

Отчеты (артефакты) аудита формируются по заявке Подрядчика. Допускается формирования отчета об обследовании Системы по результатам сканирования копии продуктивного контура Системы. Отчеты об обследовании Системы должны быть представлены в электронном виде в порядке, изложенном в п. 3.5 Приложения № 4 к Описанию объекта закупки.

3.3. Расширенные требования к статическому анализу кода

Устанавливаются расширенные требования к порядку передачи и анализа исходных кодов программного обеспечения, разработанного (доработанного) в рамках выполнения работ по Контракту, для последующего статического анализа кода Заказчиком.

Формат передачи исходного кода, дистрибутива и листинга кода базы данных должен соответствовать указанному в п. 13 Приложения № 6 к Описанию объекта закупки.

Заказчик вправе использовать для статического анализа кода свободное программное обеспечение. В ходе статического анализа кода Заказчиком контролируется:

- возможность однозначной верификации версий программного обеспечения;
- наличие уязвимостей.

Заказчик вправе передать исходный код, дистрибутив и листинг баз данных в СПб ГКУ «СПб ИАЦ», являющийся оператором автоматизированной системы «Центр оперативного управления информационной безопасностью», входящей в состав аппаратно-программного комплекса «Безопасный город», в соответствии с постановлением Правительства Санкт-Петербурга от 25.08.2016 № 759 (далее – Оператор ЦОУ ИБ АПК БГ), для проведения статического анализа кода.

В случае выявления Заказчиком и/или Оператором ЦОУ ИБ АПК БГ по результатам анализа уязвимостей, известных уязвимостей информационных систем, которые могут быть использованы нарушителями, и возможность использования которых не может быть исключена за счет применения компенсирующих мер, Подрядчик обеспечивает доработку программного обеспечения и повторную передачу исходных кодов, дистрибутивов и листинга баз данных для проведения последующих циклов анализа до достижения результатов, удовлетворяющих требованиям Заказчика. При этом Подрядчик указывает текущую версию кода, а также приводит протокол изменений с учетом версий исходного кода.

Для развертывания в целях проведения испытаний должны использоваться версии исходного кода, дистрибутива и листинга баз данных не содержащие известных уязвимостей информационных систем, которые могут быть использованы нарушителями, и возможность использования которых не может быть исключена за счет применения компенсирующих мер.

3.4. Расширенные требования к обеспечению безопасности сборочной среды программного обеспечения

Устанавливаются расширенные требования к обеспечению безопасности сборочной среды программного обеспечения. Во всех случаях, когда Подрядчику требуется удаленный доступ к ресурсам предпроектного контура РРЦОД, Подрядчик должен принять необходимые организационные и технические меры по защите информации, относящейся к разработке программного обеспечения в рамках Контракта в информационной инфраструктуре Подрядчика, включая автоматизированные рабочие места Подрядчика (далее – АРМ Подрядчика), соответствующие требованиям о защите информации, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий», согласно установленному для Системы классу защищенности и уровню защищенности, а также Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Заявка на получение доступа к ресурсам РРЦОД должна соответствовать форме, приведенной в п. 7 Приложения № 6 к Описанию объекта закупки.

Для требуемого класса защищенности Системы на АРМ Администратора Подрядчика должна быть реализована установка и настройка сертифицированных по требованиям безопасности информации средств защиты информации: средств защиты информации от несанкционированного доступа, средств антивирусной защиты, средств контроля

защищенности информации, средств межсетевого экранирования, средств построения виртуальных частных сетей с использованием шифровальных (криптографических) средств VipNet Client (с целью совместимости с криптографической сетью РРЦОД), в случае отсутствия централизованного доступа к защищенной корпоративной сети исполнительных органов государственной власти Санкт-Петербурга.

Для требуемого класса защищенности Системы на АРМ Администратора Подрядчика должна быть реализована установка и настройка сертифицированных по требованиям безопасности информации средств защиты информации: средств защиты информации от несанкционированного доступа, средств антивирусной защиты, средств контроля защищенности информации, средств межсетевого экранирования, средств построения виртуальных частных сетей, совместимых с СКЗИ центра обработки данных и соответствующих требованиям класса защищенности Системы.

3.5. Расширенные требования к обеспечению безопасности используемых секретов в Системе

Прямое указание аутентификационной и ключевой информации в технической документации недопустимо, в отчетной документации данная информация указывается в виде алиасов. Таковой информацией является: IP-адрес, номер порта, URL конечных точек доступа, пароли (включая тестовые), токены доступа (включая тестовые), и пр.

Например: #IP1, #порт7, #URL18, #пароль23, #токен3, и пр.

Список соответствия «алиас – значение» приводится в отчетном документе «Информация о Системе», а также передаются Заказчику в электронном виде. Допускается указание нескольких значений алиасов, к примеру, для продуктивного контура и для предпродуктивного контура. Формат документа «Информация о Системе» приведен в п. 14 Приложения № 6 к Описанию объекта закупки.

Наборы артефактов предоставляются в форме электронных документов, подписанных УКЭП уполномоченного лица/лиц Подрядчика, Получателя.

Наборы артефактов, соответствующие требованиям процесса, упаковываются в контейнеры формата tar или архивы формата 7z, zip, rar, gzip. Данные контейнеры, либо архивы, подлежат обязательному шифрованию с использованием предварительно предоставленных сертификатов открытых ключей представителей Заказчика с использованием алгоритмов ГОСТ Р 34.11-2012. Зашифрованные контейнеры передаются по открытым каналам связи с последующим размещением в СФУП либо для иного дальнейшего использования.

Устанавливается требование по запрету на трансляцию предварительных комплексных и приемочных испытаний в части СЗИ вне доверенных систем видеоконференцсвязи. В качестве доверенной системы видеоконференцсвязи устанавливается Городская система видеоконференцсвязи исполнительных органов государственной власти Санкт-Петербурга (ГС ВКС ИОВ Санкт-Петербурга).

3.6. Расширенные требования к нефункциональному тестированию

Устанавливаются расширенные требования к обеспечению мер защиты информации, применяемых к системам управления базами данных:

Подрядчик предоставляет Заказчику сведения о типе, структуре и назначении используемых баз данных, а также описание хранимой в базе данных информации, включая сведения о наличии персональных данных и (при наличии) иной информации ограниченного доступа в соответствии с отчетным документом «Описание организации информационной базы»;

Для осуществления автоматизированной классификации данных специализированными средствами, Подрядчик создает в СУБД отдельные (индивидуальные) учетные записи с минимально необходимыми правами (только чтение, без прав изменения/удаления/администрирования) в объеме, необходимом для классификации (по согласованному перечню баз данных/схем), и передает реквизиты доступа Заказчику.

Реквизиты доступа передаются в соответствии с п.3.5 Приложения № 4 к Описанию объекта закупки;

Учетные записи создаются на период проведения классификации; по завершении работ Подрядчик обеспечивает немедленную блокировку/удаление указанных учетных записей и смену паролей (реквизитов доступа), выданных на период работ;

Заказчик проводит классификацию данных, хранимых в базах данных, силами Оператора ЦОУ ИБ АПК БГ с даты получения реквизитов доступа;

Оператор ЦОУ ИБ АПК БГ направляет отчет Подрядчику и Заказчику.

3.7. Расширенные требования по мониторингу информационной безопасности

Расширенными требованиями по мониторингу информационной безопасности с целью сбора данных о событиях безопасности и иных данных мониторинга от различных источников для Системы определены и должны быть реализованы в продуктивном и предпродуктивном (при необходимости) контурах Системы:

интеграция и взаимодействие с системами защиты информации РРЦОД (или иной информационной инфраструктурой);

интеграция с системой защиты информации РРЦОД в части антивирусной защиты путем установки программного агента антивирусного программного обеспечения на виртуальную машину;

настройка взаимодействия виртуальной операционной системы с системой защиты информации РРЦОД в части контроля действий привилегированных пользователей;

настройка взаимодействия системы управления базами данных с системой аутентификации хостовой (по отношению к СУБД) виртуальной операционной системой с использованием Pluggable Authentication Modules;

взаимодействие со средствами защиты информации ЦОУ ИБ АПК БГ (или иной информационной инфраструктурой);

настройка взаимодействия виртуальной операционной системы с системой централизованного сбора и обработки событий безопасности;

настройка взаимодействия специального программного обеспечения с системой централизованного сбора и обработки событий безопасности.

Приложение № 5
к Описанию объекта закупки

1. Отчетные документы, за исключением случаев, прямо указанных в Таблице 1 Приложения № 5 к Описанию объекта закупки, предоставляются Подрядчиком Заказчику путем направления электронных документов, подписанных усиленной квалифицированной подписью уполномоченного лица Подрядчика в сроки, указанные в Таблице 1 Приложения № 5 к Описанию объекта закупки, в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме¹⁹. Отчетные документы, предоставляемые Подрядчиком Заказчику в электронной форме, дополнительно предоставляются в формате .docx, текстовое содержимое передаваемых файлов должно быть полностью машиночитаемым с применением распространенных текстовых редакторов.

2. В случае, если отчетный документ содержит подписи сотрудников Подрядчика (кроме лица имеющего права действовать от имени Подрядчика без доверенности, либо иного лица, уполномоченного подписывать отчетные документы от имени Подрядчика) такой документ предоставляется в виде скана-образа документа, содержащего собственноручные подписи сотрудников Подрядчика, и такой скан-образ документа должен быть подписан УКЭП уполномоченного лица Подрядчика.

3. Отчетные документы передаваемые на физических носителях передаются Подрядчиком Заказчику нарочным, почтой, курьерскими службами по адресу Заказчика, передача отчетных документов на физических носителях оформляется актом (п. 10 Приложения № 6 к Описанию объекта закупки) составляемым в двух экземплярах, по одному для Заказчика и Подрядчика.

4. Отчетные документы, указанные в Таблице 1 Приложения № 5 к Описанию объекта закупки, предоставляемые в форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, рассматриваются Получателем посредством СФУП и подписываются УКЭП уполномоченного лица Получателя.

Перечень отчетных документов²⁰

Таблица 1

№ п/п	Наименование отчетных документов	Требования к структуре, содержанию и оформлению документов	Требования к сроку предоставления отчетных документов	Требования к порядку предоставления отчетных документов
1	2	3	4	5
1 этап «Обследование объектов информатизации Системы с целью уточнения требований к подсистеме «Система защиты информации» Системы. Техническое задание и Технический проект»²¹				

¹⁹ Методический документ опубликован на сайте Санкт-Петербургского государственного казенного учреждения «Управление информационных технологий и связи» в сети Интернет, по адресу <https://uits.spb.ru/md/>

²⁰ Все разрабатываемые документы должны быть выполнены на русском языке с учетом требований Инструкции по делопроизводству в Комитете по информатизации и связи, утвержденной распоряжением Комитета по информатизации и связи от 28.12.2018 № 347-р «Об утверждении Инструкции по делопроизводству в Комитете по информатизации и связи».

²¹ Разработанные документы должны отвечать требованиям о защите информации, устанавливаемым федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

1	2	3	4	5
1.1	Акт классификации Системы ²²	В соответствии с приказом ФСТЭК России от 11.04.2025 № 117; приказом ФСТЭК России от 29.04.2021 № 77; Документ должен содержать: определение класса защищенности Системы; список представителей Подрядчика, составивших акт. При определении класса защищенности Системы приводят основание создания Системы (правовой акт/решение о создании Системы), характеристики, необходимые для определения класса защищенности, в соответствии с Требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденными приказом ФСТЭК России, от 11.04.2025 № 117. Форма Акта классификации Системы определяется приложением № 3 к Порядку организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите	Подрядчик предоставляет: не позднее чем за 13 (Тринадцать) рабочих дней до дня окончания выполнения работ по 1 этапу. Срок рассмотрения и утверждения Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.

²² Разрабатывается на Систему.

1	2	3	4	5
		информации, не составляющей государственную тайну, утвержденному приказом ФСТЭК России от 29.04.2021 № 77.		
1.2	Акт определения уровня защищенности персональных данных Системы ²³	В соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119; приказом ФСТЭК России от 11.04.2025 № 117; Документ должен содержать: определение уровня защищенности персональных данных, содержащихся в Системе; состав комиссии (список представителей Подрядчика, составивших акт). При определении уровня защищенности персональных данных, содержащихся в Системе, приводят основание создания Системы (правовой акт/решение о создании Системы), характеристики, необходимые для определения уровня защищенности персональных данных при их обработке в Системе, в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».		В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.

²³ Разрабатывается на Систему.

1	2	3	4	5
1.3	Модель угроз безопасности информации Системы ²⁴	В соответствии с приказом ФСТЭК России от 11.04.2025 № 117; приказом ФСБ России от 10.07.2014 № 378; методическим документом «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», утвержденным ФСТЭК России 12.04.2026; методическим документом «Методика оценки угроз безопасности информации», утвержденным ФСТЭК России 05.02.2021; ГОСТ Р 51583-2014; ГОСТ Р 56545-2015; ГОСТ Р 56546-2015; ГОСТ Р 56938-2016; ГОСТ Р ИСО/МЭК 27002-2021; ГОСТ Р ИСО/МЭК 27005-2010; ГОСТ Р 7.0.97-2025; Структура Модели угроз безопасности информации Системы должна соответствовать приведенной в Приложении 3 к Методике оценки угроз безопасности информации, утвержденной ФСТЭК России 05.02.2021. Модель угроз безопасности информации Системы должна учитывать требования «Базовой	Подрядчик предоставляет: не позднее чем за 10 (десять) рабочих дней до дня окончания выполнения работ по 1 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на бумажном носителе в 1 (одном) экземпляре с подписью уполномоченного лица Подрядчика.

²⁴ Разрабатывается на Систему.

1	2	3	4	5
		модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной ФСТЭК России 15.02.2008, а также требования приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» при оценке угроз безопасности информации, связанных с нарушением безопасности шифровальных (криптографических) средств защиты информации и формировании модели нарушителя, совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, в том числе, анализ угроз и обоснование класса СКЗИ и иных нормативно-		

1	2	3	4	5
		правовых актов.		
1.4	Отчет РБПО. Часть 1	В соответствии с п. 1.1.1 Приложения № 4 Описания объекта закупки должен содержать наборы артефактов требований процессов, как по базовым, так и по соответствующим им расширенным процессам, по пунктам: Процесс 1, Процесс 2, Процесс 5, Процесс 8, Процесс 13, Процесс 14, Процесс 15. Приложения № 4 Описания объекта закупки.	Подрядчик предоставляет: не позднее чем за 10 (десять) рабочих дней до дня окончания выполнения работ по 1 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
1.4.1	Информация о Системе	В соответствии с п. 14 Приложения № 6 Описания объекта закупки.		
Разработка Дополнения №10 к Техническому заданию/ на создание Системы				
1.5	Дополнение №10 к Техническому заданию на создание Системы ²⁵	Приказ ФСТЭК России от 11.04.2025 № 117; ГОСТ 34.602-2020; ГОСТ 34.201-2020 ГОСТ Р 51624-2000; ГОСТ Р 51583-2014; ГОСТ Р 56938-2016; ГОСТ Р ИСО/МЭК 27002-2021; акт классификации Системы; акт определения уровня	Подрядчик предоставляет: не позднее чем за 8 (восемь) рабочих дней до дня окончания выполнения работ по 1 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке,

²⁵ Разрабатывается Дополнение № 10 к Техническому заданию на создание Системы в виде актуализированного технического задания на всю включая подсистему «Система защиты информации». Разработанные документы должны отвечать требованиям о защите информации, устанавливаемым федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий

1	2	3	4	5
		защищенности персональных данных Системы; модель угроз безопасности информации Системы.		предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на бумажном носителе в 1 (одном) экземпляре с подписью уполномоченного лица Подрядчика.
Разработка проектных решений по Системе и оформление комплекта документации Технического проекта на Систему				
1.6	Комплект документации Технического проекта на Систему в составе²⁶:			
1.6.1	Лист утверждения Технического проекта	Титульный лист является первым листом документа. Титульный лист, составленный на альбом документов, является первым	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 1 этапу	В форме электронного документа, подписанного

²⁶ Разрабатывается в виде актуализированного технического проекта на всю Систему, включая подсистему «Система защиты информации». Указывается версия документа. Разработанные документы должны отвечать требованиям о защите информации, устанавливаемым федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

1	2	3	4	5
		листом описи этого альбома. Лист утверждения выпускают для документов, на которых по условиям их использования разработчик и (или) заказчик считает нецелесообразным приводить наименования организаций, должности и фамилии лиц, подписавших эти документы. Лист утверждения выпускают для одного документа, для нескольких документов, для альбома документов или комплекта документов. Допускается выпускать Лист утверждения для отдельной части или нескольких частей документа. Обозначение Листа утверждения состоит из обозначения документа, к которому он относится, с добавлением через дефис кода Листа утверждения, например, XXXX.XXXXXX.XXXТУ-ЛУ. Если Лист утверждения выпускается для альбома документов, ему присваивают обозначение одного из этих документов с добавлением через дефис кода Листа утверждения и записывают в опись альбома первым. Если Лист утверждения выпускается для нескольких документов, ему присваивают	Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.

1	2	3	4	5
		обозначение одного из этих документов с добавлением через дефис кода Листа утверждения и записывают в спецификацию, в которую входит этот документ. Если Лист утверждения выпускается для комплекта документов, ему присваивают обозначение спецификации с добавлением кода ЛУ и записывают в спецификацию в раздел «Документация» первым. При записи Листа утверждения в спецификацию следует указывать в графе «Примечание» — «Размножить по указанию». Лист утверждения должен соответствовать ГОСТ Р 2.105-2019. При формировании Листа утверждения: Для документа «План резервного копирования и восстановления» применять код Д1 Для документа «Технические требования к подключению автоматизированных рабочих мест пользователей государственной информационной системы» применять код Д2		
1.6.2	Ведомость Технического проекта	Приказ ФСТЭК России от 11.04.2025 № 117; ГОСТ Р 59795-2021; ГОСТ Р 51624-2000; ГОСТ Р 51583-2014;		В форме электронного документа, подписанного УКЭП
1.6.3	Пояснительная записка			
1.6.4	Схема функциональной структуры			
1.6.5	Схема организационной			

1	2	3	4	5
	структуры	ГОСТ Р ИСО/МЭК 27002-2021;		уполномоченного
1.6.6	Описание автоматизируемых функций	В Пояснительной записке должна быть отображена реализация мер защиты информации		лица Подрядчика, документ
1.6.7	Описание организации информационной базы	в разрабатываемом специальном программном обеспечении Системы, состав которых определяется на основании категории значимости, класса защищенности либо уровня защищенности Системы		предоставляется в порядке,
1.6.8	Описание систем классификации и кодирования			предусмотренном Методическим документом для Подрядчика
1.6.9	Описание программного обеспечения			(поставщика, исполнителя) по передаче
1.6.10	Описание комплекса технических средств	в соответствии с Таблицей 1 п. 2.2 Приложения № 4 к Описанию объекта закупки.		отчетности в электронной форме.
1.6.11	Схема структурная комплекса технических средств	Пояснительная записка в разделе «Описание процесса деятельности» должна содержать описание процессов, автоматизируемых Системой. Для развиваемых и создаваемых функций и подсистем Системы автоматизируемые процессы описываются в виде схем в нотациях BPMN ²⁷ , UML. Должны быть приведены сценарии переноса данных и развертывания нового ОПО и СрЗИ, развертывание нового СПО и перехода на продуктивный контур в соответствии с требованиями Процессы 13 и п. 2.2 Приложения № 4 Описания объекта закупки, а		

²⁷ Схемы, составленные в нотации BPMN должны быть созданы с использованием инструментов для создания/редактирования BPMN-диаграмм и дополнительно предоставляются в формате BPMN 2.0 XML (файл с расширением. bpmn) в состоянии пригодном для дальнейшего редактирования с помощью инструментов для создания/редактирования BPMN-диаграмм.

1	2	3	4	5
		также; - процедуры для создания либо обезличивания тестовых данных для использования на предпродуктивном контуре, и необходимые скрипты для создания либо обезличивания тестовых данных; - процедуры и необходимые скрипты для перемещения лицензий между продуктивным и предпродуктивным контурами; - состав утилизируемых мощностей, процедуры и необходимые скрипты для их утилизации. В документе «Описание программного обеспечения» должно быть приведено описание фреймворков, библиотек, сервисов и т.д. В Пояснительной записке должно содержаться описание требований к АРМ Пользователей, подключающихся к Системе. Документ «Описание организации информационной базы» должен быть оформлен в соответствии с Методическими указаниями к оформлению документа «Описание организации информационной базы»²⁸. Документ «Описание систем		

²⁸ Методические указания опубликованы на сайте Санкт-Петербургского государственного казенного учреждения «Управление информационных технологий и связи» в сети Интернет, по адресу <https://uits.spb.ru/md/>

1	2	3	4	5
		классификации и кодирования» должен быть оформлен в соответствии с Методическими указаниями к оформлению документа «Описание систем классификации и кодирования» ²⁹ .		
1.6.12	План резервного копирования и восстановления	Разрабатывается в соответствии с Требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденными приказом ФСТЭК России, от 11.04.2025 № 117		
1.6.13	Технические требования к подключению автоматизированных рабочих мест пользователей государственной информационной Системы	Технические требования к подключению АРМ пользователей Системы разрабатываются в соответствии с проектными решениями по Системе, содержат требования к техническому, программному обеспечению и каналам связи, включая требования к средствам защиты информации.		
1.6.14	Ведомость покупных изделий ³⁰	ГОСТ Р 2.106-2019 Для ОПО наименование покупного изделия указывается в соответствии с наименованием		

²⁹ Методические указания опубликованы на сайте Санкт-Петербургского государственного казенного учреждения «Управление информационных технологий и связи» в сети Интернет, по адресу <https://uits.spb.ru/md/>

³⁰ Разрабатывается в случае выявления необходимости поставки технических и программных средств.

1	2	3	4	5
		данного изделия в Едином реестре российских программ для электронных вычислительных машин и баз данных или в Едином реестре программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации, с указанием реестрового номера, а также указывается иная необходимая дополнительная уточняющая информация. Для СрЗИ наименование покупного изделия указывается в соответствии с наименованием в государственном реестре средств защиты информации ФСТЭК России, а также указывается иная необходимая дополнительная уточняющая информация.		
1.7	Акт определения вида аттестационных испытаний	В соответствии с Приказом ФСТЭК России №77 от 29 апреля 2021 г; п. 5 Приложения № 6 к Описанию объекта закупки.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 1 этапу Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для

1	2	3	4	5
				Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2 этап «Рабочая документация и ввод в действие»				
Рабочая документация. Разработка (в том числе модификация) программных средств системы				
2.1	Комплект программной документации в составе:			
2.1.1	Спецификация ³¹	ГОСТ 19.202-78; ГОСТ 19.101-2024.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.1.2	Описание программы ³²	ГОСТ 19.402-78.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания	В форме электронного документа,

³¹ Разрабатывается на Систему.

³² Разрабатывается на Систему.

1	2	3	4	5
			выполнения работ по 2 этапу.	подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.1.3	Руководство программиста ³³ системного	Руководство системного программиста должно содержать инструкцию по развертыванию Системы (при использовании компилируемого языка программирования необходимо описать процессы сборки/компиляции исходных текстов). Документ содержит разделы: общие сведения о программе; структура программы; установка программы; настройка программы; проверка программы; аварийные ситуации. В разделе «Общие сведения о программе» указывают:	Подрядчик предоставляет: не позднее чем за 9 (девять) рабочих дней до дня начала выполнения работ по подготовке персонала. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в

³³ Разрабатывается актуализированная версия с учетом создаваемого, разрабатываемого (модифицированного) функционала на Систему.

1	2	3	4	5
		наименование программы (Системы); предназначение и цели создания Системы; сведения о технических и программных средствах, обеспечивающих выполнение данной программы. В разделе «Структура программы» указывают: состав и функциональную структуру Системы (подсистема, функция, комплекс задач, задача); программно-функциональную структуру Системы (подсистема, программный комплекс, программный компонент); сведения о связях с другими смежными системами. В разделе «Установка программы» указывают: требования к сетевому взаимодействию программы/программного компонента/программного комплекса через информационно-телекоммуникационную сеть «Интернет»; требования к аппаратным и/или виртуальным серверам при установке программы, с указанием по каждому серверу следующих сведений: имя сервера; назначение сервера; описание роли сервера;		электронной форме.

1	2	3	4	5
		ОС; основное ПО; число ядер vCPU; оперативная память RAM, Гб; дисковое пространство; настройки каждого сетевого интерфейса; адреса в защищенной корпоративной сети Единой мультисервисной телекоммуникационной сети исполнительных органов государственной власти Санкт-Петербурга; адреса в информационно-телекоммуникационной сети «Интернет». требования к общему программному обеспечению, необходимому для функционирования программы/программного компонента/программного комплекса; описание процесса установки программы/программного компонента/программного комплекса (при использовании компилируемого языка программирования необходимо указывать процесс сборки/компиляции исходных текстов). Обязательно указание наименований и версий (установленных и поддерживаемых) общего и		

1	2	3	4	5
		специального ПО, основных настроек, в случае если эти настройки отличаются от настроек «по умолчанию»). Указание списка расположения конфигурационных файлов и значений в них, включая конфигурационные файлы ОПО и СПО сторонних разработчиков, в случае если в них устанавливаются значения отличные от используемых «по умолчанию» и влияющих на Систему. В разделе «Настройка программы» указывают: описание процесса настройки программы/программного компонента/программного комплекса (по каждой программе/программному компоненту/программному комплексу); описание процесса резервного копирования данных и восстановления специального программного обеспечения; описание процесса обновления/замены сертификата ЭП уполномоченного лица и SSL-сертификата веб-приложения (при условии их наличия); описание процесса замены сертификатов (ключей) порталов (сайтов), используемых в Системе с указанием имен файлов,		

1	2	3	4	5
		их расположения, перечня всех элементов программно-функциональной структуры Системы, где указываются ЭП. В разделе «Проверка программы» указывают порядок проверки и тестирования программы/программного компонента/программного комплекса по результатам установки и настройки, восстановления работоспособности системы. требования к аппаратным и/или виртуальным средствам при установке программы/программного компонента/программного комплекса В разделе «Аварийные ситуации» указывают: перечень всех ошибок, возникающих в процессе эксплуатации Системы, включая сведения о кодах таких ошибок; описание каждой ошибки из вышеуказанного перечня, а также действий системного администратора по её устранению и восстановлению работоспособности Системы, включая сведения о местоположении соответствующего лог-файла; действия в других аварийных ситуациях.		

1	2	3	4	5
		Руководство должно описывать: работу с репозиториями исходного кода в инструментах CI/CD; формат хранения исходного кода и недопустимые форматы хранения; принцип декомпозиции сервисов, приложений и т.д. по репозиториям; структуру и форму репозитория исходного кода; описание скриптов с миграциями (конвертациями) для БД. Руководство должно включать в себя описание: методов обновления ОПО без модернизации СПО; инструкции по применению автоматических скриптов тестирования; сценариев тестирования либо процесса тестирования перед развертыванием и использованием СПО в обновленной среде; описание процесса создания баз данных и дальнейшей настройки СУБД, включая файлы настройки доступа. Руководство должно содержать информацию по управлению зависимостями и хранению артефактов проектов и дистрибутивов³⁴. Руководство должно содержать описание действий, а также		

³⁴ В соответствии с «Руководством для разработчиков программного обеспечения с целью адаптации развиваемого и создаваемого программного обеспечения для совместимости с автоматизированными инструментами CI/CD» передаваемым Заказчиком Подрядчику по запросу Подрядчика после заключения Контракта.

1	2	3	4	5
		параметров настроек и конфигурационных параметров Системы, необходимых для сборки, настройки, развертывания и дальнейшей эксплуатации и сопровождения в продуктивном контуре Системы. Руководство должно описывать процесс замены сертификатов (TLS / КристоПро), а также механизмы, помогающие отслеживать время их действия.		
2.1.4	Исходный текст (код) и дистрибутив программы на DVD M-DISC³⁵	Исходные коды должны предоставляться в открытом и немодифицированном виде, актуальными и работающими (при необходимости использования в работе специального программного обеспечения сторонних библиотек их необходимо также предоставлять), должны быть максимально закомментированными. Исходный текст (код) и дистрибутив программы предоставляются в составе единого архива, структура и состав которого определены в п. 13 Приложения № 6 Описания объекта закупки. Передача сопровождается файлом контрольной суммы и манифест-файлами, подписанными УКЭП.	Подрядчик представляет Заказчику не позднее чем за 1 (один) рабочий день до дня начала проведения предварительных комплексных испытаний. В случае если по результатам предварительных комплексных испытаний, опытной эксплуатации и приемочных испытаний Подрядчиком выполнялись доработки кода программы, исходный текст (код) и дистрибутив программы на CD/DVD повторно предоставляется Подрядчиком Заказчику не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	Предоставляется в электронном виде на отдельном CD/DVD в 1 экз., и размещается в Репозитории в разделе, соответствующем проекту (предоставление доступа к Репозиторию обеспечивается Заказчиком). Передача Заказчику оформляется актом (п. 10 Приложения № 6 к Описанию объекта закупки)

³⁵ Разрабатывается на создаваемые, разрабатываемые (модифицированные) части Системы.

1	2	3	4	5
		Исходные коды должны включать в себя все файлы, необходимые для сборки прикладного и специального программного обеспечения Системы, включая: - исходные тексты на используемых языках программирования; - файлы описания зависимостей (pom.xml, package.json, requirements.txt и т.п.); - конфигурационные файлы, относящиеся к сборке и развёртыванию; - скрипты миграции базы данных и наполнения справочников; - иные файлы, связанные с исходным кодом (например, лицензии); - манифест-файлы, описывающие состав и контрольные суммы всех перечисленных компонентов. Дистрибутив программы должен быть представлен на каждый программный компонент Системы. Формат исходного кода программы указан в п. 13 Приложения № 6 к Описанию объекта закупки. Исходные коды передаются на оптическом диске однократной записи. Для обеспечения долговременного архивного хранения запись рекомендуется производить на диски, поддерживающие технологию		

1	2	3	4	5
		M-Disc. Диск должен быть финализирован. На каждом диске и его конверте наносится маркировка: - наименование ГИС; - номер и дата контракта; - версия; - дата передачи.		
2.1.5.	Листинг кода базы данных	Должен быть предоставлен скрипт, в результате запуска которого формируется база данных со всеми элементами структуры базы данных (в том числе, таблицы, индексы, процедуры (пакеты), директории, роли, группы пользователей, и иные элементы), позволяющая провести установку системы на виртуальной инфраструктуре. Листинг базы данных предоставляется в соответствии со структурой, установленной п. 13 Приложения № 6 к Описанию объекта закупки.	Подрядчик представляет Заказчику не позднее чем за 1 (один) рабочий день до дня начала проведения предварительных комплексных испытаний. В случае если по результатам предварительных комплексных испытаний, опытной эксплуатации и приемочных испытаний Подрядчиком выполнялись доработки базы данных, листинг кода повторно предоставляется Подрядчиком Заказчику не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	Предоставляется в электронном виде на отдельном DVD M-DISC в 1 экз., а также размещается в Репозитории в разделе, соответствующем проекту (предоставление доступа к Репозиторию обеспечивается Заказчиком). Передача Заказчику оформляется актом (п. 10 Приложения № 6 к Описанию объекта закупки).
2.1.6	Отчет РБПО. Часть 2	В соответствии с п. 1.1.1 Приложения № 4 Описания объекта закупки Отчет должен содержать наборы артефактов требований процессов, как по базовым, так и по соответствующим им	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика,

1	2	3	4	5
		расширенным процессам, по пунктам: Процесс 3, Процесс 4, Процесс 6, Процесс 7, Процесс 9, Процесс 10, Процесс 11, Процесс 12, Процесс 16, Процесс 17, Процесс 18, Процесс 19 Приложения № 4 Описания объекта закупки.	со дня предоставления Подрядчиком.	документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.1.7	Информация о Системе	В соответствии с п. 14 Приложения № 6 Описания объекта закупки, актуализация.		
2.2	Комплект документации для государственной регистрации прав:			
2.2.1	Акт о принадлежности исключительных прав на результаты интеллектуальной деятельности	В соответствии с п.1 Приложения № 6 к Описанию объекта закупки.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика (субподрядчика при необходимости)
2.2.2	Проекты заявлений о государственной регистрации программ для ЭВМ и баз данных ³⁶	Раздел II Правил оформления заявки на государственную регистрацию программы для ЭВМ или базы данных, утвержденных приказом Минэкономразвития России от 05.04.2016 № 211 ³⁷ ;	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного

³⁶ Изготавливается на каждую программу для ЭВМ и базу данных, разработанную (модифицированную) в целях исполнения контракта.

³⁷ Приказ Минэкономразвития России от 05.04.2016 № 211 «Об утверждении Правил оформления заявки на государственную регистрацию программы для электронных вычислительных машин или базы данных, Правил составления документов, являющихся основанием для осуществления юридически значимых действий по государственной регистрации программы для электронных вычислительных машин или базы данных, и их форм, Порядка государственной регистрации программы для электронных вычислительных машин и базы данных, Перечня сведений о зарегистрированной программе для электронных вычислительных машин или базе данных,

1	2	3	4	5
		приложение № 1 к Правилам составления документов, являющихся основанием для осуществления юридически значимых действий по государственной регистрации программы для ЭВМ или базы данных, и их формам, утвержденных приказом Минэкономразвития от 05.04.2016 № 211.		лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на бумажном носителе в 1 (одном) экземпляре.
2.2.3	Депонируемые материалы, идентифицирующие программу для ЭВМ ³⁸	Раздел III Правил оформления заявки на государственную регистрацию программы для ЭВМ или базы данных, утвержденных	Подрядчик предоставляет Заказчику не позднее 1 (одного) рабочего дня после окончания выполнения работ	В форме электронного документа, подписанного

публикуемых в официальном бюллетене Федеральной службы по интеллектуальной собственности, Перечня сведений, указываемых в свидетельстве о государственной регистрации программы для электронных вычислительных машин или базы данных, формы свидетельства о государственной регистрации программы для электронных вычислительных машин, формы свидетельства о государственной регистрации базы данных» (далее – Приказ Минэкономразвития от 05.04.2016 № 211).

³⁸ Депонируемые материалы, идентифицирующие программу для ЭВМ, изготавливаются на каждую программу для ЭВМ, разработанную (модифицированную) в целях исполнения настоящего контракта. Представляются в форме исходного текста (полного или фрагментов) или иной форме присущей языку программирования, на котором написана программа для ЭВМ. Допускается включать в состав указанных депонируемых материалов подготовительные материалы, полученные в ходе разработки программы для ЭВМ, а также порождаемые ею аудиовизуальные отображения в любой визуально воспринимаемой форме.

1	2	3	4	5
		приказом Минэкономразвития от 05.04.2016 № 211.	по 2 этапу.	УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Материалы дополнительно предоставляются не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на каждую программу для ЭВМ на отдельном машиночитаемом носителе CD/DVD в формате PDF. Передача Заказчику оформляется актом (п. 10 Приложения № 6 к Описанию объекта закупки)

1	2	3	4	5
2.2.4	Депонируемые материалы, идентифицирующие базу данных ³⁹	Раздел III Правил оформления заявки на государственную регистрацию программы для ЭВМ или базы данных, утвержденных приказом Минэкономразвития от 05.04.2016 № 211.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Материалы дополнительно предоставляются не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на каждую базу данных на отдельном машиночитаемом

³⁹ Депонируемые материалы, идентифицирующие базу данных, изготавливаются на каждую базу данных, разработанную (модифицированную) в рамках исполнения контракта. Депонируемые материалы, идентифицирующие базу данных, должны отражать объективную форму представления совокупности содержащихся в ней самостоятельных материалов в виде примеров реального наполнения и принципы их систематизации (структуру базы данных), позволяющие осуществить нахождение и обработку этих материалов с помощью ЭВМ.

1	2	3	4	5
				носителе CD/DVD в формате PDF. Передача Заказчику оформляется актом (п. 10 Приложения № 6 к Описанию объекта закупки).
2.2.5	Реферат программы для ЭВМ, реферат базы данных ⁴⁰	Раздел III Правил оформления заявки на государственную регистрацию программы для ЭВМ или базы данных, утвержденных приказом Минэкономразвития от 05.04.2016 № 211.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП

⁴⁰ Изготавливаются на каждую программу для ЭВМ и базу данных, разработанную или модифицированную в целях исполнения контракта.

1	2	3	4	5
				на бумажном носителе в 1 (одном) экземпляре.
2.2.6	Согласие автора на указание сведений об авторе, указанных в заявлении ⁴¹	Приложение № 4 к Правилам составления документов, являющихся основанием для осуществления юридически значимых действий по государственной регистрации программы для ЭВМ или базы данных, и их формам, утвержденных Приказом Минэкономразвития от 05.04.2016 № 211.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на бумажном носителе в 1

⁴¹ Согласие автора на указание сведений об авторе, указанных в заявлении, оформляется на каждого автора каждой программы для ЭВМ и базы данных, разработанной (модифицированной) в целях исполнения контракта. Оформляется в случае указания автора в проекте заявления о государственной регистрации программы для ЭВМ и (или) базы данных.

1	2	3	4	5
				(одном) экземпляре с подписями субъекта персональных данных.
2.2.7	Согласие на обработку персональных данных ⁴²	В соответствии с п. 2 Приложения № 6 к Описанию объекта закупки.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП

⁴² Согласие на обработку персональных данных Санкт-Петербургским государственным казенным учреждением «Управление информационных технологий и связи» оформляется на каждого автора каждой программы для ЭВМ и базы данных, разработанной (модифицированной) в целях исполнения контракта. Оформляется в случае указания автора в проекте заявления о государственной регистрации программы для ЭВМ и (или) базы данных.

1	2	3	4	5
				на бумажном носителе в 1 (одном) экземпляре с подписями субъекта персональных данных.
2.2.8	Согласие на обработку персональных данных ⁴³	В соответствии с п. 3 Приложения № 6 к Описанию объекта закупки	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования

⁴³ Согласие авторов на обработку персональных данных Роспатентом оформляется на каждого автора каждой программы для ЭВМ и базы данных, разработанной (модифицированной) в целях исполнения контракта. Оформляется в случае указания автора в проекте заявления о государственной регистрации программы для ЭВМ и (или) базы данных.

1	2	3	4	5
				электронного документа в СФУП на бумажном носителе в 1 (одном) экземпляре с подписями субъекта персональных данных.
2.2.9.	Ходатайство о предоставлении льготы по уплате государственной пошлины ⁴⁴	В соответствии с п. 4 Приложения № 6 к Описанию объекта закупки.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования

⁴⁴ Изготавливаются на каждую программу для ЭВМ и базу данных, разработанную или модифицированную в целях исполнения контракта.

1	2	3	4	5
				электронного документа в СФУП на бумажном носителе в 1 (одном) экземпляре.
2.2.10	Справка о программах для ЭВМ/базах данных по результатам развития Системы	В соответствии с п. 8 Приложения № 6 к Описанию объекта закупки.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
Рабочая документация. Разработка рабочей документации на Систему				
2.3	Комплект рабочей документации на Систему в составе⁴⁵:			
2.3.1	Спецификация оборудования ⁴⁶	ГОСТ Р 59795-2021; ГОСТ 21.110-2013.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного

⁴⁵ Копии документов передаются Получателю в электронном виде на носителях CD/DVD в формате PDF.

⁴⁶ Разрабатывается на Систему, если требуется поставка технических средств.

1	2	3	4	5
			Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.3.2	Программа и методика предварительных комплексных испытаний ⁴⁷	ГОСТ Р 59795-2021; ГОСТ Р 59792-2021; Методика проведения испытаний СЗИ Системы, п. 9 Приложения № 6 к Описанию объекта закупки.	Подрядчик предоставляет: не позднее чем за 5 (пять) рабочих дней до дня начала предварительных комплексных испытаний. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика,

⁴⁷ Разрабатывается на развиваемые/создаваемые части Системы, включая подсистему «Система защиты информации» Системы, в объеме развиваемых/создаваемых задач и комплексов задач, а также на задачи и комплексы задач (в том числе не входящие в развиваемые, создаваемые части Системы), функционально взаимосвязанные с развиваемыми/создаваемыми задачами и комплексами задач.

По требованию Заказчика разрабатывается на не развиваемые части Системы, не развиваемые задачи, комплексы задач с учетом принятых и реализованных Подрядчиком технических решений.

1	2	3	4	5
				исполнителя) по передаче отчетности в электронной форме.
2.3.3	Разрешительная система доступа (матрица доступа)	В соответствии с п. 11 Приложения № 6 к Описанию объекта закупки.	Подрядчик предоставляет: не позднее чем за 5 (пять) рабочих дней до дня начала предварительных комплексных испытаний. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.3.4	Матрица коммуникаций	В соответствии с п. 12 Приложения № 6 к Описанию объекта закупки.	Подрядчик предоставляет: не позднее чем за 5 (пять) рабочих дней до дня начала предварительных комплексных испытаний. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим

1	2	3	4	5
				документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.3.5	Программа и методика опытной эксплуатации ⁴⁸	ГОСТ Р 59795-2021; ГОСТ Р 59792-2021.	Подрядчик предоставляет: не позднее чем за 5 (пять) рабочих дней до дня начала опытной эксплуатации. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.3.6	Программа и методика приемочных испытаний ⁴⁹	ГОСТ Р 59795-2021; ГОСТ Р 59792-2021;	Подрядчик предоставляет: не позднее чем за 5 (пять)	В форме электронного

⁴⁸ Разрабатывается на развиваемые/создаваемые части Системы, включая подсистему «Система защиты информации» Системы, в объеме развиваемых/создаваемых задач и комплексов задач, а также на задачи и комплексы задач (в том числе не входящие в развиваемые, создаваемые части Системы), функционально взаимосвязанные с развиваемыми/создаваемыми задачами и комплексами задач.

По требованию Заказчика разрабатывается на не развиваемые части Системы, не развиваемые задачи, комплексы задач с учетом принятых и реализованных Подрядчиком технических решений.

⁴⁹ Разрабатывается на развиваемые/создаваемые части Системы, включая подсистему «Система защиты информации» Системы, в объеме развиваемых/создаваемых задач и комплексов задач, а также на задачи и комплексы задач (в том числе не входящие в развиваемые, создаваемые части Системы), функционально взаимосвязанные с развиваемыми/создаваемыми задачами и комплексами задач.

1	2	3	4	5
		Методика проведения испытаний СЗИ Системы п. 9 Приложения № 6 к Описанию объекта закупки.	рабочих дней до дня начала приемочных испытаний. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней со дня предоставления Подрядчиком.	документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.4	Комплект эксплуатационной документации на Систему в составе:			
2.4.1	Ведомость эксплуатационных документов ⁵⁰	ГОСТ Р 59795-2021; ГОСТ 19.101-2024; ГОСТ 19.507-79; ГОСТ 34.201-2020; ГОСТ Р 2.601-2019; ГОСТ 2.102-2023.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим

По требованию Заказчика разрабатывается на не развиваемые части Системы, не развиваемые задачи, комплексы задач с учетом принятых и реализованных Подрядчиком технических решений.

⁵⁰ Разрабатывается на Систему.

1	2	3	4	5
				документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.4.2	Руководство пользователя ⁵¹	ГОСТ Р 59795-2021; Документ должен содержать: - описание выполнения операций (действий) Пользователей в технологическом процессе. Описание должно строиться на основе технологических задач Пользователей с использованием возможностей Системы и не должно сводиться к простому описанию (перечислению) функций Системы; - описание выполнения операций (действий) для всех категорий (ролей) Пользователей. При описании выполнения операций (действий) должны использоваться изображения экранных форм с комментариями, видеоматериалы (при необходимости, в экземпляре руководства на бумажном носителе приводятся ссылки на видеоматериалы). Руководство пользователя Системы должно быть	Подрядчик предоставляет: не позднее чем за 9 (девять) рабочих дней до дня начала выполнения работ по подготовке персонала. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.

⁵¹ Разрабатывается актуализированная версия руководства пользователя по ролям с учетом создаваемого, разрабатываемого (модифицированного) функционала.

1	2	3	4	5
		интерактивным, снабжено навигацией и доступно для загрузки из личного кабинета Пользователя Системы. Руководство пользователя Системы должно обеспечивать снижение нагрузки на первую линию технической поддержки Системы за счет ответов на наиболее часто возникающие вопросы Пользователей системы, удобства поиска необходимой информации внутри документа, выбора способа подачи информации, не затрудняющего ее восприятие.		
2.4.3	Руководство администратора безопасности Системы ⁵²	В соответствии с приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152; приказом ФСБ России от 09.02.2005 № 66; ГОСТ Р ИСО/МЭК ТО 18044-2007; п. 8 ГОСТ Р 59795-2021. Документ содержит разделы: введение; назначение и условия применения; подготовка к работе; описание операций; аварийные ситуации; рекомендации по освоению. В разделе «Введение» указывают:	Подрядчик предоставляет: не позднее чем за 9 (девять) рабочих дней до дня начала выполнения работ по подготовке персонала. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в

⁵² Разрабатывается на подсистему «Система защиты информации» Системы.

1	2	3	4	5
		область применения; краткое описание возможностей; уровень подготовки администратора безопасности; перечень эксплуатационной документации, с которыми необходимо ознакомиться администратору безопасности. В разделе «Назначение и условия применения» указывают: виды деятельности, функции, для автоматизации которых предназначено данное средство автоматизации; условия, при соблюдении (выполнении, наступлении) которых обеспечивается применение средства автоматизации в соответствии с назначением (например, вид ЭВМ и конфигурация технических средств, операционная среда и общесистемные программные средства, входная информация, носители данных, база данных, требования к подготовке специалистов и т. п.). В разделе «Подготовка к работе» указывают: состав и содержание дистрибутивного носителя данных; параметры и порядок настройки средств защиты информации; порядок загрузки данных		электронной форме.

1	2	3	4	5
		и программ; порядок проверки работоспособности. В разделе «Описание операций» указывают: перечень действий сотрудников при выполнении задач по эксплуатации подсистемы «Система защиты информации» Системы; описание всех выполняемых функций, задач, комплексов задач; описание операций технологического процесса обработки данных, необходимых для выполнения функций, комплексов задач (задач), процедур; перечень, виды, объемы и периодичность оказания услуг по обеспечению функционирования подсистемы «Система защиты информации» Системы; контроль работоспособности подсистемы «Система защиты информации» Системы и ее компонентов; перечень неисправностей, которые могут возникнуть в процессе эксплуатации подсистемы «Система защиты информации» Системы, и рекомендации в отношении действий при их возникновении; перечень режимов работы		

1	2	3	4	5
		подсистемы «Система защиты информации» Системы и их характеристики, а также порядок и правила перевода подсистемы «Система защиты информации» Системы с одного режима работы на другой с указанием необходимого для этого времени. Для каждой операции обработки данных указывают: - наименование; - условия, при соблюдении которых возможно выполнение операции; - подготовительные действия; - основные действия в требуемой последовательности; - заключительные действия, - ресурсы, расходуемые на операцию. В описании действий допускаются ссылки на файлы подсказок, размещенные на магнитных носителях. В разделе «Аварийные ситуации» указывают: - действия в случае несоблюдения условий выполнения технологического процесса, в том числе при длительных отказах технических средств; - действия по восстановлению программ и/или данных при отказе магнитных носителей или обнаружении ошибок в данных; - действия в случаях обнаружения		

1	2	3	4	5
		несанкционированного вмешательства в данные; действия в других аварийных ситуациях. В разделе «Рекомендации по освоению» указывают рекомендации по освоению и эксплуатации, включая описание контрольного примера, правила его запуска и выполнения.		
2.4.4	Описание базы данных ⁵³	ГОСТ Р 59795-2021; Составляется в соответствии с Методическими указаниями к оформлению документа «Описание базы данных» ⁵⁴	Подрядчик предоставляет: не позднее чем за 9 (девять) рабочих дней до дня начала выполнения работ по подготовке персонала. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.4.5.	Инструкция по формированию и ведению баз данных	Составляется в соответствии с Методическими указаниями к оформлению документа	Подрядчик предоставляет: не позднее чем за 9 (девять) рабочих дней до дня начала	В форме электронного документа,

⁵³ Разрабатывается на Систему.

⁵⁴ Методические указания опубликованы на сайте Санкт-Петербургского государственного казенного учреждения «Управление информационных технологий и связи» в сети Интернет, по адресу <https://uits.spb.ru/md/>

1	2	3	4	5
		«Инструкция по формированию и ведению баз данных» ⁵⁵	выполнения работ по подготовке персонала. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.4.6	Паспорт Системы ⁵⁶	ГОСТ Р 59795-2021.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по

⁵⁵ Методические указания опубликованы на сайте Санкт-Петербургского государственного казенного учреждения «Управление информационных технологий и связи» в сети Интернет, по адресу <https://uits.spb.ru/md/>

⁵⁶ Разрабатывается на Систему.

1	2	3	4	5
				передаче отчетности в электронной форме.
2.4.7	Технический паспорт Системы ⁵⁷	В соответствии с приказом ФСТЭК России от 29.04.2021 № 77.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу. Срок рассмотрения и утверждения Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.4.8	Общее описание Системы ⁵⁸	ГОСТ Р 59795-2021.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном

⁵⁷ Разрабатывается на Систему.

⁵⁸ Разрабатывается на Систему.

1	2	3	4	5
				Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.4.9	Информация о Системе	В соответствии с п. 14 Приложения № 6 к Описанию объекта закупки, предоставляется актуализированная информация.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
Ввод в действие. Подготовка объекта автоматизации к вводу в действие Системы				
2.5	План мероприятий по вводу Системы в действие (План-график работ)	Документ устанавливает перечень мероприятий, сроки выполнения, и исполнителей работ, связанных с вводом в действие Системы, и состав отчетной документации. Документ должен содержать: наименование мероприятий;	Подрядчик предоставляет не позднее 2 (двух) рабочих дней с начала выполнения работ по 2 этапу. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика,

1	2	3	4	5
		участника мероприятий; сроки проведения мероприятия; отчетную документацию.	со дня предоставления. В случае если в рамках исполнения настоящего государственного контракта сроки выполнения работ (отдельных мероприятий в рамках выполнения работ) были смещены ввиду выявленных нарушений, и/или по причине невозможности одного из участников мероприятия принять в нем участие, и/или иных причин, документ «План мероприятий по вводу Системы в действие (План-график работ)» повторно предоставляется Подрядчиком не позднее 2 (двух) рабочих дней с момента получения официального запроса со стороны Заказчика. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней со дня предоставления.	документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.6	Отчет о подготовленности объектов автоматизации к вводу в действие Системы⁵⁹	Содержит перечень объектов автоматизации, количественный и качественный анализ объектов автоматизации.	Подрядчик предоставляет: не позднее чем за 5 (пять) рабочих дней до дня начала предварительных комплексных испытаний. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ

⁵⁹ Разрабатывается на Систему.

1	2	3	4	5
			со дня предоставления Подрядчиком.	предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
Ввод в действие. Проведение предварительных комплексных испытаний Системы				
2.7	Протокол предварительных комплексных испытаний	ГОСТ Р 59795-2021; Подрядчик осуществляет видеозапись процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ в формате скринкаста, а именно видеозахвата экрана с параллельной записью голосовых комментариев. Видеозапись процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ передается Подрядчиком Заказчику по результатам проведения предварительных комплексных испытаний Системы. ⁶⁰	Подрядчик предоставляет: не позднее 2 (двух) рабочих дней после проведения предварительных комплексных испытаний Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно

⁶⁰ Предоставляется в электронном виде на носителях CD/DVD.

1	2	3	4	5
				предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на бумажном носителе в 3 (трех) ⁶¹ экземплярах с подписями уполномоченных лиц Подрядчика (Субподрядчика при наличии).
Ввод в действие. Подготовка персонала				
2.8	Документация по подготовке персонала:			
2.8.1	План подготовки персонала ⁶²	Включает пояснительную записку, тематический план и программу подготовки персонала с учетом их ролей, п. 15 Приложения № 6 к Описанию объекта закупки.	Подрядчик предоставляет: не позднее чем за 9 (девять) рабочих дней до дня начала выполнения работ по подготовке персонала. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика

⁶¹ В случае привлечения к выполнению работ организаций-субподрядчиков, количество экземпляров документа увеличивается на число данных организаций.

⁶² Копия документа направляется на электронный адрес Получателя и слушателей в форматах DOCX (DOC) и PDF/A. Указывается ссылка для скачивания руководства пользователя и иных рабочих материалов, указанных в контракте и необходимых для проведения подготовки персонала.

1	2	3	4	5
				(поставщика, исполнителя) по передаче отчетности в электронной форме.
2.8.2	Акт о завершении подготовки персонала	п. 16 Приложения № 6 к Описанию объекта закупки; журнал аудита (журнал событий системы видеоконференцсвязи); заключение о результатах завершённой подготовки.	Подрядчик предоставляет: не позднее 3 (трех) рабочих дней со дня окончания подготовки персонала. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней со дня предоставления.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
Ввод в действие. Проведение опытной эксплуатации и приемочных испытаний Системы				
2.9	Акт приемки в опытную эксплуатацию ⁶³	ГОСТ Р 59795-2021, Документ должен содержать: наименование Системы (или ее части), принимаемой в опытную эксплуатацию, и соответствующего объекта автоматизации; наименование документа,	Подрядчик предоставляет: не позднее чем за 5 (пять) рабочих дней до дня начала опытной эксплуатации. Срок рассмотрения и согласования Получателем не более 3 (трех) рабочих дней со дня предоставления	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ

⁶³ Разрабатывается на развиваемые/создаваемые части Системы.

1	2	3	4	5
		на основании которого разработана Система; список и подписи должностных лиц Заказчика и Получателя (Оператора, Обладателя информации), принимающих решение о принятии Системы в опытную эксплуатацию; период времени работы должностных лиц Заказчика и Получателя (Оператора, Обладателя информации); наименование Подрядчика, организации-субподрядчика, Заказчика и Получателя; состав функций Системы (или ее части), принимаемых в опытную эксплуатацию; перечень составляющих технического, программного, информационного и организационного обеспечений, проверяемых в процессе опытной эксплуатации; перечень документов, предъявляемых должностным лицам Заказчика и Получателя (Оператора, Обладателя информации); оценку соответствия принимаемой Системы Техническому заданию на ее создание; основные результаты приемки	Подрядчиком.	предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на бумажном носителе в 3 (трех)⁶⁴ экземплярах с подписями уполномоченных лиц Подрядчика (Субподрядчика при наличии).

⁶⁴ В случае привлечения к выполнению работ организаций-субподрядчиков, количество экземпляров документа увеличивается на число данных организаций.

1	2	3	4	5
		в опытную эксплуатацию; решение Заказчика и Получателя (Оператора, Обладателя информации) о принятии Системы в опытную эксплуатацию.		
2.10	Акт завершения опытной эксплуатации	ГОСТ Р 59795-2021, Документ должен содержать: наименование завершенной работы (работ); список представителей Заказчика, Подрядчика и организации- Получателя, принимающих участие в опытной эксплуатации; наименование документа (-ов), на основании которого (-ых) проводилась работа; основные результаты завершенной работы; заключение о результатах завершенной работы.	Подрядчик предоставляет не позднее 1 (одного) рабочего дня после завершения опытной эксплуатации Срок рассмотрения и согласования Получателем не более 2 (двух) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче ответственности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на бумажном носителе в 3 (трех) ⁶⁵

1	2	3	4	5
				экземплярах с подписями уполномоченных лиц Подрядчика (Субподрядчика при наличии)
2.11	Рабочий журнал опытной эксплуатации	ГОСТ Р 59792-2021.	Подрядчик предоставляет не позднее 1 (одного) рабочего дня после завершения опытной эксплуатации Срок рассмотрения и согласования Получателем не более 2 (двух) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика,

1	2	3	4	5
				исполнителя) по передаче отчетности в электронной форме.
2.12	Протокол испытаний приемочных	ГОСТ Р 59795-2021; Видеозапись процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ ^{66,67} .	Подрядчик предоставляет не позднее 1 (одного) рабочего дня после завершения приемочных испытаний Срок рассмотрения и согласования Получателем не более 2 (двух) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не

⁶⁶ Предоставляется в электронном виде на носителях CD/DVD.

⁶⁷ В случае если по результатам опытной эксплуатации Подрядчик выполнил доработку программного обеспечения Системы, в процессе проведения приемочных испытаний Системы Подрядчик должен провести повторную демонстрацию процесса компиляции, создания дистрибутива и установки (развертывания) разработанных программ для ЭВМ с использованием средств, указанных в пункте 3.15 Описания объекта закупки, а также в соответствии с инструкциями, приведенными в рабочей документации на Систему в тестовом контуре.

1	2	3	4	5
				позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на бумажном носителе в 3 (трех) ⁶⁸ экземплярах с подписями уполномоченных лиц Подрядчика (Субподрядчика при наличии).
2.13	Акт приемки в постоянную эксплуатацию ⁶⁹	ГОСТ Р 59795-2021, Документ должен содержать: наименование объекта автоматизации и Системы (или ее части), принимаемой в постоянную эксплуатацию; список и подписи должностных лиц Заказчика и Получателя, принимающих решение о принятии Системы в постоянную эксплуатацию; наименование Подрядчика, организации-субподрядчика,	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления Подрядчиком.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для

⁶⁸ В случае привлечения к выполнению работ организаций-субподрядчиков, количество экземпляров документа увеличивается на число данных организаций.

⁶⁹ Разрабатывается на Систему.

1	2	3	4	5
		Заказчика и Получателя; состав функций Системы (или ее части), принимаемой в постоянную эксплуатацию; перечень составляющих технического, программного, информационного и организационного обеспечений, принимаемых в постоянную эксплуатацию; перечень документов, предъявляемых должностным лицам Заказчика и Получателя; заключение о результатах опытной эксплуатации Системы; оценку соответствия принимаемой Системы Техническому заданию на ее создание; краткую характеристику и основные результаты выполненной работы по созданию Системы; решение Заказчика и Получателя. В приложении к акту приемки в постоянную эксплуатацию Подрядчик указывает исчерпывающий перечень мероприятий, необходимых для ввода Системы в постоянную эксплуатацию, в соответствии с		Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме. Документ дополнительно предоставляется не позднее 3 (трех) рабочих дней после дня согласования электронного документа в СФУП на бумажном носителе в 3 (трех) экземплярах с подписями уполномоченных лиц Подрядчика.

1	2	3	4	5
		подпунктами а-б пункта 14 «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 06.07.2015 № 676.		
2.14	Проект правового акта о вводе Системы в постоянную эксплуатацию ⁷⁰	Постановление Правительства Российской Федерации от 06.07.2015 № 676; постановление Правительства Санкт-Петербурга от 24.10.2016 № 928.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче

⁷⁰ Проект правового акта о вводе Системы в постоянную эксплуатацию должен быть выполнен на русском языке с учетом требований Типовой инструкции по делопроизводству в исполнительных органах государственной власти Санкт-Петербурга, утвержденной распоряжением Правительства Санкт-Петербурга от 30.07.2004 № 76-рп «Об организации делопроизводства в исполнительных органах государственной власти Санкт-Петербурга» и инструкции по делопроизводству Администрации Губернатора Санкт-Петербурга, утвержденной распоряжением Администрации Губернатора Санкт-Петербурга от 13.12.2007 № 89-ра «Об Инструкции по делопроизводству в Администрации Губернатора Санкт-Петербурга».

1	2	3	4	5
				отчетности в электронной форме.
2.15	Рекомендации по развитию Системы ⁷¹	Документ должен содержать следующие разделы: общие сведения; рекомендации к Системе в целом; рекомендации к функциям (задачам), выполняемым Системой; рекомендации к видам обеспечения. В разделе «Общие сведения» приводят: описание существующей информационной системы; направления развития; изменения нормативных правовых актов; предложения пользователей Системы во время подготовки пользователей, по результатам предварительных комплексных испытаний, опытной эксплуатации Системы, приемочных испытаний Системы; анализ соответствия предложений пользователей требованиям нормативных правовых актов. В разделе «Рекомендации к Системе в целом» приводят требования к общесистемным характеристикам и показателям. В разделе «Рекомендации к функциям (задачам),	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу. Срок рассмотрения и согласования Получателем не более 5 (пяти) рабочих дней со дня предоставления.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.

⁷¹ Разрабатывается на Систему.

1	2	3	4	5
		выполняемым Системой» приводят требования к функциональному развитию системы: требования к функциям, комплексам задач, задачам подсистемы. В разделе «Рекомендации к видам обеспечения» приводят требования к математическому, организационному, информационному, программному, техническому обеспечениям и иным видам обеспечения, обусловленные развитием Системы.		
2.16	Заполненный акт приемки данных о Системе для актуализации в Реестре ГИС	В виде документа в формате .pdf. Передача Подрядчику шаблона для заполнения обеспечивается Заказчиком на основании письменного запроса Подрядчика.	Подрядчик предоставляет: не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	В форме электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.
2.17	Отчет РБПО. Часть 3	В соответствии с п. 1.1.1	Подрядчик предоставляет:	В форме

1	2	3	4	5
		Приложения № 4 Описания объекта закупки должен содержать наборы артефактов требований процессов, как по базовым, так и по соответствующим им расширенным процессам, по пунктам: Процесс 20, Процесс 21, Процесс 22, Процесс 23, Процесс 24.	не позднее 1 (одного) рабочего дня после окончания выполнения работ по 2 этапу.	электронного документа, подписанного УКЭП уполномоченного лица Подрядчика, документ предоставляется в порядке, предусмотренном Методическим документом для Подрядчика (поставщика, исполнителя) по передаче отчетности в электронной форме.

Документы, предоставляемые Заказчику на бумажном носителе, прошиваются и подписываются Подрядчиком, в указанном количестве экземпляров.

Подрядчик предоставляет Заказчику отчетные документы, подготовленные с учетом мотивированных замечаний Заказчика (при наличии), в сроки, установленные требованиями к порядку и сроку предоставления отчетных документов настоящего приложения к Описанию объекта закупки.

В соответствии с требованиями постановления Правительства Санкт-Петербурга от 24.10.2016 № 928 «О мерах по реализации постановления Правительства Российской Федерации от 06.07.2015 № 676» комплект документов по каждому виду работ должен содержать на титульных листах отчетных документов гриф утверждения Комитета по информатизации и связи, за исключением отчетного документа «Проект правового акта о вводе Системы в постоянную эксплуатацию», титульный лист которого должен содержать гриф согласования Комитета по информатизации и связи в соответствии с положениями постановления Правительства Санкт-Петербурга от 24.10.2016 № 928 «О мерах по реализации постановления Правительства Российской Федерации от 06.07.2015 № 676».

В соответствии с приказом Федерального архивного агентства от 31.07.2023 № 77 «Об утверждении правил организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в государственных органах, органах местного самоуправления и организациях», в случае, если отчетный документ на бумажном носителе содержит более 250 листов, он должен быть разделен на тома.

Проекты заявлений о государственной регистрации программ для ЭВМ и баз данных, реферат программы для ЭВМ, реферат базы данных, согласие автора на указание сведений об авторе, указанных в заявлении, согласие на обработку персональных данных Санкт-Петербургским государственным казенным учреждением «Управление информационных технологий и связи», согласие на обработку персональных данных Роспатентом предоставляются Заказчику на бумажном носителе не прошитыми. Проекты заявлений о государственной регистрации программ для ЭВМ и баз данных, дополнения к заявлениям (в случае необходимости), представляемые на бумажном носителе, печатаются двусторонней печатью на одном листе.

Депонируемые материалы, идентифицирующие программы для ЭВМ или базы данных, разработанные (модифицированные) в целях исполнения настоящего контракта, представляются в электронной форме на машиночитаемых носителях в формате PDF/A. Если представленная на регистрацию база данных содержит аудиовидеоматериалы, то примеры таких материалов представляются в форматах MP3, AVI, MPEG-2, JPEG (JPG). Депонируемые материалы на каждую программу для ЭВМ или базу данных представляются на отдельном машиночитаемом носителе. Машиночитаемый носитель должен удовлетворять следующим требованиям:

не должен допускать последующую запись на него информации и должен позволять осуществлять многократное считывание записанной на нем информации;

должен иметь надпись на лицевой поверхности носителя, не влияющую на свойства чтения носителя, либо прикрепленный к упаковке носителя постоянным образом ярлык, где печатными буквами указываются наименование Заказчика (Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи»), название программы для ЭВМ или базы данных и дата, на которую произведена запись.

**РЕКОМЕНДУЕМЫЕ ФОРМЫ
отчетных документов**

1. Акт о принадлежности исключительных прав на результаты интеллектуальной деятельности

**АКТ
о принадлежности исключительных прав
на результаты интеллектуальной деятельности**

Санкт-Петербург

«__» _____ 20XX

Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи» (далее – СПб ГКУ «УИТС») в лице заместителя директора по цифровой трансформации <ФИО>, действующего на основании Устава и доверенности от _____ № ____ и <наименование организации подрядчика> (далее – <краткое наименование организации Подрядчика>) в лице <должность, ФИО представителя Подрядчика>, действующего на основании <наименование документа>, (далее – «Стороны») составили настоящий Акт о нижеследующем:

1. С даты подписания Сторонами настоящего Акта <наименование организации подрядчика>, являясь Подрядчиком по государственному контракту Санкт-Петербурга <номер, дата государственного контракта Санкт-Петербурга> на выполнение работ <наименование работ> (далее – государственный контракт Санкт-Петербурга), отказывается от претензий на исключительные права на результаты интеллектуальной деятельности, разработанные и (или) модифицированные в целях исполнения обязательств по государственному контракту Санкт-Петербурга, в составе следующих изобретений, полезных моделей, промышленных образцов, программ для электронных вычислительных машин, баз данных, топологий интегральных микросхем, а также исключительные права на результаты работ, включая объекты авторских прав и потенциально патентоспособные технические решения, секреты производства (ноу-хау) (далее – Объекты):

<перечень изобретений/полезных моделей/промышленных образцов/программ для электронных вычислительных машин/баз данных/топологий/интегральных микросхем/потенциально патентоспособных технических решений/секретов производства (ноу-хау)/иных результатов интеллектуальной деятельности>⁷².

2. Исключительные права на Объекты принадлежат субъекту Российской Федерации городу федерального значения Санкт-Петербургу, от имени которого выступает Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи».

СПб ГКУ «УИТС»

**<Наименование организации
Подрядчика>**

⁷² Указывается полный перечень созданных, модифицированных Объектов. При этом для каждого объекта в скобках указывается создан или модифицирован Объект. В случае модификации программного комплекса, указывается его полный состав с учетом немодифицированных программных комплексов/программных компонентов и делается соответствующая отметка «не модифицирован».

191144, Санкт-Петербург,
вн.тер.г. муниципальный округ Смольнинское, <Адрес>
ул. Новгородская, д. 20,
литера А, часть пом. 2-Н
ИНН 7842444610
КПП 784201001
ОГРН 1117847006617
ОКПО 69251796
л/с № 0710002
в Комитете финансов Санкт-Петербурга
ОКОПФ 75204
ОКТМО 40911000
ОКОГУ 2300280
тел. 8 (812) 576-2264
e-mail: uits@uits.spb.ru

ИНН
ОГРН
E-mail:
тел.
факс:

**Заместитель директора
по цифровой трансформации
СПб ГКУ «УИТС»**

**<Должность представителя
Подрядчика>**

_____ФИО

_____<ФИО>

2. Согласие на обработку персональных данных Санкт-Петербургским государственным казенным учреждением «Управление информационных технологий и связи»

В СПб ГКУ «УИТС»
ул. Новгородская, д. 20,
литера А, часть пом. 2-Н,
вн.тер.г. муниципальный округ
Смольнинское, Санкт-Петербург,
Российская Федерация

Согласие на обработку персональных данных

Ф. И. О. субъекта персональных данных

Иванов Иван Иванович

Адрес места жительства **111111, Российская Федерация, Санкт-Петербург, пр. Невский, д. 1, корп. 1, кв. 1**

Документ, удостоверяющий личность субъекта персональных данных, дата его выдачи и выдавший орган **паспорт серия 40 00 № 123456 выдан (заполняется в соответствии с данными, указанными в паспорте) 01.01.2006 (дата выдачи)**

в соответствии со ст. 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», даю согласие Санкт-Петербургскому государственному казенному учреждению «Управление информационных технологий и связи» на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных, а именно на сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение вышеуказанных персональных данных в целях государственной регистрации программ для электронных вычислительных машин и баз данных.

Подтверждаю согласие на обработку моих персональных данных.

Мне известно, что в случае отзыва согласия на обработку персональных данных Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи» вправе продолжить обработку персональных данных без моего согласия в соответствии с частью 2 статьи 9, пунктом 4 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Настоящее согласие действует со дня его подписания до дня отзыва в письменной форме.

Подпись

/ **И.И.Иванов** /
(Ф. И. О. субъекта персональных данных)

Дата

3. Согласие на обработку персональных данных Роспатентом

В Федеральную службу
по интеллектуальной собственности
Бережковская наб., д. 30, корп. 1,
г. Москва, Г-59, ГСП-3, 125993,
Российская Федерация

Название программы для ЭВМ или базы данных указать название программы
для ЭВМ/базы данных строго в соответствии с наименованием, указанным
в акте о принадлежности исключительного права и депонируемых материалах
№ заявки _____
(указывается при наличии регистрационного номера заявки)

Согласие на обработку персональных данных

Ф. И. О. субъекта персональных данных

Иванов Иван Иванович

Адрес места жительства 111111, Российская Федерация, Санкт-Петербург,
пр. Невский, д. 1, корп. 1, кв. 1

Документ, удостоверяющий личность субъекта персональных данных, дата его
выдачи и выдавший орган паспорт серия 40 00 № 123456 выдан (заполняется в
соответствии с данными, указанными в паспорте) 01.01.2006 (дата выдачи)

Подтверждаю согласие на обработку моих персональных данных, предусмотренную частью 3 статьи 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», в целях предоставления Федеральной службой по интеллектуальной собственности государственной услуги в соответствии с Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

Мне известно, что в случае отзыва согласия на обработку персональных данных Федеральная служба по интеллектуальной собственности вправе продолжить обработку персональных данных без моего согласия в соответствии с частью 2 статьи 9, пунктом 4 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Подпись

/ И.И.Иванов /
(Ф. И. О. субъекта персональных данных)

Дата

4. Ходатайство о предоставлении льготы по уплате государственной пошлины

Дата поступления <i>(заполняется Федеральной службой по интеллектуальной собственности)</i>	В Федеральную службу по интеллектуальной собственности Бережковская наб., д. 30, корп. 1, г. Москва, Г-59, ГСП-3, 125993, Российская Федерация
ХОДАТАЙСТВО о предоставлении льготы по уплате государственной пошлины	
Заявка № _____ на государственную регистрацию: ☐ Программы для ЭВМ ☐ Базы данных, государственная регистрация которой осуществляется в соответствии с пунктом 4 статьи 1259 Кодекса ☐ Базы данных, государственная регистрация которой осуществляется в соответствии с пунктом 3 статьи 1334 Кодекса <i>(отметить знаком «Х» вид результата интеллектуальной деятельности)</i> название: _____	
Правообладатель (и) (Заявитель)(и) <i>(указываются фамилия, имя, отчество (последнее – при наличии), место жительства физического лица, наименование, место нахождения, ОГРН и ИНН юридического лица)</i> Санкт-Петербург, от имени которого выступает Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи» (RU) Российская Федерация, Санкт-Петербург ОГРН: 1117847006617 ИНН: 7842444610	
Адрес для переписки: 191144, Санкт-Петербург, вн.тер.г. муниципальный округ Смольнинское, ул. Новгородская, д. 20, литера А, часть пом. 2-Н, Санкт-Петербургское государственное казенное учреждение «Управление информационных технологий и связи»	
Прошу предоставить мне льготу по уплате государственной пошлины в соответствии с подпунктом 4 пункта 1 статьи 333.35 Налогового кодекса Российской Федерации на основании следующих прилагаемых документов: выписка ЕГРЮЛ, Устав СПб ГКУ «УИТС»	
Приложение к настоящему ходатайству: на 23 л. в 1 экз.	
Заявителю известно, что с информацией о состоянии делопроизводства, в том числе о направленных заявителю документах, можно ознакомиться на сайтах Роспатента (www.rupto.ru) и ФИПС (www.fips.ru) в информационно-телекоммуникационной сети «Интернет»	
Подпись(и) правообладателя(ей), заявителя(ей), ходатайствующего(их) о предоставлении льготы Директор Санкт-Петербургского государственного казенного учреждения «Управление информационных технологий и связи» ФИО _____ « » 20 г. <i>(от имени юридического лица ходатайство подписывается руководителем организации или иным лицом, уполномоченным в установленном законодательством Российской Федерации порядке, с указанием должности, подпись удостоверяется печатью юридического лица при наличии печати. Подпись любого лица должна быть расшифрована путем указания фамилии и инициалов, и указана дата подписания ходатайства)</i>	

5. Акт определения вида аттестационных испытаний

УТВЕРЖДАЮ

СПБ ГКУ «УИТС»

УТВЕРЖДАЮ

Комитет по информатизации и
связи

«___» _____ 20XX г.

М.П.

«___» _____ 20XX г.

М.П.

*(Полное наименование государственной информационной системы)***АКТ ОПРЕДЕЛЕНИЯ ВИДА АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ**

Листов ____

СОГЛАСОВАНО

*(наименование организации, должность
представителя Обладателя информации,
подпись, расшифровка)*

«___» _____ 20XX г.

М.П.

СОГЛАСОВАНО

*(наименование _____ организации,
должность представителя Оператора,
подпись, расшифровка)*

«___» _____ 20XX г.

М.П.

АКТ

определения вида аттестационных испытаний

Санкт-Петербург

«__» ____ 20XX г.

1. (наименование организации подрядчика), являясь Подрядчиком по государственному контракту Санкт-Петербурга (номер, дата государственного контракта Санкт-Петербурга) на выполнение работ (наименование работ) установили, что при развитии (модернизации) Системы были изменены конфигурация (параметры настройки) программных, программно-технических средств и средств защиты информации, исключались или были заменены на аналогичные средства программные, программно-технические средства и средства защиты информации и (или) дополнительно были включены аналогичные средства.

В связи с этим сделан вывод о необходимости проведения дополнительных аттестационных испытаний в соответствии с «Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну», утвержденным приказом ФСТЭК России от 29.04.2021 № 77⁷³.

2. (наименование организации подрядчика), являясь Подрядчиком по государственному контракту Санкт-Петербурга (номер, дата государственного контракта Санкт-Петербурга) на выполнение работ (наименование работ) установили, что развитие (модернизация) Системы привела к повышению класса защищенности (уровня защищенности, категории значимости) Системы и (или) к изменению архитектуры системы защиты информации Системы в части изменения видов и типов программных, программно-технических средств и средств защиты информации, изменения структуры системы защиты информации, состава и мест расположения объекта информации и его компонентов.

В связи с этим сделан вывод о необходимости проведения повторной аттестации в соответствии с «Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну», утвержденным приказом ФСТЭК России от 29.04.2021 № 77⁷⁴.

<Наименование организации Подрядчика>

<Адрес>

ИНН

ОГРН

Тел.

Факс

E-mail:

<Должность представителя подрядчика>

<Дата> <ФИО>

М.П.

6. Анкета для предоставления доступа к Репозиторию

⁷³ Указывается в акте, в случае необходимости проведения дополнительных аттестационных испытаний Системы.

⁷⁴ Указывается в акте, в случае необходимости проведения повторной аттестации Системы (при этом приводится описание конкретных изменений Системы, обусловивших повышение класса защищенности (уровня защищенности, категории значимости) Системы).

АНКЕТА
для предоставления доступа к Репозиторию

1.	ФИО пользователя (полностью)	
2.	Наименование организации пользователя	
3.	Должность пользователя	
4.	Электронная почта пользователя	
5.	Контактный телефон пользователя	
6.	ФИО руководителя проекта со стороны Разработчика (полностью)	
7.	Контактный телефон руководителя проекта со стороны Разработчика	
8.	Номер и дата заключения государственного контракта	
9.	Срок завершения работ по государственному контракту	
10.	Полное наименование государственной информационной системы	
11.	Сокращенное наименование государственной информационной системы	
12.	Роль (developer, maintainer)	
	Наименование существующего проекта, или создать новый	
	Наименование существующей группы или создать новую	

7. Заявка на получение доступа к ресурсам РРЦОД



Информация об организации, направляющей заявку

**Директору Санкт-Петербургского
государственного казенного
учреждения «Управление
информационных технологий и
связи»**

№ _____

На № _____

от _____

Уважаемый (-ая) _____!

В связи с заключением контракта (указать номер и дату заключения контракта) на (указать предмет контракта) прошу Вас дать поручение актуализировать/предоставить/заблокировать доступы к (указать наименование ГИС) согласно приложениям.

Приложение: 1. Форма «Сведения об уполномоченных лицах по информационным системам» на 1 л. в 1 экз.
2. Форма «Список Администраторов контуров информационной системы с доступом к консоли управления виртуализацией РРЦОД» на 1 л. в 1 экз.
3. Форма «Сведения об администраторах серверов ИС и администрируемых системах» (образец для заполнения) на 2 л. в 1 экз.
4. Аттестат соответствия требованиям о защите информации на 1 л. в 1 экз.

**Должность руководителя
организации**

Место для подписи

**ФИО руководителя
организации**

1. Сведения об Уполномоченных лицах по информационным системам

Полное наименование информационной системы*					
Краткое наименование информационной системы*					
№ п/п	ФИО*	Электронная почта*	Телефон*	Наименование организации*	Должность*
1	2	3	4	5	6
1					

* – поля, обязательные к заполнению

2. Список Администраторов контуров информационной системы с доступом к консоли управления виртуализацией РРЦОД

Полное наименование информационной системы*						
Краткое наименование информационной системы*						
№ п/п	Имя локального домена контура информационной системы**	ФИО*	Служебная электронная почта*	Служебный номер телефона*	Наименование организации*	Должность*
1	2	3	4	5	6	7
1						

* – поля, обязательные к заполнению

** – Если не указан – доступ предоставляется ко всем контурам ИС

3. Сведения об администраторах серверов ИС и администрируемых системах

Полное наименование информационной системы		Государственная Информационная система*			
Краткое наименование информационной системы		ГИС*			
	Сведения о серверах				
№ п/п	Имя сервера*	Описание сервера	IP-адрес в РРЦОД*	IP-адрес в ЗКС	Протокол доступа* (выбрать из RDP/SSH/VNC)**
1	2	3	4	5	6
1	app1.gis.adc.spb	сервер приложений	192.168.2.2	10.144.144.144	SSH

* – поля, обязательные к заполнению

** – в данном поле следует конкретно определить к какому из указанных протоколов будет осуществляться взаимодействие

4. Декларация о соответствии требованиям о защите информации

(Указать наименование организации) (краткое наименование - _____) в лице _____ действующего на основании _____ принимает необходимые организационные и технические меры по защите информации, обрабатываемой на автоматизированных рабочих местах (далее – АРМ) пользователей информационных систем, соответствующие требованиям приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» применительно к персональным данным при их обработке в информационной системе персональных данных, приказа ФСТЭК России от 11.04.2025 № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий», применительно к требованиям инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 №152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», а также Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

На АРМ пользователя информационными ресурсами укажите информационную систему установлены и настроены следующие сертифицированные по требованиям безопасности информации средства защиты информации:

№ п/п	Тип средства защиты информации	Наименование средства защиты информации	Производитель средства защиты информации	Сертификат соответствия
1	2	3	4	5

Должность

ФИО

(подпись)

8. Справка о программах для ЭВМ/базах данных по результатам создания/развития Системы

СПРАВКА о программах для ЭВМ/базах данных по результатам создания/развития Системы

Таблица 1

№ п/п	Созданная/модифицированная программа для ЭВМ, база данных			Исходная программа для ЭВМ, база данных	
	Наименование программного комплекса, программного компонента, базы данных ⁷⁵ (с указанием версииности)*	Действие (создание/модификация)	Количество строк исходного кода	Наименование программного комплекса, программного компонента, базы данных ⁷⁶ (с указанием версииности)	Количество строк исходного кода
1	2	3	4	5	6
1					
2					
3					
...					

Таблица 2

№ п/п	Созданная/модифицированная база данных						Исходная база данных					
	Наименование базы данных ⁷⁷ (с указанием версииности)*	Действие (создание/модификация)	Количество таблиц в базе данных	Количество атрибутов в таблице базы данных	Количество полей в таблице базы данных	Количество связей базы данных с другими объектами Системы	Наименование базы данных ⁷⁸ (с указанием версииности)	Действие (создание/модификация)	Количество таблиц в базе данных	Количество атрибутов в таблице базы данных	Количество полей в таблице базы данных	Количество связей базы данных с другими объектами Системы
1	2	3	4	5	6	7	8	9	10	11	12	13
1												
2												
3												
...												

*Наименование программного комплекса, программного компонента, базы данных (далее – Объект) необходимо строить по следующему принципу: вид Объекта «Сокращенное наименование Системы. Наименование Объекта. вер. год». Данное требование необходимо учитывать, в том числе и при разработке технических решений по Системе и подготовке документации Технического проекта.

⁷⁵ Для нереляционных баз данных

⁷⁶ Для нереляционных баз данных

⁷⁷ Для реляционных баз данных

9. Методика проведения испытаний СЗИ Системы

Краткая характеристика испытаний.

Вид испытаний: <предварительные комплексные испытания> <приемочные>

Условия проведения испытаний: <на тестовом контуре Подрядчика/Заказчика> <на тестовом контуре РРЦОД> <на промышленном контуре>
<иное>

2. Перечень и комплектность объектов испытаний.

Проверка осуществляется путем сверки состава и характеристик объектов испытаний (далее ОИ) с данными, приведенными в Таблице1.

Таблица 1. Объекты испытаний.

№ п/п	Тип и наименование ¹	Местоположение	Наименование компонента	Тип компонента (средство/настройка/функция/параметр)	Сертификат, только для средства (реестровый номер и срок окончания)	Лицензия, только на средство (номер лицензии и срок окончания действия)	Примечание
1							
2							

3. Перечень функций, подлежащих проверке и критерии приемки.

Перечень функций, подлежащих проверке и критерии приемки ОИ соответствуют мерам защиты, определенных в техническом задании на <создание>/<развитие>, модели угроз, дополнению к техническому заданию и техническому проекту на Систему.

4. Материально-техническое обеспечение испытаний подсистемы СЗИ.

Состав, наименование, назначение, характеристики, способы размещения и способы взаимодействия технических средств приведены в разделе «Материально-техническое обеспечение испытаний».

¹ Указывается тип и наименование объекта испытаний, например, Виртуальный сервер AWZ-01, Сервер WM-45775, Информационный обмен с ГИС ЕССК. Наименование должно обеспечивать однозначную идентификацию ОИ (Имя, доменное имя, IP адрес, алиас). Допускается группировка ОИ по признаку общности состава компонентов ОИ при условии идентичности иных характеристик ОИ. Под ОИ принимается объект или часть объекта защиты Системы, содержащий компоненты в виде одного или нескольких средств защиты информации, настроек для работы с иными средствами защиты информации, функциями защиты информации или параметров Системы. На этапах ПКИ и ПИ указываются ОИ, предъявляемые к испытаниям. При проведении проверок после развертывания Системы указываются все ОИ Системы.

⁷⁸ Для реляционных баз данных

5. Порядок, методики и условия проведения контрольных проверок. Перечень контрольных заданий по проверке компонентов ОИ⁷⁹ и порядок проведения проверок приведен в последующих разделах.

6. Контрольные задания

6.1. Контрольные задания ОИ⁸⁰: <наименование ОИ >

Таблица 2. Перечень контрольных заданий.

№ п/п	Наименование компонента ОИ	Мера защиты/требование				Номер контрольного задания ⁸¹	Наименование контрольного задания
		№ 117 ФСТЭК ⁸²	№ 21 ФСТЭК ⁸³	№ 239 ФСТЭК ⁸⁴	ТЗ (пункт/мера СПО) ⁸⁵		
1							

6.1.1 Контрольное задание № <номер контрольного задания> <наименование контрольного задания> для компонента: <наименование компонента ОИ>

⁷⁹ Указывается тип и наименование объекта испытаний, например, Виртуальный сервер AWZ-01, Сервер WM-45775, Информационный обмен с ГИС ЕССК. Наименование должно обеспечивать однозначную идентификацию ОИ (Имя, доменное имя, IP адрес, алиас). Допускается группировка ОИ по признаку общности состава компонентов ОИ при условии идентичности иных характеристик ОИ. Под ОИ принимается объект или часть объекта защиты Системы, содержащий компоненты в виде одного или нескольких средств защиты информации, настроек для работы с иными средствами защиты информации, функциями защиты информации или параметров Системы. На этапах ПКИ и ПИ указываются ОИ, предъявляемые к испытаниям. При проведении проверок после развертывания Системы указываются все ОИ Системы.

⁸⁰ Указывается наименование компонента ОИ, в качестве компонента рассматриваются: средства защиты информации, настройки для работы с иным средством защиты информации, функции защиты информации, параметры Системы. В случае наличия у компонента версии указание версии обязательно.

⁸¹ В случае наличия у компонента сертификата указывается сертификат ФСТЭК России или ФСБ РФ для СрЗИ, входящих в объект испытаний (номер сертификата из Реестра, срок окончания действия сертификата).

⁸² В случае наличия у компонента лицензии указывается номер лицензии и срок окончания действия на СрЗИ, входящее в ОИ. В случае использования временной лицензии указывается «Лицензия временная»

⁸³ Контрольные задания по проверке формируются для всех мер защиты модели угроз, технического задания, дополнения к техническому заданию или технического проекта на Систему.

⁸⁴ На этапе ПКИ и ПИ допускается указать контрольные проверки, непосредственно относящиеся к данным этапам испытаний. При проведении проверок после развертывания Системы указываются все контрольные проверки всех ОИ Системы.

⁸⁵ Нумерация контрольных заданий производится в рамках ОИ.

Последовательность действий для выполнения контрольного задания приведены в таблице 3. Критерием успешности выполнения задания является соответствие результата выполняемого действия его ожидаемому результату.

Таблица 3. Проверка меры защиты.⁸⁶

№ п/п	Требование	Действие	Ожидаемый результат
1			
2			

6.1.2 Контрольное задание № *<номер контрольного задания>* *<наименование контрольного задания>* для компонента: *<наименование компонента ОИ>*

.....

6.2. Контрольные задания ОИ: *<наименование ОИ>*

.....

⁸⁶ Указывается условное обозначение, номер меры защиты информации в информационных системах в соответствии с приказом № 117 ФСТЭК России.

Лист регистрации изменений

[illegible]

10. Акт приема-передачи отчетных материалов (документов, информации)

АКТ

Приема-передачи отчетных материалов (документов, информации) на электронном носителе/на бумажном носителе

Санкт-Петербург
20XX г.

«__» _____

Мы, нижеподписавшиеся, представитель Государственного заказчика и представитель Подрядчика, составили настоящий акт о том, что представитель Подрядчика передает, а представитель Государственного заказчика принимает следующие материалы, подготовленные в рамках ____ этапа работ по государственному контракту Санкт-Петербурга № _____ от _____ на выполнение работ по созданию (развитию) государственной информационной системы Санкт-Петербурга

1. Перечень документов (информации) на электронных носителях

№ п/п	Наименование отчетного документа	Кол-во экземпляров	Тип электронного носителя	Дата получения документа в	Примечание
№ этапа					

2. Перечень документов (информации) на бумажных носителях

№ п/п	Наименование отчетного документа	Кол-во томов	Кол-во листов в 1 томе	Прошивка документа	Дата получения документов	Примечание
№ этапа						

Материалы передал:
Представитель Подрядчика

Наименование подрядчика

Должность представителя

Материалы принял
Представитель Государственного заказчика
СПб ГКУ УИТС

Наименование заказчика

Должность представителя

Подпись

ФИО

Подпись

ФИО

11. Разрешительная система доступа (матрица доступа)

УТВЕРЖДАЮ

<Ответственное лицо
со стороны Комитета
по информатизации и связи>

_____ <Ф.И.О.>

МП

«___» _____ 202__ г.

УТВЕРЖДАЮ

СПб ГКУ «УИТС»

_____/_____

УТВЕРЖДАЮ

<Ответственное лицо
со стороны СПб ГКУ «СПб ИАЦ»>

_____ <Ф.И.О.>

МП

«___» _____ 202__ г.

<ПОЛНОЕ НАИМЕНОВАНИЕ ГИС>

**РАЗРЕШИТЕЛЬНАЯ СИСТЕМА ДОСТУПА
(МАТРИЦА ДОСТУПА)**

На ____ листах

СОГЛАСОВАНО

<Ответственное лицо

со стороны Получателя⁸⁷>

_____ <Ф.И.О.>,
МП

«_____» _____ 202__ г.

Санкт-Петербург ГГГГ

⁸⁷ Указывается условное обозначение, номер меры защиты информации в информационных системах в соответствии с приказом № 21 ФСТЭК России.

1. Общие сведения

Разрешительная система доступа (далее – Матрица доступа) представляет собой разрешительную неперсонифицированную систему управления доступом к государственной информационной системе (**наименование системы**) (далее – Система). Матрица доступа является эксплуатационным документом, на основании которого **Получатель (Оператор)** Системы формирует и утверждает персонифицированную матрицу доступа в составе организационно-распорядительной документации Системы.

В Матрице доступа определен перечень групп внешних пользователей Системы, внутренних привилегированных и внутренних непривилегированных пользователей Системы (далее – Субъекты доступа), которым предоставлен доступ к информационным ресурсам Системы (далее – Объекты защиты), уровней их полномочий и типов доступа.

Доступ любых субъектов доступа, не указанных в Матрице доступа, к Объектам защиты категорически запрещен. Запрет доступа реализуется с использованием организационных и технических мер защиты информации Системы.

2. Уровни доступа

Для Субъектов доступа устанавливаются уровни доступа⁸⁸, перечень и условные обозначения которых приведены в таблице

Таблица 1 – Уровни доступа

№ п/п	Условное обозначение	Описание прав доступа
1	2	3
	Неизменяемые уровни доступа	
1.	ПД	Полный доступ
2.	ЧЗ	Чтение и запись
3.	Ч	Доступ на чтение
4.	Ч(Г)	Доступ на чтение только конкретной группы/групп субъектов доступа
5.	Ч(С)	Доступ на чтение только конкретного субъекта/субъектов доступа
6.	У	Доступ на удаление
7.	В	Доступ на выполнение

⁸⁸ Указывается условное обозначение, номер меры защиты информации в информационных системах в соответствии с приказом № 239 ФСТЭК России для государственных информационных систем ЗОКИИ.

8.	3	Запрет на любой доступ
9.	—	Не определены права доступа, эквивалентен запрету
Дополнительные уровни доступа		
10.	ПД (СУБД №1)	Полный доступ к СУБД №1
11.	ЧЗ (Документы СПО)	Чтение и запись всех дочерних документов, хранимых в СПО

3. Объекты защиты Системы

Перечень Объектов защиты⁸⁹, определенных в (пункт и наименование документа *технического проекта, в котором определены объекты защиты*), приведен в Таблице Error: Reference source not found.

Таблица 2 – Перечень объектов защиты
Защищаемый ресурс

№ п/п	Размещение/ обозначение объекта защиты ⁹⁰	Защищаемый ресурс
1	2	3
1.	Информация, содержащаяся в информационной системе	- открытая информация, предоставляемая зарегистрированными пользователями; - персональные данные; - данные, используемые для аутентификации пользователей; - маркеры доступа; - парольная информация
2.	Технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации)	- данные, используемые для аутентификации пользователей, маркеры доступа, парольная информация; - данные файлов журналов регистрации событий; - данные конфигурации технических средств
3.	Общесистемное программное обеспечение	- данные, используемые для аутентификации пользователей; - маркеры доступа; - парольная информация; - данные файлов журналов регистрации событий;

⁸⁹ Указывается условное обозначение, номер меры защиты информации при разработке СПО (в соответствии с Таблицей №1 Приложения №2 к Описанию объекта закупки) либо пункт ТЗ, содержащий требование.

⁹⁰ Допускается вместо табличного использовать текстовый вид представления информации.

1	2	3
		- данные конфигурации программных средств;
4.	Прикладное программное обеспечение	- данные, используемые для аутентификации пользователей; - маркеры доступа; - парольная информация; - данные файлов журналов регистрации событий; - данные конфигурации программных средств;
5.	Специальное программное обеспечение	- данные, используемые для аутентификации пользователей; - маркеры доступа; - парольная информация; - данные файлов журналов регистрации событий; - данные конфигурации программных средств;
6.	Информационные технологии	- данные файлов журналов регистрации событий; - данные конфигурации программно-аппаратных средств;
7.	Криптографические средства защиты информации	- ключевая информация; - данные файлов журналов регистрации событий; - рабочая документация СКЗИ; - данные конфигурации программно-аппаратных средств, включая СКЗИ
8.	Средства защиты информации	- общедоступная информация; - открытая информация, предоставляемая зарегистрированным пользователям; - данные, используемые для аутентификации пользователей, маркеры доступа, парольная информация; - данные файлов журналов регистрации событий; - данные конфигурации программно-аппаратных средств

Группы и роли пользователей⁹¹ (Субъектов доступа), определенных в *(пункт и наименование документа технического проекта, в котором определены роли субъектов доступа)*, приведены в Error: Reference source not found.

Таблица 3. Группы и роли субъектов доступа

№ п/п	Тип и вид группы субъектов	Наименование группы субъектов в Системе	Определение группы в Системе	Роли в Системе	Основные обязанности
1	2	3	4	5	6
1.	Внутренние привилегированные	Администраторы информационной безопасности	Группа лиц, уполномоченных выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты информации системы	- администратор СрЗИ от несанкционированного доступа; - администратор СКЗИ; - администратор баз данных - аудитор информационной безопасности; - администратор журнала сообщений ПДн - администратор	

⁹¹ Указывается требование или мера защиты.

№ п/п	Тип и вид группы субъектов	Наименование группы субъектов в Системе	Определение группы в Системе	Роли в Системе	Основные обязанности
1	2	3	4	5	6
				мониторинга журнала сообщений ПДн - администратор журнала безопасности ПДн - администратор мониторинга журнала безопасности ПДн администратор интеграций ЦОУ ИБ АПК БГ	
2.	Внутренние привилегиров анные	Администраторы информационной системы	Группа лиц, уполномоченных выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) информационной системы	- администратор прикладных сервисов; - системный администратор; администратор баз данных.	
3.	Внутренние привилегиров анные	Операторы информационной системы	Группа лиц, обеспечивающие проведение контрольной и уполномоченные ими лица надзорной деятельности (проводят эксплуатацию штатного функционирования Системы, не участвуют в процессах настройки прикладного ПО и настройки бизнес- процессов)	- координатор (организует, контролирует, оценивает степень внедрения Системы); - администратор (осуществляет настройку личных кабинетов и добавляет пользователей в систему в рамках конкретного органа власти и организации); - помощник руководителя (работает с документами, административными делами); - руководитель (формирует отчеты, работает с документами, административными делами); - исполнитель (осуществляет рассмотрение поступивших запросов на предоставление	

№ п/п	Тип и вид группы субъектов	Наименование группы субъектов в Системе	Определение группы в Системе	Роли в Системе	Основные обязанности
1	2	3	4	5	6
				государственных(муниципальных) услуг); - инспектор (рассматривает поступившие сведения, которые могут являться основанием для проведения контрольных (надзорных) и иных мероприятий, ведение дел об административных правонарушениях); - методолог (выполняет конструирование процессов предоставления государственных (муниципальных) услуг и (или) исполнения функций); - проектировщик сервиса (выполняет надстройки для стандартов предметной области, которые определяют структуру, а также состав, вид и тип используемых полей в стандартах предметной области на различных вкладках). Формирует структуры и отображение заявления, расположение и наименование вкладок в нем, задается статусная модель заявления; - юридическое лицо (осуществляет рассмотрение поступивших запросов на предоставление государственных(муниципальных) услуг и функций) в соответствии с	

№ п/п	Тип и вид группы субъектов	Наименование группы субъектов в Системе	Определение группы в Системе	Роли в Системе	Основные обязанности
1	2	3	4	5	6
				функциональными требованиями к Системе.	
4.	Внутренние непривилегир ованные пользователи	Операторы технической поддержки	Обеспечение мониторинга заявок о нештатных ситуациях (проблемах) и их дальнейшую маршрутизацию на привилегированных пользователей ГИС: Специалисты (инженеры) технической поддержки ГИС		
5.	Внутренние привилегиров анные пользователи	Системные пользователи	Обеспечение взаимодействия частей Системы: - взаимодействия приложений с СУБД; - взаимодействия с СрЗИ; - взаимодействия с внешними СрЗИ		
6.	Внешние привилегиров анные	Системные пользователи	Обеспечение взаимодействия с внешними информационными Системами: - взаимодействи я Системы с внешней СУБД; - взаимодействи я с внешними информационными системами		
7.	Внешние непривилегир ованные	Внешние пользователи	Обеспечение работы	аутентифицированный пользователь	

Перечень полномочий (ролей) пользователей⁹² по отношению к соответствующим объектам защиты, определенных в *(пункт и наименование документа технического проекта, в котором определены роли субъектов доступа)*, приведен в Error: Reference source not found.

⁹² Указывается необходимое действие, достаточное для проверки требования технического задания.

№ п/п	Объекты защиты	Информация	Технические средства	Общее ПО	Прикладное ПО	СПО	Информационные технологии	СКЗИ	СрЗИ
1	2	3	4	5	6	7	8	9	10
1.	Администраторы информационной безопасности								
1.1.	Администратор СрЗИ от несанкционированного доступа	-	-	-	-	-	-	-	ПД
1.2.	Администратор СКЗИ	-	-	-	-	-	-	ПД	-
1.3.	Администратор баз данных	-	-	-	ПД	-	-	-	ПД
1.4.	Аудитор информационной безопасности	Ч	Ч	-	-	Ч	Ч	Ч	Ч
1.5.	Администратор журнала сообщений ПДн	Ч	-	-	-	ПД	-	-	-
1.6.	Администратор мониторинга журнала сообщений ПДн	-	-	-	-	Ч	-	-	-
1.7.	Администратор журнала безопасности ПДн	Ч	-	-	-	ПД	-	-	-
1.8.	Администратор мониторинга журнала безопасности ПДн	Ч	-	-	-	Ч	-	-	-
1.9.	Администратор интеграций ЦОУ ИБ АПК БГ	-	-	ПД	ПД	-	-	ПД	-
2.	Администраторы информационной системы								
2.1.	Администратор прикладных сервисов	-	-	-	-	ПД	-	-	-
2.2.	Системный администратор	-	ПД	ПД	ПД	ПД	ПД	Ч	Ч
2.3.	Администратор баз данных	-	-	Ч	ПД	-	-	-	-
3.	Операторы информационной системы								
3.1.	Координатор (организует, контролирует, оценивает степень внедрения Системы)	-	-	-	-	-	-	-	-
3.2.	Администратор (осуществляет настройку личных кабинетов и добавляет пользователей в систему в рамках конкретного органа власти и организации)	-	-	-	-	-	-	-	-
3.3.	Помощник руководителя (работает с документами, административными делами)	-	-	-	-	-	-	-	-
3.4.	Руководитель (формирует отчеты, работает с документами, административными делами)	-	Ч	-	-	-	-	-	-
3.5.	Исполнитель (осуществляет рассмотрение поступивших запросов)	-	-	-	-	-	-	-	-

	на предоставление государственных(муниципальных) услуг)								
3.6.	Инспектор (рассматривает поступившие сведения, которые могут являться основанием для проведения контрольных (надзорных) и иных мероприятий, ведение дел об административных правонарушениях)	-	-	-	-	-	-	-	-
3.7.	Методолог (выполняет конструирование процессов предоставления государственных (муниципальных) услуг и (или) исполнения функций)	-	Ч	-	-	-	-	-	-
3.8.	Проектировщик сервиса (выполняет надстройки для стандартов предметной области, которые определяют структуру, а также состав, вид и тип используемых полей в стандартах предметной области на различных вкладках). Формирует структуры и отображение заявления, расположение и наименование вкладок в нем, задается статусная модель заявления	-	-	-	-	-	-	-	-
3.9.	Юридическое лицо (осуществляет рассмотрение поступивших запросов на предоставление государственных(муниципальных) услуг и функций) в соответствии с функциональными требованиями к Системе	-	-	-	-	-	-	-	-
4.	Операторы технической поддержки	-	-	-	-	-	-	-	-
4.1.	Специалисты (инженеры) технической поддержки ГИС	-	-	-	-	-	-	-	-
5.	Системные пользователи	-	-	-	-	-	-	-	-
5.1.	Пользователь СУБД №1	-	-	-	-	-	-	-	-
5.2.	Пользователь СрЗИ №1	-	-	-	-	-	-	-	-
5.3.	Пользователь внешнего СрЗИ №1	-	-	-	-	-	-	-	-
5.4.	Пользователь внешней СУБД №1	-	-	-	-	-	-	-	-
5.5.	Пользователь внешней информационной системы №1	-	-	-	-	-	-	-	-
6.	Внешние пользователи	-	-	-	-	-	-	-	-
6.1.	Анонимный пользователь	-	-	-	-	-	-	-	-
6.2.	Аутентифицированный пользователь	-	-	-	-	-	-	-	-

12. Матрица коммуникаций

УТВЕРЖДАЮ

<Ответственное лицо
со стороны Комитета
по информатизации и связи>

_____ <Ф.И.О.>

МП

«___» _____ 202__ г.

УТВЕРЖДАЮ
СПб ГКУ «УИТС»

_____/_____

УТВЕРЖДАЮ

<Ответственное лицо
со стороны СПб ГКУ «СПб ИАЦ»>

_____ <Ф.И.О.>

МП

«___» _____ 202__ г.

<ПОЛНОЕ НАИМЕНОВАНИЕ ГИС>

МАТРИЦА КОММУНИКАЦИЙ

На _____ листах

СОГЛАСОВАНО

<Ответственное лицо
со стороны Получателя⁹³>

_____ <Ф.И.О.>,

МП

«___» _____ 202__ г.

Санкт-Петербург ГГГГ

⁹³ Указывается ожидаемый результат проверочного действия.

1. Публичные сетевые адреса, интерфейсы и сервисы Системы

Публичные сетевые адреса, интерфейсы и сервисы и их URL-ссылки, используемые для обеспечения функционирования ГИС в информационно-телекоммуникационной сети общего пользования «Интернет» в объектах защиты⁹⁴, разработанная в соответствии с Техническим заданием от «дата», используемые в государственной информационной системе (наименование системы) (далее – Система), определенные в (пункт и наименование документа Технического проекта, в котором определены конечные точки), приведены в Таблице 1.

Таблица 1. Публичные сетевые адреса, интерфейсы и сервисы

№ п/п	Публичный сетевой адрес	Предназначение	URL-ссылка для доступа из сети Интернет	Доменное имя
1	2	3	4	5
1	46.203.100.100	Сайт комитета комитетов	https://komitet.gov.ru/test1/	komitet.gov.ru
2	46.203.100.100	API для интеграции с мессенджером MAX	https://46.203.100.100/api/	-

2. Матрица коммуникаций ГИС с сетью Интернет для входящих соединений

Матрица коммуникаций ГИС с информационно-телекоммуникационной сетью общего пользования «Интернет» для входящих соединений, определенные в (пункт и наименование документа Технического проекта, в котором определены перенаправления), приведены в Таблице 2.

Таблица 2. Матрица коммуникаций ГИС с информационно-телекоммуникационной сетью общего пользования «Интернет» для входящих соединений

№ п/п	Источник	Назначение	Порт	Обоснование необходимости
1	2	3	4	5
1	ССОП «Интернет»	46.203.100.100	80/tcp, 443/tcp	Доступ к взб-порталу, API

3. Матрица коммуникаций ГИС с сетью Интернет для исходящих соединений

Матрица коммуникаций ГИС с информационно-телекоммуникационной сетью общего пользования «Интернет» для исходящих соединений, определенные в (пункт и наименование документа Технического проекта, в котором определены перенаправления), приведены в

⁹⁴ При наличии требования о предоставлении документа на согласование Получателю.

Таблице 3.

Таблица 3. Матрица коммуникаций ГИС
с информационно-телекоммуникационной сетью общего пользования «Интернет»
для исходящих соединений

№ п/п	Источник	Назначение	Порт	Обоснование необходимости
1	2	3	4	5
1	192.168.38.4	ips.rosminzdrav.ru	80/tcp, 443/tcp	

4. Матрица коммуникаций ГИС для входящих соединений (вне сети Интернет)

Матрица коммуникаций ГИС для входящих соединений (вне информационно-телекоммуникационной сети общего пользования «Интернет»), определенные в (пункт и наименование документа Технического проекта, в котором определены перенаправления), приведены в Таблице 4.

Таблица 4. Матрица коммуникаций ГИС
для входящих соединений
(вне информационно-телекоммуникационной сети общего пользования «Интернет»)

№ п/п	Источник	FQDN BM	Назначение	Порт	Назначение взаимодействия	URL-ссылка (при наличии)
1	2	3	4	5	6	7
1	192.168.38.4	prod.sfup.adc.gov.ru	192.168.2.5	22/tcp	Загрузка отчетов	sftp://192.168.2.5/

5. Матрица коммуникаций ГИС для исходящих соединений (вне сети Интернет)

Матрица коммуникаций ГИС для исходящих соединений (вне информационно-телекоммуникационной сети общего пользования «Интернет»), определенные в (пункт и наименование документа Технического проекта, в котором определены перенаправления), приведены в Таблице 5.

Таблица 5. Матрица коммуникаций ГИС
для исходящих соединений
(вне информационно-телекоммуникационной сети общего пользования «Интернет»)

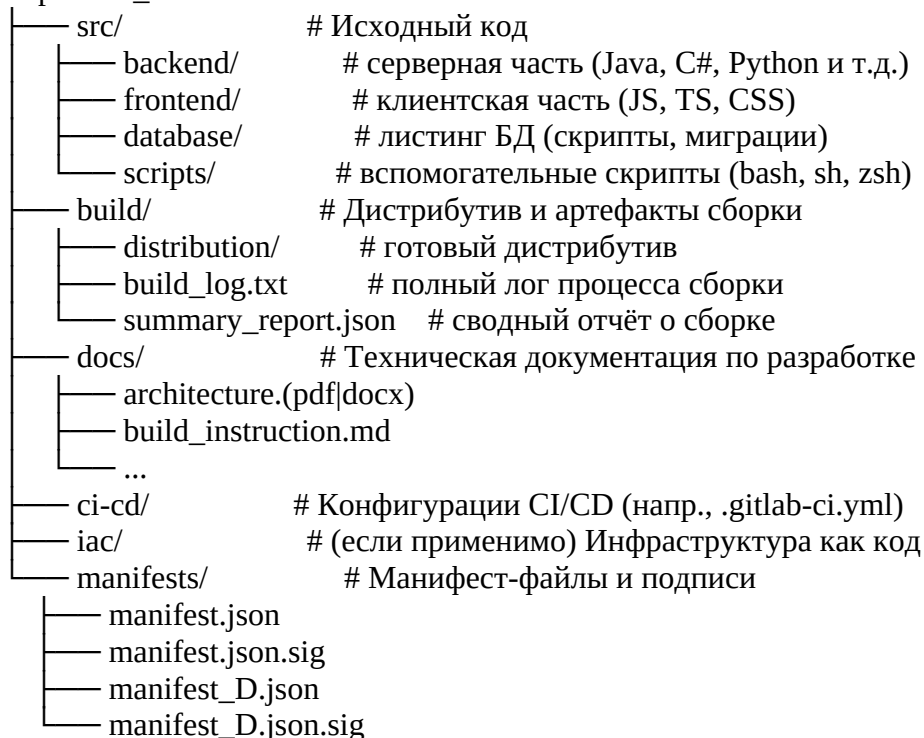
№ п/п	Источник	FQDN BM	Назначение	Порт	Назначение взаимодействия	URL-ссылка (при наличии)
1	2	3	4	5	6	7
1	10.10.10.254	192.168.38.4	prod.sfup.adc.gov.ru	443/tcp	Доступ к веб-порталу	https://192.168.38.4/prod/

13. Формат документа «Исходный код»

Все компоненты передаются в виде единого архива (формат .tar.gz или .zip). Имя архива должно содержать краткое наименование ГИС и версию, например: GIS_ShortName_vX.Y.Z_YYYYMMDD.tar.gz, не более 30 символов. Передача должна сопровождаться файлом контрольной суммы, рассчитанной по алгоритму ГОСТ Р 34.11-2012 (256 бит), для проверки целостности и подлинности архива.

Внутри архива обязательна следующая иерархия каталогов:

Корневой_каталог/



Примечание: каталоги docs, ci-cd, iac включаются при наличии соответствующих материалов.

Требования к содержимому каталогов

src/

Исходный код должен быть организован по функциональным модулям или слоям (бэкенд, фронтенд, БД).

Все не модифицируемые сторонние библиотеки и фреймворки размещаются в отдельных подкаталогах с явным указанием версий и источника, из которого были взяты.

Файлы должны быть в кодировке UTF-8 без BOM (для текстовых форматов).

Запрещено включать в исходный код учётные данные (пароли, ключи), они должны выноситься в переменные окружения или защищённое хранилище.

build/

distribution/ – содержит дистрибутив, собранный из финальной версии исходного кода. Допускается несколько подкаталогов для разных компонентов (например, server, client).

build_log.txt – полный лог сборки, фиксирующий все шаги, версии инструментов, предупреждения и ошибки.

summary_report.json – структурированный отчёт, включающий статус сборки, версии используемых компиляторов/интерпретаторов. Дополнительно (в отдельных файлах) могут быть приложены артефакты статического анализа и сканирования зависимостей (SCA).

manifests/

manifest.json – манифест исходного кода. Содержит суммарную информацию по коду Системы в начале и для каждого файла в каталогах src/, docs/, ci-cd/, iac/ (если есть) следующие атрибуты: относительный путь, размер в байтах, дата модификации, SHA-256 хеш.

manifest_D.json – манифест дистрибутива. Содержит суммарную информацию по дистрибутиву Системы и перечень файлов из каталога build/distribution/ с их хешами, а также информацию о версиях использованных библиотек, параметрах сборки, контрольные суммы внешних зависимостей.

Оба манифеста формируются автоматически (например, средствами CI/CD) и подписываются квалифицированной электронной подписью (КЭП) уполномоченного лица Исполнителя. Файлы подписи (**.sig**) сохраняются рядом с соответствующими манифестами.

Порядок формирования и передачи

Размещение в GitLab ССПК.

После завершения опытной эксплуатации Подрядчик загружает окончательную версию исходного кода в репозиторий GitLab ССПК (<https://gitlab.sspk.spb.ru/>). Ветка должна быть явно зафиксирована и версионирована (например, release/v.X.Y.Z).

Автоматизированная сборка и создание дистрибутива

В репозитории должно быть настроено задание CI/CD с именем **Distribution**, которое: выполняет полную сборку Системы;

генерирует build_log.txt и summary_report.json;

формирует архив дистрибутива в каталоге build/distribution/;

создаёт манифест-файлы manifest.json и manifest_D.json с актуальными хешами;

подписывает манифесты с помощью УКЭП Подрядчика (если технически возможно в среде GitLab – с использованием защищённых переменных или внешнего инструмента; в противном случае подписание выполняется вручную после выгрузки архива, но строго до передачи Заказчику).

Особые требования к листингу базы данных

Листинг БД должен позволять развернуть схему данных на пустой СУБД в той же версии, которая используется в Системе.

Если в процессе эксплуатации используются начальные данные (справочники, роли), они должны быть включены в виде отдельных файлов (INSERT-скриптов или CSV) с явным указанием порядка загрузки.

Версия СУБД и список всех расширений фиксируются в summary_report.json.

Для статического анализа кода на этапах до проведения испытаний допускается использование свободного программного обеспечения.

14. Формат документа «Информация о Системе»

<Краткое наименование ГИС>/<Реквизиты Контракта⁹⁵>/<Номер версии текущего документа⁹⁶>/<Дата версии текущего документа>

<Tab><Порядковый номер АС⁹⁷>/<Наименование АС>

<Tab><Tab><Порядковый номер подсистемы⁹⁸>/<Наименование подсистемы>

<Tab><Tab><Tab><Порядковый номер алиаса⁹⁹>< ><Алиас>< ><Значение алиаса в ГК>< ><Значение алиаса в проде¹⁰⁰>¹⁰¹

Пример:

АПК БГ/1643541154165465465 от 01.01.2025/2/05.06.2055

1/ПППУР

2/Система защиты информации

1 #IP23 192.168.0.25 192.168.15.78

2 #порт6 8080

⁹⁵ Перечень уровней доступа может быть изменен/дополнен исходя из структуры, архитектуры, состава программных и технических средств, особенностей функционирования Системы.

⁹⁶ Перечень Объектов защиты может быть изменен/дополнен исходя из структуры, архитектуры, состава программных и технических средств, особенностей функционирования Системы.

⁹⁷ Объекты защиты указываются в соответствии с отчетным документом «Модель угроз безопасности информации Системы».

⁹⁸ Перечень групп субъектов доступа может быть изменен/дополнен исходя из структуры, архитектуры, состава программных и технических средств, особенностей функционирования Системы.

⁹⁹ Перечень полномочий (ролей) пользователей может быть изменен/дополнен исходя из структуры, архитектуры, состава программных и технических средств, особенностей функционирования Системы.

¹⁰⁰ При наличии требования о предоставлении документа на согласование Получателю.

¹⁰¹ Под объектами защиты в соответствии с отчетным документом «Модель угроз безопасности информации Системы» понимаются: информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

15. Список слушателей, направляемых на подготовку персонала

СОГЛАСОВАНО

<Должность представителя Получателя>

_____ <ФИО>
М.П.**СПИСОК**
слушателей, направляемых на подготовку персонала

№ п/п	ФИО работника	Должность	Роль	Контактные данные (служебный e-mail, номер телефона)	Даты прохождения подготовки персонала
1					
2					
...					

16.

16. Акт о завершении подготовки персонала

АКТ о завершении подготовки персонала

Санкт-Петербург

«__» _____ 20XX

1. Наименование завершённой работы

<Наименование завершённой работы>.

2. Список представителей Подрядчика, принимающих участие в подготовке персонала

<ФИО представителей> - <Должность>.

3. Наименование документов, на основании которых проводились работы

Подготовка персонала проводилась на основании следующих документов:

<номер, дата государственного контракта Санкт-Петербурга>;

<наименования иных документов>.

4. Период выполнения подготовки

Подготовка персонала проводилась <дата или период>.

5. Список слушателей

В рамках подготовки персонала было сформировано <количество> групп(ы), общим числом пользователей в количестве <число> человек.

6. Материалы, подтверждающие проведение подготовки персонала

Список слушателей, направленных на подготовку персонала (в том числе копии списков, направленных Получателем (Оператором, Обладателем информации)

<Ведомость о прохождении подготовки персонала / Журнал аудита (журнал событий системы видеоконференцсвязи)>¹⁰².

7. Заключение о результатах завершённой подготовки

Подготовка персонала <роль администратор/пользователь> <наименование системы> проведена в срок и в соответствии с <наименование документа>.

<Наименование организации Получателя> <Адрес> ИНН ОГРН E-mail: тел. факс:	<Наименование организации Подрядчика> <Адрес> ИНН ОГРН E-mail: тел. факс:
<Должность представителя Получателя> _____<ФИО> М.П.	<Должность представителя Подрядчика> _____<ФИО> М.П.

¹⁰² Реквизиты контракта должны включать номер и дату заключения контракта