

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на выполнение работ по развитию Системы электронного
документооборота Минэкономразвития России

Москва, 2026

Содержание

1	ОБЩИЕ СВЕДЕНИЯ.....	4
1.1	Наименование объекта работ.....	4
1.2	Наименование работ.....	4
1.3	Заказчик.....	4
1.4	Исполнитель.....	4
1.5	Сроки выполнения работ.....	4
1.6	Сведения об источниках и порядке финансирования работ.....	5
1.7	Перечень нормативных правовых документов, стандартов и иных документов, которые должны быть учтены при выполнении работ.....	5
1.8	Перечень терминов, сокращений и обозначений.....	10
1.9	Порядок оформления и предъявления результатов работ.....	15
2	ЦЕЛИ И ЗАДАЧИ РАБОТ.....	18
2.1	Цели.....	18
2.2	Задачи.....	19
3	ХАРАКТЕРИСТИКА ОБЪЕКТА ВЫПОЛНЕНИЯ РАБОТ.....	21
3.1	Назначение и краткое описание Системы.....	21
3.2	Сведения о ранее заключенных контрактах.....	23
3.3	Пользователи Системы.....	23
3.4	Сведения о программном комплексе Системы.....	24
3.4.1	Подсистемы и компоненты.....	24
3.4.2	Перечень частей программного обеспечения.....	26
3.5	Взаимодействие с внешними информационными системами.....	30
4	ТРЕБОВАНИЯ К РАБОТАМ.....	31
4.1	Требование к передаче прав и уровней доступа к Системе.....	31
4.2	Численность, квалификация персонала и режим его работы.....	31
4.3	Требования к характеристикам взаимосвязей Системы со смежными системами, требованиям к ее совместимости.....	32
4.4	Требования к информационной безопасности.....	32
4.5	Требования к Системе в целом.....	42
4.5.1	Требования к показателям назначения.....	42
4.5.2	Требования к надежности.....	42
4.5.3	Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов.....	43
4.5.4	Требования к режимам функционирования.....	44
4.5.5	Требования по сохранности информации при авариях.....	45
4.5.6	Требования к эргономике и технической эстетике.....	46
4.5.7	Требования к информационному обмену между компонентами Системы.....	46
4.5.8	Требования к патентной чистоте.....	47
4.5.9	Требования по стандартизации и унификации.....	47
4.6	Требования к видам обеспечений.....	47
4.6.1	Требования к организационному обеспечению.....	47
4.6.2	Требования к методическому обеспечению.....	48
4.6.3	Требования к лингвистическому обеспечению.....	48
4.6.4	Требования к программному обеспечению.....	48
4.7	Требования к функциям (задачам) по развитию Системы.....	49
4.7.1	Требования к развитию (адаптации) функционала модуля МЭДО в части обмена данными с глобальным адресным справочником (ГАС).....	49
4.7.2	Требования к развитию (адаптации) функционала модуля МЭДО в части поддержки формата обмена данными МЭДО 3.0.....	50

4.7.3	Требования к развитию (адаптации) функционала СЭДО в части обмена данными по событиям цифровых поручений второй очереди.....	51
4.7.4	Требования к развитию (адаптации) функционала СЭДО интеграции с сайтом Минэкономразвития России в части передачи контактной информации структурного подразделения Министерства по запросу юридического лица.....	52
4.7.5	Требования к развитию (адаптации) функционала СЭДО в части отправки одного исходящего события по нескольким пунктам цифрового поручения.....	52
4.7.6	Требования к развитию (адаптации) функционала СЭДО в части автоматической простановки вида контроля «ВК» по пунктам цифрового поручения, где Минэкономразвития России является соисполнителем. .	53
4.7.7	Требования к развитию (адаптации) функционала СЭДО в части отображения подписанта цифрового поручения в дереве резолюций РК.....	53
4.7.8	Требования к развитию (адаптации) функционала СЭДО в части изменения последовательности отображения значений в поле «Номер пункта» в резолюциях по событиям Цифровых поручений.....	54
4.7.9	Требования к развитию (адаптации) функционала СЭДО в части автоматического указания Министра экономического развития Российской Федерации исполнителем по пунктам цифрового поручения. .	54
4.7.10	Требования к развитию (адаптации) функционала СЭДО в части изменения порядка отображения пунктов цифрового поручения.....	54
4.7.11	Требования к развитию (адаптации) функционала СЭДО в части реализации возможности вывода информации в поле «Текст поручения» в пункте внешней резолюции РК.....	54
4.7.12	Требования к развитию (адаптации) функционала СЭДО в части реализации возможности направления исходящего документа по пунктам цифрового поручения, созданным вручную во внешней резолюции .	55
4.7.13	Требования к разработке Частного технического задания на развитие Системы.....	55
4.7.14	Требование к актуализации Модели угроз и Модели нарушителя информационной безопасности Системы .	56
4.7.15	Требование к актуализации Частного технического задания на модернизацию системы защиты информации Системы.....	57
5	СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО РАЗВИТИЮ СИСТЕМЫ.....	61
6	ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ ВЫПОЛНЕННЫХ РАБОТ.....	67
6.1	Виды, состав, объем и методы испытаний Системы и ее составных частей.....	67
6.1.1	Требования к проведению предварительных испытаний.....	67
6.1.2	Требования к проведению опытной эксплуатации.....	68
6.1.3	Требования к проведению приемочных испытаний.....	69
6.1.4	Требования к мероприятиям по подготовке и проведению аттестационных испытаний Системы.....	70
7	ОБЪЕМ И СРОКИ ГАРАНТИЙ КАЧЕСТВА.....	72
8	ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ.....	73
8.1	Перечень подлежащих разработке документов.....	73
8.2	Требования к эксплуатационной и программной документации.....	73
8.3	Требования по использованию ЕСКД и ЕСПД при разработке документов.....	73

1 Общие сведения

1.1 Наименование объекта работ

Наименование объекта работ: Система электронного документооборота Минэкономразвития России (далее – СЭДО, Система).

Код по ОКПД2/КТРУ: 58.29.50.000/58.29.11.000-000000003; 62.01.11.000.

1.2 Наименование работ

Полное наименование работ: работы по развитию Системы электронного документооборота Минэкономразвития России (далее – выполнение работ, работы, развитие).

Сокращенное наименование работ: работы по развитию Системы.

1.3 Заказчик

Заказчиком настоящих работ является Министерство экономического развития Российской Федерации (далее – Заказчик, Министерство).

Сведения о реквизитах Заказчика представлены в Таблице 1.

Таблица 1 – Реквизиты Заказчика

№ п/п	Наименование	Описание
1	Место нахождения и почтовый адрес	123112, г. Москва, Пресненская наб., д. 10, стр. 2
2	Телефон	+7 (495) 870-29-21
3	Контактный адрес электронной почты	mineconom@economy.gov.ru
4	Адрес Заказчика в сети Интернет	www.economy.gov.ru

1.4 Исполнитель

Исполнитель определяется по результатам проведения открытого аукциона в электронной форме соответствии с федеральным законом от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

1.5 Сроки выполнения работ

Сроки выполнения работ: с даты заключения контракта по 20 декабря 2026 г. включительно, в том числе:

- этап Работ № 1: в течение 7 календарных дней с даты заключения Контракта;
- этап Работ № 2: с даты заключения контракта по 25 ноября 2026 г. включительно;
- этап Работ № 3: с даты завершения этапа работ № 2 по 11 декабря 2026 г. включительно;

- этап Работ № 4: с даты завершения этапа работ № 3 по 20 декабря 2026г. включительно.

1.6 Сведения об источниках и порядке финансирования работ

Источником финансирования работ является федеральный бюджет.

Порядок финансирования определяется действующими нормативными правовыми актами, регулирующими вопросы финансирования расходов федерального бюджета, и Контрактом, заключаемым с Исполнителем.

1.7 Перечень нормативных правовых документов, стандартов и иных документов, которые должны быть учтены при выполнении работ

Перечень нормативных правовых документов, стандартов и иных документов, которые должны быть учтены при выполнении работ:

- приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 11 июля 2024 г. № 610 «Об утверждении цифровых шаблонов и форматов документов, используемых при работе с поручениями Правительства Российской Федерации в информационной системе обеспечения внутриведомственного и межведомственного документооборота и контроля исполнения поручений, в том числе с использованием облачных сервисов»;
- приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации № 611, ФСО России № 96 от 12 июля 2024 г. «Об утверждении Требований к организационно-техническому взаимодействию государственных органов и государственных организаций»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;
- Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;
- Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при

использовании информационно-телекоммуникационных сетей международного информационного обмена»;

- Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

- Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

- Постановление Правительства Российской Федерации от 18 мая 2009 г. № 424 «Об особенностях подключения федеральных государственных систем к информационно-телекоммуникационным сетям»;

- Постановление Правительства Российской Федерации от 24 ноября 2009 г. № 953 «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации, подведомственных ему организаций и федеральных органов исполнительной власти»;

- Постановление Правительства Российской Федерации от 8 сентября 2010 г. № 697 «О единой системе межведомственного электронного взаимодействия»;

- Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»;

- Постановление Правительства Российской Федерации от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

- Постановление Правительства Российской Федерации от 16 апреля 2012 г. № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных

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

- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства Российской Федерации от 6 июля 2015 г. № 675 «О порядке осуществления контроля за соблюдением требований, предусмотренных частью 2.1 статьи 13 и частью 6 статьи 14 Федерального закона «Об информации, информационных технологиях и о защите информации»;

- Постановление Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

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

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

- Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;

- Приказ ФСТЭК России от 4 июля 2022 г. № 118 «Требования по безопасности информации к средствам контейнеризации (выписка)»;

- Приказ ФСТЭК России от 1 декабря 2023 № 240 «Об утверждении Порядка проведения сертификации процессов безопасной разработки программного обеспечения средств защиты информации»;

- Приказ ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»;

- Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

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

- Приказ ФСБ России от 24 июля 2018 г. № 367 «Об утверждении перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

- Приказ ФСБ России от 4 ноября 2022 г. № 547 «Об утверждении перечня сведений в области военной, военно-технической деятельности Российской Федерации, которые при их получении иностранными источниками могут быть использованы против безопасности Российской Федерации»;

- Приказ ФСБ России от 13 февраля 2023 г. № 77 «Об утверждении порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных»;

- Приказ ФАПСИ от 13 июня 2001 г. № 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 Министерства связи и массовых коммуникаций Российской Федерации от 25 августа 2009 г. № 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»;

- Приказ Министерства связи и массовых коммуникаций Российской Федерации от 23 июня 2015 г. № 210 «Об утверждении технических требований к

взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия»;

- Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18 августа 2021 г. № 857 «Об утверждении единых требований к формам доверенностей, необходимых для использования квалифицированной электронной подписи»;

- Приказ Министерства экономического развития Российской Федерации от 13 ноября 2023 г. № 785 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении Министерством экономического развития Российской Федерации функций, определенных законодательством Российской Федерации»;

- Приказ Министерства экономического развития Российской Федерации от 24 ноября 2023 г. № 821 «Об утверждении Регламента выявления, анализа и устранения уязвимостей в информационных системах Министерства экономического развития Российской Федерации»;

- Методика испытаний систем защиты информации информационных систем методами тестирования на проникновение, утв. ФСТЭК России 25 июня 2025 г.;

- Методический документ «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечение безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержден ФСТЭК России 11 ноября 2025 г.;

- Методический документ «Методика анализа защищенности информационных систем», утвержден ФСТЭК России 25 ноября 2025 г.;

- Методический документ «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», утвержден ФСТЭК России 12 апреля 2026 г.;

- Методический документ «Методика оценки угроз безопасности информации», утвержден ФСТЭК России от 5 февраля 2021 г.;

- Методический документ «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств», утвержден ФСТЭК России от 30 июня 2025 г.;

- Методический документ «Методика тестирования обновлений безопасности программных, программно-аппаратных средств», утвержден ФСТЭК России от 28 октября 2022 г.;

- Методический документ «Руководство по организации процесса управления уязвимостями в органе (организации)», утвержден ФСТЭК России от 17 мая 2023 г.

- Приказ ФСБ России от 22 августа 2026 г. № 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»;

- ГОСТ Р 59792-2021. Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем;

Требования указанных выше нормативно-правовых актов применяются только и исключительно в той части, которая не ведет к изменению объема и стоимости работ по Государственному контракту.

1.8 Перечень терминов, сокращений и обозначений

В Таблице 2 приведены термины, сокращения и обозначения, используемые в настоящем ТЗ.

Таблица 2 – Термины, сокращения и определения

Термин, сокращение, обозначение	Полная форма
АРМ	Автоматизированное рабочее место
БД	База данных
БДУ	Банк данных угроз безопасности информации ФСТЭК России
Вычислительные ресурсы	Технические средства ЭВМ, в том числе процессор, объемы оперативной и внешней памяти, время, в течение которого программа занимает эти средства в ходе выполнения
Веб-браузер	Приложение для просмотра и взаимодействия посредством сети Интернет-ресурсов, размещенных в удаленном доступе (документы, файлы, сервисы)
Веб-клиент	Приложение СЭДО, выполняющее функции Тонкого клиента
ГК	Государственный контракт
ГИС «ТОР СЭД»	Государственная информационная система «Типовое облачное решение системы электронного документооборота»
ГОСТ	Государственный стандарт

ГОСТ РО	Государственный стандарт, действующий только на территории Российской Федерации ограниченного распространения
ГОСТ Р	Государственный стандарт, действующий только на территории Российской Федерации
ГосЭДО	Государственный электронный документооборот (платформа для юридически значимого обмена электронными документами между бизнесом и государственными органами)
ДСП	Гриф «для служебного пользования», используется для обозначения документов, содержащих информацию, отнесенную к сведениям, составляющим служебную тайну
ЕИС	Единая информационная система в сфере закупок
ЗК	Закрытый контур
ИБ	Информационная безопасность
Информационно-телекоммуникационная сеть «Интернет»	Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники
ИС	Информационная система
Исполнитель	Организация, определенная победителем по результатам проведения открытого конкурса в электронной форме в соответствии с Федеральным законом от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»
КЗ	Карточка задания, сформированная в СЭДО для одного исполнителя при утверждении инициативного поручения или резолюции, при запуске маршрута согласования или при передаче документа на рассмотрение
МРМР	Мобильное рабочее место руководителя. Интегрированный с СЭДО модуль на базе программного обеспечения «Мобильное Рабочее Место Руководителя», предоставляющий возможность выполнения операций с документами и поручениями СЭДО на мобильных устройствах
МЭДО	Система межведомственного электронного документооборота – федеральная информационная система, обеспечивающая в автоматизированном режиме защищенный обмен электронными сообщениями, в том числе ДСП, между Администрацией Президента Российской Федерации, Аппаратом Правительства Российской Федерации и федеральными органами исполнительной власти, а также иными федеральными органами и ведомствами государственной власти
Контракт	Государственный контракт на выполнение работ по развитию Системы электронного документооборота Минэкономразвития России
Министерство, Минэкономразвития России, Заказчик	Министерство экономического развития Российской Федерации
МУиН	Модель угроз безопасности информации и Модель нарушителя безопасности информации
НСД	Несанкционированный доступ
ОК	Открытый контур
ОС	Операционная система

Оператор	Организация, которая технически подключает участников (госорганы, организации) к системе обмена электронными документами и обеспечивает их связь с общей инфраструктурой ГАС/МЭДО.
Оператор ОЦОД ПК	Организация, обслуживающая ОЦОД ПК и предоставляющая доступ к мощностям ОЦОД ПК
ОЦОД ПК	Объединенный центр обработки данных Правительственного комплекса
Патентная чистота ПО	Юридическое свойство технической реализации программного обеспечения, означающее отсутствие нарушения на территории РФ исключительных прав третьих лиц на объекты промышленной собственности (охраняемые патентами в соответствии со ст. 1350–1352 ГК РФ), а также отсутствие препятствий для использования ПО, связанных с правами на другие объекты интеллектуальной собственности.
ПДн	Персональные данные
ПК	Правительственный комплекс, расположенный по адресу г. Москва, Пресненская наб., д.10, стр.2 (Башня 2)
ПО	Программное обеспечение
ПОС	Единое цифровое окно обратной связи (Платформа обратной связи) федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)»
Ресурс Минэкономразвития России для размещения отчетной документации	Информационная система (или компонент информационной системы) Минэкономразвития России, с функциональностью по размещению отчетной документации, предусмотренной Государственными контрактами
РК	Регистрационная карточка
Сайт	Система экспертного сопровождения и общественного обсуждения Плана деятельности Министерства экономического развития Российской Федерации (официальный информационный сайт) в информационно-телекоммуникационной сети «Интернет»
СДУ	Система документационного управления
СМЭВ	Система межведомственного электронного взаимодействия – федеральная государственная информационная система, в задачу которой входит обеспечение исполнения государственных функций и предоставления государственных услуг в электронной форме, а также обеспечение информационного взаимодействия при предоставлении этих услуг и исполнении этих функций
ССТУ.РФ	Портал коммутационной платформы сетевого справочного телефонного узла – сетевой информационный ресурс, на котором публикуются данные об органах местного самоуправления, государственных учреждениях и органах, а также соответствующих лицах, уполномоченных на решение государственных и территориальных вопросов. На ресурсе также публикуются результаты рассмотрения обращений граждан в вышеуказанные органы и к соответствующим лицам
СЗИ	Система защиты информации

СПО	Специальное программное обеспечение, часть программного обеспечения, представляющая собой совокупность программ, разработанных при создании/развитии данной Системы (ГОСТ Р 59853-2021. Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения)
СрЗИ	Средства защиты информации
ОПО	Общее программное обеспечение, часть программного обеспечения, представляющая собой совокупность программных средств, разработанных вне связи с созданием/развитием данной Системы. Обычно ОПО представляет собой совокупность программ общего назначения, предназначенных для организации вычислительного процесса и решения часто встречающихся задач обработки информации (ГОСТ Р 59853-2021. Национальный стандарт Российской Федерации. Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения)
Система, СЭДО	Система электронного документооборота Минэкономразвития России
СКЗИ	Средства криптографической защиты информации
СУБД	Система управления базами данных
ТЗ	Техническое задание
ТС	Технические средства
ТУ	Технические условия
ТК, Транспортный контейнер	Основная единица передачи данных по МЭДО, представляющая собой ZIP-архив, содержащий данные в соответствии с утверждёнными форматами взаимодействия
Тонкий клиент	Приложение, выполняющее задачи по обработке данных, у которого ресурсы для выполнения задач и данные для их выполнения находятся на сервере баз данных, а на устройстве, на котором оно установлено, находится только интерфейс, выполняющий соответствующие запросы к серверу. В рамках настоящего документа термин аналогичен термину «Веб-клиент»
ТУ ИС ФОИВ ОЦОД ПК	Технические условия по размещению информационных систем федеральных органов исполнительной власти в объединённом центре обработки данных правительственного комплекса, редакция АГРВ.466459.301-01ТУ
Фаззинг-тестирование	Техника тестирования программного обеспечения, часто автоматическая или полуавтоматическая, заключающаяся в передаче приложению на вход неправильных, неожиданных или случайных данных
ФОИВ	Федеральный орган исполнительной власти
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
ФТ	Функциональные требования
Хеш-сумма	Результат обработки данных математическим алгоритмом (хеш-функцией), который отображает данные произвольного размера в битовый массив фиксированного размера

ЦОД	Специализированный объект, представляющий собой связанную систему ИТ-инфраструктуры и инженерной инфраструктуры, оборудование и части которых размещены в здании или помещении, подключенном к внешним сетям, как инженерным, так и телекоммуникационным
ЦП	Цифровое поручение
ЧТЗ	Частное техническое задание
ЧТЗ на СЗИ	Частное техническое задание на модернизацию системы защиты информации
ЭВМ	Электронная вычислительная машина
ЭП	Электронная подпись
AppArmor	Реализация безопасности линукс по управлению доступом на основе имен
API	(англ. Application Programming Interface, интерфейс прикладного программирования) — набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах
BPMN	Business Process Model and Notation (нотация и модель бизнес-процессов) – система условных обозначений (нотация) и их описания в XML для моделирования бизнес-процессов
CAPTCHA	(англ. Completely Automated Public Turing test to tell Computers and Humans Apart, полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей) — компьютерный тест, используемый для того, чтобы определить, кем является пользователь системы: человеком или компьютером
CSS	(англ. Cascading Style Sheets) формальный язык декорирования и описания внешнего вида документа (веб-страницы), написанного с использованием языка разметки
CVE	(англ. Common Vulnerabilities and Exposures) база данных общеизвестных уязвимостей информационной безопасности
DDMWeb Service	Сервис для сканирования и печати документов на принтере в Веб-клиенте
DocsVision	Комплексная программная платформа, предназначенная для автоматизации процессов управления, документооборота и для создания интегрированных приложений. Платформа DocsVision представляет собой трехуровневое приложение, центральным элементом которого является карточка – совокупность описания структуры, соответствующих ей данных и одного или нескольких элементов управления ActiveX, реализующих пользовательский интерфейс. Платформа включает в себя основную часть серверных компонентов СЭДО
ERD	(англ. Entity Relationship Diagram) визуальное представление структуры данных и связей между ними в системе
HTML (HyperText Markup Language)	Стандартизированный язык гипертекстовой разметки документов для просмотра веб-страниц в браузере
HTTP (HyperText Transfer Protocol)	Сетевой протокол прикладного уровня, который изначально предназначался для получения с серверов гипертекстовых документов в формате HTML.

HTTPS (HyperText Transfer Protocol Secure)	Расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IP, IP-адрес	(англ. Internet Protocol, межсетевой протокол) — маршрутизируемый протокол сетевого уровня стека TCP/IP
IEDMS	(Англ. Integrated Electronic Document Management System) – интегрированная электронная система управления документами
JavaScript	(англ. JS) — мультипарадигменный язык программирования
OOM	(англ. out-of-memory) механизм ядра ОС Linux, который в случае исчерпания оперативной памяти (RAM) освобождает ее путем завершения существующих процессов
ReCAPTCHA	Система, разработанная в университете Карнеги — Меллона для защиты веб-сайтов от интернет-ботов и одновременной помощи в оцифровке текстов книг. Является продолжением проекта CAPTCHA
REST	(Англ. Representational State Transfer) – способ организации программного взаимодействия с помощью протокола HTTP
RSA	(Аббревиатура от фамилий Rivest, Shamir и Adleman) – криптографический алгоритм с открытым ключом, используемый и для шифрования, и для цифровой подписи
SELinux	(англ. Security-Enhanced Linux) реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа
SBOM	(англ. Software Bill of Materials) — спецификация программного обеспечения
SCA	(англ. Software Composition Analysis) анализ состава программного обеспечения.
SPDX	(англ. Software Package Data Exchange) международный открытый стандарт (ISO/IEC 5962:2021) для представления спецификации программного обеспечения
SSL	(англ. Secure Sockets Layer, уровень защищённых сокетов) — криптографический протокол, который использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений
SWID	(англ. Software Identification Tag) формат маркировки программного обеспечения, регламентированный международным стандартом ISO/IEC 19770-2:2015 и его адаптированными версиями
TCP/IP	Набор сетевых протоколов передачи данных, используемых в сетях, включая сеть Интернет. Протоколы работают друг с другом в стеке (англ. stack, стопка) – это означает, что протокол, располагающийся на уровне выше, работает «поверх» нижнего, используя механизмы инкапсуляции. Например, протокол TCP работает поверх протокола IP
Unicode Bidi (Unicode Bidirectional Algorithm)	(англ. unicode bidirectional algorithm) алгоритм двунаправленного юникода
URL	(англ. Uniform Resource Locator) адрес ресурса в сети Интернет
XSS уязвимость	(англ. Cross-Site Scripting) подтип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода и взаимодействии этого кода с веб-сервером злоумышленника

1.9 Порядок оформления и предъявления результатов работ

Результаты работ оформляются и передаются в соответствии с разделом 5 настоящего ТЗ Заказчику в порядке, установленном Контрактом и настоящим ТЗ.

Результатами выполнения Исполнителем работ, требования к которым определены в настоящем ТЗ, является функционирование адаптированных функций Системы в соответствии с требованиями, приведенными в пункте 4.7.

В ходе и по завершении выполнения работ по отчетному периоду Исполнитель размещает отчетную документацию, определенную требованиями Контракта как результат выполнения работ по отчетному периоду, на Ресурсе Минэкономразвития России для размещения отчетной документации.

По факту размещения материалов Исполнителем на Ресурсе Минэкономразвития России для размещения отчетной документации и уведомления Заказчика об этом Заказчик проводит экспертизу (в порядке, определенном Контрактом) представленной отчетной документации на предмет полноты и качества выполненных работ, в том числе на предмет их соответствия требованиям Контракта.

В случае выявления замечаний по результатам экспертизы к представленной отчетной документации Заказчик направляет перечень замечаний Исполнителю, а Исполнитель обязуется устранить указанные замечания до предоставления Заказчику итоговых отчетных материалов, определенных требованиями Контракта как результат выполненных работ за отчетный период.

Заказчик вправе запросить внеочередное предоставление отчетных материалов по выполнению работ за отчетный период (не чаще 1 раза в квартал, не более 2 раз в ходе выполнения работ за отчетный период). В случае такого запроса от Заказчика Исполнителем должны быть представлены отчетные документы официальным письмом, в которых содержатся сведения о работах, фактически выполненных на момент поступления данного запроса. Срок внеочередного предоставления отчетных материалов – 3 (три) рабочих дня с даты запроса.

В установленный Контрактом срок Исполнитель формирует итоговые отчетные документы и материалы по выполнению работ за отчетный период и предоставляет с использованием Единой информационной системы в сфере закупок (далее – ЕИС), подписывает усиленной квалифицированной электронной подписью лица, имеющего право действовать от имени Исполнителя, и размещает в ЕИС документ о приемке в соответствии с требованиями ч.13 ст. 94 Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных

и муниципальных нужд».

Документация в виде электронных документов и (или) электронных образов документов должна быть подписана усиленной квалифицированной электронной подписью юридического лица с указанием фамилии, имени, отчества, имеющего право действовать без доверенности от имени Исполнителя, либо представителем на основании доверенности (личной усиленной квалифицированной электронной подписью физического лица), либо усиленной квалифицированной электронной подписью физического лица, исполняющего соответствующие должностные обязанности Исполнителя.

Контроль и приемка выполненных работ за отчетный период осуществляется в соответствии с условиями Контракта, пунктом 6 настоящего ТЗ и оформляется Актами приемки выполненных работ за отчетный период. Условия оплаты выполненных работ определяются Контрактом.

В случае, если при проверке представленных отчетных документов в ходе контроля и приемки выполненных работ за отчетный период будет установлена неактуальность, противоречивость либо неполнота сведений, Заказчик в порядке, определенном Контрактом, возвращает Исполнителю документы на доработку с указанием причин отказа в приемке результатов выполненных работ.

Требования к оформлению отчетной документации по результату выполненных работ обозначены в пункте 8 настоящего ТЗ.

2 Цели и задачи работ

2.1 Цели

Целями выполнения работ являются:

- Оптимизация процессов электронного документооборота за счет обмена данными с глобальным адресным справочником (ГАС);
- Реализация взаимодействия с внешними ИС по формату обмена данными МЭДО 3.0 за счет развития модуля МЭДО;
- Соответствие нормативным требованиям в части обработки цифровых поручений по событиям «Принятие информации об исполнении», «Изменение срока поручения», «Представление промежуточного доклада» и «Запрос изменения срока поручения»;
- Автоматизация процесса передачи информации об департаменте, ответственном за обработку обращения юридического лица;
- Расширение функциональных возможностей в части подготовки одного закрывающего документа по нескольким пунктам цифрового поручения;
- Автоматизация процесса указания вида контроля для соисполнителей по пунктам цифрового поручения во внешней резолюции;
- Повышение эргономичности интерфейса СЭДО за счет отображения внешнего контрагента в дереве резолюций;
- Повышение эргономичности интерфейса СЭДО за счет изменения последовательности отображения значений в поле «Номер пункта» во внешней резолюции цифрового поручения;
- Автоматизация процесса заполнения поля «Исполнитель» во внешней резолюции цифрового поручения;
- Повышение эргономичности интерфейса СЭДО за счет развития функциональности изменения последовательности пунктов внешней резолюции цифрового поручения;
- Расширение функциональных возможностей СЭДО в части вывода информации в поле «Текст поручения» в пункте внешней резолюции цифрового поручения;
- Оптимизация возможности отчитаться по пунктам цифрового поручения, созданных вручную во внешней резолюции;
- Обеспечение защиты информации ограниченного доступа (персональных данных, иной информации конфиденциального характера), обрабатываемой в Системе, от несанкционированного или случайного доступа, уничтожения,

изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации ограниченного доступа; поддержание требуемого уровня защищенности информации в Системе.

2.2 Задачи

Задачи, которые необходимо решить для достижения поставленных целей:

- Развитие (адаптация) функционала модуля МЭДО в части обмена данными с глобальным адресным справочником (ГАС);
- Развитие (адаптация) функционала модуля МЭДО в части поддержки формата обмена данными МЭДО 3.0;
- Развитие (адаптация) функционала СЭДО в части обмена данными по событиям цифровых поручений второй очереди;
- Развитие (адаптация) функционала СЭДО в части интеграции с сайтом Минэкономразвития России для передачи контактной информации структурного подразделения Министерства по запросу юридического лица;
- Развитие (адаптация) функционала СЭДО в части отправки одного исходящего события по нескольким пунктам цифрового поручения;
- Развитие (адаптация) функционала СЭДО в части автоматической простановки вида контроля «ВК» по пунктам цифрового поручения, где Минэкономразвития России является соисполнителем;
- Развитие (адаптация) функционала СЭДО в части отображения подписанта внешнего контрагента в дереве резолюций;
- Развитие (адаптация) функционала СЭДО в части изменения формата отображения номера пункта цифрового поручения;
- Развитие (адаптация) функционала СЭДО в части автоматического указания руководителя Минэкономразвития России исполнителем по пунктам внешней резолюции цифрового поручения;
- Развитие (адаптация) функционала СЭДО в части изменения порядка отображения пунктов цифрового поручения во внешней резолюции и дереве резолюции;
- Развитие (адаптация) функционала СЭДО в части реализации возможности вывода информации в поле «Текст поручения» в пункте внешней резолюции цифрового поручения;

- Развитие (адаптация) функционала СЭДО в части реализации возможности направления исходящего документа по пунктам цифрового поручения, созданным вручную во внешней резолюции;
- Актуализация действующей Модели угроз и нарушителя безопасности информации Системы (МУиН);
- Проверка Системы на наличие уязвимостей программного обеспечения и устранение выявленных уязвимостей;
- Осуществление комплекса мероприятий по подготовке Системы к аттестационным испытаниям на соответствие требованиям о защите информации»;
- Разработка частного технического задания на развитие Системы и/или СЗИ.

3 Характеристика объекта выполнения работ

3.1 Назначение и краткое описание Системы

СЭДО предназначена для комплексной автоматизации документооборота, а именно для автоматизации следующих видов деятельности:

- регистрация входящих документов (в том числе обращений граждан);
- подготовка, согласование и регистрация внутренних и исходящих документов (в том числе ответов на обращения граждан);
- подготовка резолюций и инициативных поручений;
- исполнение заданий по резолюциям;
- контроль исполнительской дисциплины;
- формирование отчетности;
- поиск регистрационных карточек и карточек заданий;
- ведение оперативного архива.

Система оснащена сертифицированными средствами защиты информации и эксплуатируется в соответствии с требованиями по информационной безопасности, Аттестатом соответствия системы требованиям о защите информации, внутренними стандартами, требованиями по безопасности информации, требованиями к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов Системы, определяемыми производителями средств защиты информации, внутренними регламентами Заказчика и ТУ ИС ФОИВ ОЦОД ПК в инфраструктуре объединенного центра обработки данных Правительственного комплекса (далее – ОЦОД ПК).

ОЦОД ПК имеет Аттестат соответствия требованиям о защите информации от 23 марта 2023 г. № Л024-00107-00/00582586.00547.2023 и соответствует требованиям о защите информации в части реализации мер защиты предъявляемым к государственным информационным системам первого класса защищенности (К1) в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», и к информационным системам персональных данных, для которых установлена необходимость обеспечения первого уровня защищенности персональных данных (УЗ-1) в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

В соответствии с «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 апреля 2025 г. № 117 предполагаемый класс защищенности ОЦОД ПК – К1 (высокий уровень значимости, масштаб – федеральный).

Система имеет Аттестат соответствия требованиям о защите информации от 14.03.2025. № Л024-00107-0000580416.232.2023 и соответствует требованиям, предъявляемым к государственным информационным системам 1 класса защищенности (К1) в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», и к информационным системам персональных данных, для которых установлена необходимость обеспечения третьего уровня защищённости персональных данных (УЗ-3) в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

В соответствии с «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 апреля 2025 г. № 117 предполагаемый класс защищенности Системы – К1 (высокий уровень значимости, масштаб – федеральный, масштаб – федеральный).

Система введена в эксплуатацию приказом Минэкономразвития России от 25 января 2007 г. № 19 «Об организации промышленной эксплуатации Системы электронного документооборота Минэкономразвития России».

Система не является объектом критической информационной инфраструктуры Российской Федерации, в связи с тем, что Минэкономразвития России не является субъектом критической информационной инфраструктуры Российской Федерации, так как сфера деятельности не попадает под определение части 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

В качестве основы функционирования СЭДО и прикладного программного обеспечения используется система документационного управления «Приоритет» (далее –

СДУ «Приоритет») на базе платформы DocsVision 5 и включает в себя серверные и клиентские компоненты.

Обеспечение взаимодействия с Национальным координационным центром по компьютерным инцидентам (НКЦКИ) в рамках Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА) осуществляется силами Корпоративного центра ГосСОПКА «Ростелеком-Солар» при оказании услуг информационной безопасности и технической защите информационно-телекоммуникационной инфраструктуры правительственного комплекса по отдельному государственному контракту.

Обеспечение взаимодействия в автоматизированном режиме с Национальной системой противодействия DDoS-атакам (НСПА) Центра мониторинга и управления сетью связи общего пользования ФГУП «ГРЧЦ» в рамках реализации мер по защите Системы от атак, направленных на отказ в обслуживании, осуществляется владельцем ОЦОД ПК при оказании услуг информационной безопасности и технической защите информационно-телекоммуникационной инфраструктуры правительственного комплекса по отдельному государственному контракту.

3.2 Сведения о ранее заключенных контрактах

Развитие и сопровождение Системы осуществлялось на основании следующих контрактов:

- от 10 ноября 2020 г. № 0173100008620000045;
- от 29 октября 2021 г. № 0173100008621000054;
- от 17 октября 2022 г. № 0173100008622000030;
- от 25 ноября 2024 г. № 0173100008624000031.

3.3 Пользователи Системы

Пользователями СЭДО являются сотрудники Минэкономразвития России, исполнение должностных обязанностей которых связано с документооборотом.

3.4 Сведения о программном комплексе Системы

Система размещена на вычислительных ресурсах облачной инфраструктуры ОЦОД ПК.

Система построена на основе программных компонентов и модулей, обеспечивающих как внутреннее взаимодействие подсистем, так и взаимодействие с внешними ИС в закрытом сегменте ОЦОД ПК.

3.4.1 Подсистемы и компоненты

Система включает следующие подсистемы (Таблица 3):

Таблица 3 – Перечень подсистем

№ п/п	Наименование модуля / подсистемы	Описание и предназначение
1.	Платформа DocsVision 5	Обеспечивает базовые функции автоматизации документооборота и процессов управления, содержит параметрические механизмы настройки функциональности без программирования
2.	Делопроизводство/TakeOffice	Обеспечивает расширение набора атрибутов РК для организации типового документооборота Организации, а также предоставляет справочники для ведения справочной информации, используемой для заполнения атрибутов РК
3.	Расширенные отчеты/Reporting	Реализует функциональность построения отчетов высокой сложности. Отчеты такого типа могут использоваться при необходимости отображения данных, требующих формирования сложных запросов, а также, если внешний вид отчета не может быть реализован стандартным механизмом представлений или требует выгрузки в специальный формат
4.	Служебные карточки/BackOffice	Реализует функциональность разграничения прав доступа к определенным элементам системы
5.	Системные карточки/.NET	Реализует функциональность управления настройками СЭДО и ее составляющих модулей
6.	Административное делопроизводство/DDM	Предоставляет интерфейс для создания и обработки регистрационных карточек входящих и исходящих документов, просмотра уведомлений МЭДО, работу со «Справочником сопоставления» и «Справочником наложения штампов», позволяет выполнять анализ состояний входящих/исходящих карточек в виртуальных поисковых папках

№ п/п	Наименование модуля / подсистемы	Описание и предназначение
7.	АРМ контролера/Card Control	Модуль предназначен для контроля исполнения поручений, поставленных на внешний контроль, контроль на уровне организации или контроль на уровне подразделения
8.	Веб-клиент/DDMWeb	Предназначен для выполнения пользовательских задач по работе с модулем Административное делопроизводство системы документооборота с использованием веб-браузера
9.	АРМ Руководителя/Executive Workspace	Предоставляет возможность выполнения операций с документами и поручениями СЭДО на мобильных устройствах как в онлайн, так и в оффлайн режиме, после предварительной синхронизации с сервером
10.	Модуль интеграционного интерфейса/Integration Service	Предоставляет программный интерфейс для интеграции СЭДО с внешними ИС
11.	Модуль интеграции с ПОС/FeedbackService	Предназначен для получения из ПОС данных по обращениям граждан через СМЭВ, обработки адаптером СМЭВ и отправки через адаптер в СМЭВ, а затем в ПОС ответов на обращения граждан и статусов их рассмотрения
12.	Модуль интеграции с МЭДО/IEDMS	Позволяет организовывать обмен документами электронного документооборота между различными федеральными органами исполнительной власти, а также отслеживать процесс обработки документа на стороне получателя через получение уведомлений о ключевых этапах обработки документа
13.	Модуль интеграции с CCTY.РФ/ SSTU Integration Service	Предназначен для отправки данных о результатах рассмотрения обращений граждан на портал CCTY.РФ
14.	Сервис синхронизации /Synchronizationservice	Обеспечивает обмен данными между СЭДО и АРМ Руководителя, в том числе преобразование данных в нужный формат и изменение объектов СЭДО на основании данных, полученных из МРМР
15.	Сервис конвертации/ Conversion-service	Обеспечивает конвертацию файлов вложений документов СЭДО для обеспечения функций клиента
16.	Мастер наложения штампов/Stamp Wizard	Предназначен для наложения штампов на утвержденные и подписанные ЭП документы
17.	Модуль архивного делопроизводства/Archive	Позволяет вести систематизированный перечень дел с указанием необходимых атрибутов и параметров
18.	Модуль интеграции с Российским офисным	Обеспечивает возможность интеграции с

№ п/п	Наименование модуля / подсистемы	Описание и предназначение
	ПО/R7Office	Российским офисным ПО (с Р7-Офис)
19.	Транспортные расширения/ TransportExtensions	Предназначен для формирования записей в блоке «Журнал обмена»
20.	Сервис отправки почтовых уведомлений/Notification Service	Предназначен для рассылки пользователям системы почтовых сообщений об операциях, выполняемых с карточками системы, и сообщений о необходимости выполнения определенных заданий
21.	Сервис периодических задач/Scheduled Job Launcher	Предназначен для автоматизации выполнения периодических или отложенных операций над объектами Системами. Особенности выполняемых операций определяется устанавливаемыми плагинами (расширениями). Сервис обеспечивает запуск плагинов с указанной при настройке периодичностью
22.	Модуль ИИ авторосписи документов	Модуль Искусственного интеллекта Системы электронного документооборота Министерства экономического развития Российской Федерации, использующего искусственный интеллект в задачах документооборота

3.4.2 Перечень частей программного обеспечения

Программное обеспечение Системы включает:

- общее программное обеспечение (далее – ОПО);
- специальное программное обеспечение (далее – СПО);
- ПО автоматизированных рабочих мест пользователей.

ОПО Системы обеспечивает:

- штатное функционирование комплекса технических средств Системы;
- функционирование СПО;
- взаимодействие с периферийными устройствами;
- сетевое взаимодействие;
- другие необходимые общесистемные функции.

Перечень ОПО Системы представлен в Таблице 4.

Таблица 4 – Перечень ОПО и СПО Системы

Сервер	Программное обеспечение
Продуктивная зона	

Сервер	Программное обеспечение
Сегмент закрытого контура	
Сервер СУБД	Astra Linux 1.7 Docker 24.0.2 PostgreSQL 12.16
Сервер кворум etcd	Astra Linux 1.7 Docker 24.0.2
Сервер бэкапов	Astra Linux 1.7 Docker 24.0.2 PostgreSQL 12.16
Сервер приложений – платформа Docsvision 5 Core ЕСМ и модули СДУ «Приоритет»	Astra Linux 1.7 Docker 24.0.2 Sdu astra 90 (Вся функциональность сервера приложений СДУ с серверными расширениями, установочными скриптами БД и настроенным КриптоПро CSP) Reportingsite-astra 5.0.2026.19 (Сайт для расширенных отчетов) Reportingservice-astra 5.0.2026.19 (Сервис для расширенных отчетов)
Сервер веб-приложений – Тонкий клиент	Astra Linux 1.7 Docker 24.0.2 Ddmweb-ui-astra 5.20.20.0 (Клиентская часть Тонкого клиента) Ddmweb-api-astra 5.20.20.0 (REST API сервис Тонкого клиента) Ddmwebadmin-ui-astra 5.20.20.0 (Административная часть Тонкого клиента) Entityextractor-astra 1.0.16.1
Сервер сервисов	Astra Linux 1.7 Docker 24.0.2 Scheduledjoblauncher-astra 5.0.2028.26 (Сервис периодических задач) Notificationsender-astra 2.0.30.5 (Сервис отправки уведомлений)
Сервер предпросмотра	Astra Linux 1.7 Docker 24.0.2 R7Office 7.4.0.112
Сервер конвертации	Astra Linux 1.7 Docker 24.0.2 Conversion-service-astra 5.5.0.65 (Сервис конвертации в PDF) R7Office 7.4.0.112
Сервер интеллектуального поиска	Astra Linux 1.7 Docker 24.0.2 Elasticsearch 7.15 (утилита для поиска и анализа данных в БД) elasticsearch-analysis-morphology 7.15 ingest-attachment 7.15 Java (open jdk) 1.8 Cerebro 0.9.2 (инструмент администрирования Elasticsearch)
Сервер координатор интеллектуального поиска	Astra Linux 1.7 Docker 24.0.2 Elasticsearch 7.15 (утилита для поиска и анализа данных в БД) elasticsearch-analysis-morphology 7.15 ingest-attachment 7.15 Java (open jdk) 1.8 Cerebro 0.9.2 (инструмент администрирования Elasticsearch)
Сервер синхронизации АРМ	Astra Linux 1.7 Docker 24.0.2 Сруптопро-проху (Проксирующий сервер для SSL с шифрованием по ГОСТ алгоритмам)

Сервер	Программное обеспечение
	Synchronizationservice-astra 5.27.0.180 (Сервис синхронизации) Rsa-proxy-astra 19 (Проксирующий сервер для SSL RSA)
Балансировщик серверных узлов	Astra Linux 1.7 Docker 24.0.2 Naproxy 2.4.24 KeepAlived 2.0.19
Сервер распределенного кэша	Astra Linux 1.7 Docker 24.0.2 Redis 6.2.6
Сервер файлового хранилища	Astra Linux 1.7 NFS v4
Сервер управления	Astra Linux 1.7 Docker 24.0.2
Сервер интеграций	Astra Linux 1.7 Docker 24.0.2
Сегмент открытого контура	
Сервер push-уведомлений	Astra Linux 1.7 Docker 24.0.2 Proxyservice 5.26.0.154 (Прокси-сервис сервиса синхронизации)
Балансировщик серверных узлов	Astra Linux 1.7 Docker 24.0.2 Naproxy 2.4.24 KeepAlived 2.0.19
Сервер управления	Astra Linux 1.7 Docker 24.0.2
Предпродуктивная зона	
Сегмент закрытого контура	
Сервер СУБД	Astra Linux 1.7 Docker 24.0.2 PostgreSQL 12.16
Сервер приложений – платформа Docsvision 5 Core ЕСМ и модули СДУ «Приоритет»	Astra Linux 1.7 Docker 24.0.2 Sdu astra 90 (Вся функциональность сервера приложений СДУ с серверными расширениями, установочными скриптами БД и настроенным КриптоПро CSP) Reportingsite-astra 5.0.2026.19 (Сайт для расширенных отчетов) Reportingservice-astra 5.0.2026.19 (Сервис для расширенных отчетов)
Сервер веб-приложений – Тонкий клиент	Astra Linux 1.7 Docker 24.0.2 Ddmweb-ui-astra 5.20.20.0 (Клиентская часть Тонкого клиента) Ddmweb-api-astra 5.20.20.0 (REST API сервис Тонкого клиента) Ddmwebadmin-ui-astra 5.20.20.0 (Административная часть Тонкого клиента) Entityextractor-astra 1.0.16.1
Сервер сервисов	Astra Linux 1.7 Docker 24.0.2 Scheduledjoblauncher-astra 5.0.2028.26 (Сервис периодических задач) Notificationsender-astra 2.0.30.5 (Сервис отправки уведомлений)

Сервер	Программное обеспечение
Сервер предпросмотра	Astra Linux 1.7 Docker 24.0.2 R7Office 7.4.0.112
Сервер конвертации	Astra Linux 1.7 Docker 24.0.2 Conversion-service-astra 5.5.0.65 (Сервис конвертации в PDF) R7Office 7.4.0.112
Балансировщик серверных узлов	Astra Linux 1.7 Docker 24.0.2 Haproxy 2.4.24 KeepAlived 2.4.24
Сервер распределенного кэша	Astra Linux 1.7 Docker 24.0.2 Redis 6.2.6
Сервер интеллектуального поиска	Astra Linux 1.7 Docker 24.0.2 Elasticsearch 7.15 elasticsearch-analysis-morphology 7.15 ingest-attachment 7.15 Java (open jdk) 1.8 Cerebro 0.9.2
Сервер управления	Astra Linux 1.7 Docker 24.0.2 Ansible 2.13
Сервер интеграций	Astra Linux 1.7 Docker 24.0.2
Сервер синхронизации АРМ	Astra Linux 1.7 Docker 24.0.2 Cryptopro-проху (Проксирующий сервер для SSL с шифрованием по ГОСТ алгоритмам) Synchronizationservice-astra 5.27.0.180 (Сервис синхронизации) Rsa-proxy-astra 19 (Проксирующий сервер для SSL RSA)
Сервер машинного обучения	Astra Linux 1.7 Docker 24.0.2
Сегмент открытого контура	
Балансировщик серверных узлов	Astra Linux 1.7 Docker 24.0.2 Haproxy 2.4.24 KeepAlived 2.4.24
Сервер push-уведомлений	Astra Linux 1.7 Docker 24.0.2 Cryptopro-проху (Проксирующий сервер для SSL с шифрованием по ГОСТ алгоритмам)
Сервер управления	Astra Linux 1.7 Docker 24.0.2 Ansible 2.13

Сервер	Программное обеспечение
Сервер мониторинга	Alpine Linux 3.16.1 Zabbix-alpine 6.0.7
Клиентские рабочие места для работы с веб-клиентом	Астра Линукс 1.7 и выше/ Windows 10 или выше; Р7-Офис / Microsoft Office 2016 или выше; КриптоПро CSP 4.0 R4 для Windows / КриптоПро CSP 5.0; Веб-браузер: Яндекс браузер версии 24.x и выше

СПО Системы устанавливается на сервер приложений и взаимодействует со всеми компонентами Системы.

СПО предназначено для решения поставленных задач Пользователя, реализации функций разрабатываемых подсистем и разработано с учетом характеристик ОПО объекта автоматизации и особенностей автоматизируемых процессов.

СПО отвечает следующим требованиям:

- высокая степень готовности для решения поставленных задач;
- совместимость программных продуктов в части используемых технических средств, общего программного обеспечения и общесистемной инфраструктуры в пределах требований к техническому обеспечению, а также их информационная совместимость в пределах требований к информационному обмену;
- наличие эксплуатационной документации на русском языке.

3.5 Взаимодействие с внешними информационными системами

Система осуществляет информационное взаимодействие со следующими информационными системами:

1. Система межведомственного электронного документооборота (МЭДО): двусторонний обмен данными в части получения и отправки электронных документов, а также уведомлений о ключевых этапах их обработки;
2. Единое цифровое окно обратной связи (Платформа обратной связи) федеральной государственной информационной системы «Единый портал государственных и муниципальных услуг (функций)» (ПОС): двусторонний обмен в части получения данных по обращениям граждан, отправки ответов на них и статусов их рассмотрения. Обмен данными с ПОС осуществляется посредством системы межведомственного электронного взаимодействия (СМЭВ);
3. Коммутационная платформа сетевого справочного телефонного узла (ССТУ.РФ): отправка данных о результатах рассмотрения обращений граждан;

4. Интеграция с Официальным сайтом Минэкономразвития Российской Федерации:
односторонний обмен в части передачи информации по статусам обработки
обращений граждан.

4 Требования к работам

Проектные решения Системы должны отвечать требованиям действующего законодательства Российской Федерации по патентной чистоте.

В целях обеспечения модульности Системы и снижения затрат на её интеграцию и эксплуатацию взаимодействие подсистем Системы должно строиться на основе общепринятых открытых технологических стандартов.

Все доработки, произведенные в результате развития Системы, должны быть размещены в ОЦОД ПК и не противоречить требованиям положений ТУ ИС ФОИВ ОЦОД ПК.

4.1 Требование к передаче прав и уровней доступа к Системе

В течение 5 (пяти) рабочих дней с начала выполнения работ за 1 отчетный период Исполнитель обязан получить на территории Заказчика необходимые атрибуты доступа (логин и пароль) к ОЦОД ПК и необходимые атрибуты доступа к действующей версии Системы: параметры подключения к серверам, параметры доступа к экземпляру Системы, находящейся в эксплуатации.

После получения атрибутов и параметров доступа Исполнитель в течение 1 (одного) рабочего дня обязан произвести изменение атрибутов доступа.

В течение 5 (пяти) рабочих дней с начала выполнения работ за 1 отчетный период Исполнитель обязан определить ответственных лиц, для которых предполагается удаленный доступ к инфраструктуре Заказчика, направить перечень ответственных лиц Заказчику.

Исполнитель не должен разглашать и использовать в своих целях информацию (без разрешения Заказчика), которая может стать ему известной в ходе выполнения работ, а также не должен передавать информацию третьим лицам без письменного разрешения Заказчика.

Исполнитель обязан использовать доступ к информационным ресурсам Заказчика только в целях выполнения работ и не распространять в любой форме любые материалы, содержащиеся на серверах и прочих средствах хранения информации Заказчика. Исполнитель несет ответственность за соблюдение данных требований в соответствии с законодательством Российской Федерации.

4.2 Численность, квалификация персонала и режим его работы

Численность персонала и необходимый уровень квалификации определяется Исполнителем таким образом, чтобы обеспечить выполнение требований к выполнению работ, указанных в настоящем ТЗ.

Исполнитель в течение 5 (пяти) рабочих дней с начала выполнения работ направляет Заказчику информацию о представителе (представителях) Исполнителя, ответственном за организацию информационной безопасности, разработку программного обеспечения, администрирование, тестирование Системы, предоставление аналитики и иных штатных и (или) привлекаемых специалистах, задействованных в реализации соответствующих процессов, предусмотренных ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

Режим работы персонала должен соответствовать действующему законодательству Российской Федерации и обеспечить выполнение работ Исполнителем в соответствии с требованиями к качеству, режиму и периодичности выполнения работ, определенными настоящим ТЗ.

Заказчик вправе запросить заверенные копии документов, подтверждающих квалификацию персонала, в том числе дипломов, протоколов подготовки специалистов, и провести проверку соответствия заявленных в них сведений фактическим в отношении всех или отдельных работников Исполнителя.

4.3 Требования к характеристикам взаимосвязей Системы со смежными системами, требованиям к ее совместимости

Взаимодействие с внешними системами должно осуществляться с помощью интеграционных модулей или веб-сервисов путем обмена структурированными файлами в специализированных форматах.

Информационное взаимодействие СЭДО с внешними системами должно осуществляться только при наличии технических возможностей по взаимодействию с интегрируемыми системами.

Перечень внешних информационных систем, с которыми интегрирована СЭДО, приведен в п.3.5.

4.4 Требования к информационной безопасности

Каждое средство защиты информации, поставляемое в составе общесистемного и специального программного обеспечения (ОПО и СПО) в рамках работ по развитию Системы, а также СЗИ, уже присутствующее в текущей версии Системы (независимо от того, изменяется ли соответствующий компонент Системы (подсистема, модуль, функция) в рамках Контракта), должно иметь действующий сертификат соответствия ФСТЭК России и/или ФСБ России на встроенные функции защиты информации на момент поставки и в течение всего гарантийного срока по Контракту. Исполнитель или фирма-производитель ПО обязаны

обеспечивать официальную техническую поддержку СЗИ до окончания гарантийного срока, включая выпуск обновлений для устранения уязвимостей, критических обновлений безопасности и бюллетеней по безопасности. Прекращение поддержки или истечение срока сертификата ранее указанных сроков не допускается, за исключением замены СЗИ на равноценное с действующим сертификатом. В случае выявления в ходе выполнения работ по развитию Системы СЗИ, не имеющего действующего сертификата (в том числе в компонентах Системы, не затрагиваемых развитием), Исполнитель обязан предоставить Заказчику план приведения таких СЗИ в соответствие требованиям ФСТЭК России и/или ФСБ России (замена, модернизация, изоляция с компенсирующими мерами).

В случае выявления Исполнителем необходимости при развитии Системы использовать средства защиты информации сторонних фирм-производителей, то все используемое ОПО и СПО должно иметь совместимость с данными средствами защиты информации сторонних фирм-производителей.

В случае выявления Исполнителем необходимости при развитии Системы использовать шифровальные (криптографические) средств защиты информации (далее – СКЗИ), Исполнитель должен обеспечить неукоснительное соблюдение требований формуляров на СКЗИ, в частности, на требование, касающееся проведения оценки влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований. Проведение работ по оценке влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований является обязательным условием действия сертификата на СКЗИ, в соответствии с которым СКЗИ обеспечивает заданный уровень информационной безопасности при выполнении требований эксплуатационной документации согласно формуляру на СКЗИ.

В соответствии с Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утвержденным приказом ФСБ России от 9 февраля 2005 г. № 66 (далее – Положение ПКЗ-2005), оценка влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований осуществляется Исполнителем совместно со специализированной организацией. Результаты исследований оценки влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к ним требований, а также опытные образцы СКЗИ и аппаратные, программно-аппаратные и программные средства, необходимые для штатного

функционирования СКЗИ, передаются в ФСБ России для проведения экспертизы, по итогам которой утверждается заключение ФСБ России по результатам оценки влияния.

В случае применения Исполнителем при развитии Системы СКЗИ, не имеющего положительного заключения ФСБ России по результатам оценки влияния аппаратных, программно-аппаратных и программных средств, если такое требование установлено в формуляре на это СКЗИ, приводит к нарушению п. 46 Положения ПКЗ-2005 и влечет за собой административную ответственность операторов персональных данных, предусмотренную ч. 6 ст. 13.12. Кодекса Российской Федерации об административных правонарушениях.

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

Развитие Системы должно осуществляться на базе программного обеспечения, соответствующего требованиям законодательства Российской Федерации, приведенного в ТЗ, в том числе на предмет обеспечения соответствующего уровня защиты в отношении персональных данных по согласованию с Заказчиком.

Исполнитель в рамках выполнения работ должен провести проверку развернутой версии Системы на наличие уязвимостей программного обеспечения с использованием программного обеспечения представленного на официальном сайте ФСТЭК России по адресу в сети Интернет: <https://bdu.fstec.ru/scanoval> и/или <https://bdu.fstec.ru/scanovalforlinux>, а в случае невозможности применения иного программного обеспечения, указанного в Государственном реестре сертифицированных средств защиты и направляет результаты проверки Заказчику с приложением плана по устранению выявленных уязвимостей (далее – проверка на наличие уязвимостей программного обеспечения). В случае невозможности проведения проверки на наличие уязвимостей программного обеспечения Системы указанным выше программным обеспечением, при наличии действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации Исполнитель в соответствии с подпунктом «б» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79 направляет соответствующее заключение

от своего имени, либо от субподрядной организации, имеющей указанную лицензию.

Порядок оценки уровня критичности уязвимостей программных, программно-аппаратных средств и принятие мер защиты информации, направленных на устранение уязвимостей, определяется в соответствии с Методикой оценки уровня критичности

уязвимостей программных, программно-аппаратных средств (утв. Федеральной службой по техническому и экспортному контролю 30 июня 2025 г.).

Результаты проверки на наличие уязвимостей программного обеспечения должны быть представлены в виде Отчета о проведении проверки на наличие уязвимостей программного обеспечения, включающего в себя отчет, полученный в результате работы программного обеспечения для автоматизированных проверок на наличие уязвимостей, либо заключение в соответствии с подпунктом «б» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

После выполнения проверок на наличие уязвимостей программного обеспечения Системы Исполнитель должен определить перечень уязвимостей, для устранения которых требуется доработка СПО Системы. Соответствующие требования к доработке СПО Системы, необходимые для устранения уязвимостей, должны быть включены в ЧТЗ на развитие Системы и (при необходимости) в ЧТЗ на СЗИ.

Все выполняемые работы в части информационной безопасности должны осуществляться с учетом положений Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», приказа ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», Приказа ФСБ России от 22 августа 2026 г. № 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. N 149-ФЗ «Об информации, информационных технологиях и о защите информации" с использованием шифровальных (криптографических) средств», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Методики испытаний систем защиты информации информационных систем методами тестирования на проникновение, утв. ФСТЭК России 25 июня 2025 г., Методики анализа защищенности информационных

систем, утвержден ФСТЭК России 25 ноября 2025 г., и иных указаний ФСТЭК России и(или) ФСБ России о мерах по повышению защищенности информационной инфраструктуры Российской Федерации. В случае, если указанные документы утратят силу в период исполнения Контракта, необходимо руководствоваться действующими документами, принятыми взамен утративших силу.

В течение 15 (пятнадцати) календарных дней (включительно) с начала выполнения работ за 1 отчетный период Исполнитель обязан:

- определить ответственных лиц, ответственных за обеспечение информационной безопасности, имеющее квалификацию, позволяющую реализовывать требования безопасности информации.

- определить ответственных лиц, для которых предполагается удаленный доступ к информационной инфраструктуре, согласовать с Заказчиком состав ответственных лиц и количество учетных записей, с которых предполагается удаленный доступ к информационной инфраструктуре;

- организовать для ответственных лиц выделение автоматизированных рабочих мест:

- не имеющих сторонних подключений;
- не использующихся в личных целях;
- к которым применяются корпоративные меры по информационной безопасности Исполнителя;
- с установленными на них сертифицированными средствами защиты информации, реализующими аутентификацию и идентификацию Пользователей, а также антивирусную защиту.

- согласовать с Заказчиком перечень IP-адресов, с которых может осуществляться подключение работников Исполнителя и отразить информацию в перечне ответственных лиц, в т. ч. лиц, для которых предполагается удаленный доступ к инфраструктуре, и информация об их рабочих местах;

- предоставить Заказчику актуальный документ «Перечень ответственных лиц, в том числе лиц, для которых предполагается удаленный доступ к инфраструктуре и информация об их рабочих местах»;

- предоставить Заказчику политику информационной безопасности Исполнителя, результаты внутренних (внешних) аудитов информационной безопасности, результаты тестирования на проникновение инфраструктуры Исполнителя, план реагирования на компьютерные инциденты, а также регламент действий работников Исполнителя в случае нештатных ситуаций (при наличии);

– предоставить Заказчику рассчитанный показатель защищенности инфраструктуры Исполнителя, в том числе значения частных показателей безопасности (по форме в соответствии с Приложением А к настоящему ТЗ), с подтверждающими документами и материалами, на основании которых показателю присваивается значение, в соответствии с методическим документом «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденным ФСТЭК России 11 ноября 2025 года.

В случае изменения состава указанных ответственных лиц Исполнитель обязан уведомлять Заказчика о фактах таких изменений в течение 1 рабочего дня.

Исполнитель несет ответственность в соответствии с действующим законодательством Российской Федерации за реализацию угроз безопасности при удаленном доступе к Системе с использованием средств криптографической защиты информации и/или учетных записей, предоставленных работникам Исполнителя.

Исполнитель должен обеспечивать защиту информации, обрабатываемую в Системе, в целях:

а) недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения конфиденциальности, целостности, доступности информации (далее - нарушение безопасности информации);

б) недопущения (снижения возможности) наступления негативных последствий (событий) от нарушения функционирования информационных систем вследствие реализации (возникновения) угроз безопасности информации.

Исполнитель обязан при выполнении работ на развитие руководствоваться утвержденной Заказчиком политикой защиты информации, а также утвержденными Заказчиком внутренними регламентами по защите информации.

Исполнитель обязан исключить использование программного обеспечения для удаленного управления собственными автоматизированными рабочими местами Исполнителя (например, TeamViewer, AnyDesk, AmmyAdmin, AeroAdmin, Radmin, LiteManager, Удаленный рабочий стол Chrome, Microsoft Remote Assistance, Microsoft Remote Desktop и аналогичное схожим функционалом ПО).

Исполнителем во взаимодействии с Заказчиком в указанный 15-дневный срок должны быть определены каналы для оперативного взаимодействия (в том числе резервные каналы взаимодействия) ответственных лиц по обеспечению информационной безопасности со стороны Исполнителя и Заказчика, а также порядок такого взаимодействия. Для

оперативного взаимодействия с Заказчиком должны использоваться не персонализированные, а официальные каналы взаимодействия.

До начала выполнения работ Исполнитель обязан реализовать следующие базовые меры по информационной безопасности в собственной ИТ – инфраструктуре (инструментам и оборудованию Исполнителя, применяемому для выполнения работ), результаты которых указать в Декларации о выполнении указанных мер и мероприятий по защите информации в ИТ-инфраструктуре Исполнителя:

- 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;
- обеспечение процесса управления уязвимостями;
- 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), цифры (0-9), специальные символы (~!@#\$%^&*()-+_=}{[]'>?/\)), в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов). Запретить использование комбинаций соседних клавиш и словарных слов. Пароли от учетных записей на разных сервисах должны отличаться. Пароли от учетной записи Исполнителя и учетной записи заказчика должны отличаться). Не использовать пароли «по умолчанию» (запретить использование комбинаций, которые присутствуют в предустановленных списках стандартных паролей производителей; указаны в документации к ПО как заводские; входят в топ-N наиболее часто используемых паролей. Система должна блокировать установку таких паролей на этапе создания/смены).

При выполнении работ и при информационном взаимодействии в ходе выполнения работ Исполнитель обязан использовать электронные почтовые сервисы, инфраструктура которых полностью расположена на территории Российской Федерации.

Исполнитель обязан уведомлять Заказчика о наступлении в своей инфраструктуре (непосредственно задействованной в выполнении работ по настоящему ТЗ) компьютерных инцидентов.

Исполнителем должна вестись запись всех действий работников Исполнителя (событий) на АРМ Исполнителя при осуществлении удаленного подключения к инфраструктуре Заказчика со сроком хранения журналов событий не менее 1 года. В случае возникновения инцидента информационной безопасности в собственной ИТ-инфраструктуре

Исполнителя, Исполнитель обязан предоставлять указанные журналы событий Заказчику. Состав передаваемой информации в журналах должен быть определен Исполнителем в своей инфраструктуре (ГОСТ Р 59709-59712 2022 г.).

Подключения работников Исполнителя к инфраструктуре Заказчика должны осуществляться в периоды установленного рабочего времени Заказчика. В случае необходимости доступа к инфраструктуре Заказчика в периоды вне рабочего времени такие подключения должны быть согласованы с Заказчиком.

Удаленный сетевой доступ должен осуществляться с применением средств криптографической защиты информации, при этом обмен ключами шифрования необходимо осуществлять по алгоритмам, исключающим их раскрытие сторонним лицам. Маршруты сетевого трафика не должны проходить по сторонним сетям в незашифрованном виде.

Система оснащена сертифицированными средствами защиты и должна эксплуатироваться в соответствии с требованиями по информационной безопасности, указанными в аттестате соответствия, внутренними стандартами, требованиями по безопасности информации, требованиями к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы, определяемыми производителями средств защиты информации, внутренними регламентами Заказчика и Оператора ОЦОД ПК, где размещена Система.

При реализации функций по защите информации должны использоваться:

- встроенные средства защиты информации: возможности и механизмы защиты информации, предоставляемые операционными системами, системами управления базами данных и приложениями;
- иные средства защиты информации: программные, программно-технические средства, предназначенные для выполнения требований по безопасности информации, не реализуемые встроенными средствами защиты информации.

Применяемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации Российской Федерации. Классы защиты и уровни доверия применяемых при развитии Системы сертифицированных средств защиты информации и средств криптографической защиты информации должны соответствовать классу защищенности Системы.

Не допускается применение СрЗИ, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

В случае, если в ходе исполнения настоящего Контракта в адрес Заказчика поступит решение ФСБ России (или ФСТЭК России) о необходимости осуществления организационных и технических мер, связанных с обеспечением информационной безопасности, Заказчик совместно с Исполнителем должны определить, затрагивают ли указанные меры развиваемую Систему, и в случае, если затрагивают – разработать и согласовать план мероприятий по выполнению указанных мер (в части развиваемой Системы и в пределах компетенций и ответственности Заказчика и Исполнителя), с указанием сроков реализации мер и ответственных (Заказчик или Исполнитель). К компетенции Исполнителя относятся вопросы, связанные с дорабатываемым программным обеспечением Системы, включая вопросы интеграционного взаимодействия с внешними системами.

Требования к СЗИ должны определяться в зависимости от класса защищенности и актуальных угроз безопасности информации, включенных в модель угроз безопасности информации Системы. Указанные требования включаются в ЧТЗ на СЗИ с учетом требований нормативной правовой базы в области защиты информации государственных информационных систем.

Программное обеспечение Системы должно разрабатываться Исполнителем с учетом ГОСТ Р 56939-2024. «Защита информации. Разработка безопасного программного обеспечения. Общие требования», ГОСТ Р 71207–2024. «Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования», ГОСТ Р 58412-2019. «Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке безопасного программного обеспечения» и по согласованию с Заказчиком.

Выполняемые работы в части защиты информации должны осуществляться с учетом положений Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

При возникновении необходимости выполнения работ в части обеспечения защиты информации, требующих наличия лицензий, Исполнитель обязан предоставить Заказчику копии действующих лицензий Исполнителя либо субподрядной организации в случае ее привлечения (в случае выполнения работ в области информационной безопасности, требующих наличия такой лицензии):

– лицензия ФСБ России, дающая право на осуществление работ, предусмотренных пунктами 13, 28 Перечня выполняемых работ, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению о лицензировании деятельности по разработке, производству, распространению шифровальных(криптографических) средств, информационных систем

и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 (далее – Перечень):

на осуществление работ в соответствии с пунктом 13 Перечня. Монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем;

на осуществление работ в соответствии с пунктом 28 Перечня. Изготовление и распределение ключевых документов и (или) исходной ключевой информации для выработки ключевых документов с использованием аппаратных, программных и программно-аппаратных средств, систем и комплексов изготовления и распределения ключевых документов для шифровальных (криптографических) средств.

– лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации на работы и услуги, предусмотренные подпунктами «б», «в», «д» и «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79:

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

услуги по мониторингу информационной безопасности средств и систем информатизации (подпункт «в»);

работы и услуги по проектированию в защищенном исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений (подпункт «д»);

услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации,

защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации) (подпункт «е»).

4.5 Требования к Системе в целом

4.5.1 Требования к показателям назначения

Система должна отвечать требованиям обеспечения показателей назначения, представленным в Таблице 5.

Таблица 5 – Показатели назначения

Операция	Максимальное время выполнения
Открытие главной страницы Веб-клиента (время аутентификации)	3 секунды
Открытие регистрационной карточки документа (отрисовка первого элемента карточки)	2 секунды
Открытие карточки задания	2 секунды
Открытие формы создания резолюции	2 секунды
Исполнение задания с предварительно подготовленным отчетом об исполнении	2 секунды
Создание регистрационной карточки	5 секунд
Создание резолюции	2 секунды
Утверждение резолюции (5 исполнителей)	4 секунды
Предпросмотр файлов PDF не более 10 Мб	3 секунды
Запуск маршрута согласования (5 согласующих)	5 секунд

4.5.2 Требования к надежности

СЭДО должна обеспечивать возможность бесперебойной работы пользователей 7 дней в неделю и оперативное восстановление работоспособности при возникновении сбоев, аварий и отказов. Уровень доступности Системы должен быть не менее 99,7%.

Система должна функционировать непрерывно в круглосуточном режиме 365 дней в году. Допускается временное ограничение полнофункциональной доступности отдельных частей подсистем Системы:

- в периоды выполнения регламентированных работ по обслуживанию аппаратных и программных средств Системы, предусмотренных эксплуатационной документацией;

- как результат возникновения внештатных ситуаций, вызванных отказами в работе аппаратных или программных средств Системы;
- в случае частичной или полной потери работоспособности внешних информационных систем-поставщиков первичной информации для Системы;
- во время перехода с одной версии на другую системного или прикладного программного обеспечения Системы.

Надежность СЭДО должна достигаться путем принятия организационных и технических мер, обеспечивающих требуемые уровни доступности и надежности.

Технические меры по обеспечению надежности должны предусматривать:

- резервирование критически важных компонентов и данных СЭДО;
- использование технических средств с избыточными компонентами и возможностью их замены без выключения питания и остановки работы;
- использование программного резервирования (программной избыточности);
- конфигурирование используемых средств и применение ПО, обеспечивающего высокую надежность.

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

- обеспечения требуемого уровня квалификации пользователей;
- обеспечения требуемого уровня квалификации обслуживающего персонала;
- регламентации и нормативного обеспечения выполнения работ обслуживающего персонала и пользователей;
- своевременного оповещения пользователей о случаях нештатной работы компонентов СЭДО;
- своевременной диагностики неисправностей.

4.5.3 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов

Система должна быть рассчитана на эксплуатацию в соответствии с требованиями к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы, определяемыми внутренними регламентами Оператора ОЦОД ПК.

Техническая и физическая защита аппаратных компонентов Системы, носителей данных, бесперебойное энергоснабжение, резервирование ресурсов, создание резервных

копий и текущее техническое обслуживание реализуется техническими и организационными средствами, предусмотренными в ИТ-инфраструктуре Заказчика.

Для нормальной эксплуатации Системы должно быть обеспечено бесперебойное питание технических средств, на которых функционирует серверная часть Системы.

Эксплуатация Системы должна быть организована Заказчиком и осуществляться в соответствии с «Требованиями к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации», утвержденными постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676.

4.5.4 Требования к режимам функционирования

Функционирование Системы должно предусматривать следующие режимы:

1. Штатный режим: непрерывная круглосуточная работа. В штатном режиме все основные операции по текущей настройке и обслуживанию Системы выполняются без приостановки действия Системы. Переход Системы в этот режим должен происходить автоматически при первоначальном запуске Системы в эксплуатацию или по завершении других режимов.

Выход из этого режима должен происходить:

- в режим технического обслуживания – вручную по команде администратора Системы;
- в аварийный режим – автоматически.

2. Технического обслуживания (сервисный): прекращение доступа пользователей к Системе для выполнения технических работ, обслуживания, реконфигурации Системы. При переходе в режим технического обслуживания Система завершает обработку данных без нарушения их целостности и сохраняет свое текущее состояние. Переход в этот режим должен происходить по команде администратора Системы из штатного или аварийного режима эксплуатации.

Выход из этого режима должен происходить автоматически при завершении запланированных операций;

3. Аварийный режим работы – данный режим предполагает полное или частичное ограничение полнофункциональной доступности Системы, явившееся следствием отказа аппаратно-программных средств, обеспечивающих их функционирование. Переход Системы в этот режим должен происходить автоматически.

Выход из этого режима должен происходить:

– автоматически при устранении причины отказа;
вручную по команде администратора Системы в режим технического обслуживания с целью устранения отказа.

4.5.5 Требования по сохранности информации при авариях

Специалистами, осуществляющими техническую поддержку СЭДО, должна быть обеспечена защита данных СЭДО от утраты или нарушения целостности в следующих случаях:

при сбоях в электропитании серверного оборудования: средствами СУБД, обеспечивающей сохранность данных в состоянии на момент последней завершенной транзакции;

при авариях, приведших к невозможности восстановления данных с сервера СУБД: использованием процедур резервного копирования баз данных СЭДО и хранения резервных копий на съемном носителе.

Требования к настройкам системы резервного копирования, охват компонентов СЭДО, глубина отката и параметры резервного копирования устанавливаются в рамках соответствующего государственного контракта на техническую поддержку СЭДО, а также зависят от регламентов резервного копирования организации, в инфраструктуре которой размещена серверная часть СЭДО.

В СЭДО специалистами, осуществляющими техническую поддержку СЭДО, должна предусматриваться возможность ручного восстановления обрабатываемой информации из резервной копии в следующих аварийных ситуациях:

физический выход из строя дисковых накопителей;
ошибочные действия обслуживающего персонала.

В СЭДО специалистами, осуществляющими техническую поддержку СЭДО, должно предусматриваться автоматическое восстановление работоспособности серверной части СЭДО в следующих ситуациях:

штатное и аварийное отключение электропитания серверной части;
штатная перезагрузка СЭДО и загрузка после отключения;
программный сбой системного ПО, приведший к перезагрузке СЭДО.

В СЭДО специалистами, осуществляющими техническую поддержку СЭДО, должно предусматриваться полуавтоматическое восстановление работоспособности серверной части СЭДО в следующих аварийных ситуациях:

физический выход из строя любого аппаратного компонента, кроме дисковых накопителей: после замены компонента и восстановления конфигурации системного ПО;

аварийная перезагрузка СЭДО, приведшая к не фатальному (исправимому) нарушению целостности файловой системы: после восстановления файловой системы.

4.5.6 Требования к эргономике и технической эстетике

Взаимодействие пользователей с СЭДО должно осуществляться посредством визуального графического интерфейса: ввод и вывод данных Системы, прием управляющих команд и отображение результатов их исполнения должны выполняться в интерактивном режиме.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», управление функциональностью должно осуществляться с помощью набора экранных меню, кнопок, значков, имеющих однозначную интерпретацию визуализации. Клавиатурный режим ввода должен использоваться при заполнении и/или редактировании значений полей экранных форм.

Расположение надписей, элементов управления, ввода и просмотра данных должно быть логичным и интуитивно понятным.

Надписи экранных форм, а также сообщения, выдаваемые пользователям СЭДО (кроме служебных системных сообщений), должны быть на русском языке.

СЭДО должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. При этом СЭДО должна выдавать пользователям соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

4.5.7 Требования к информационному обмену между компонентами Системы

Информационный обмен между компонентами Системы и клиентскими приложениями должен осуществляться по локальной сети и по сети «Интернет».

4.5.8 Требования к патентной чистоте

Патентная чистота СЭДО и ее подсистем должна быть обеспечена в отношении патентов, действующих на территории Российской Федерации.

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

Работы, выполняемые Исполнителем в рамках работ по развитию СЭДО, не должны включать в себя действия по модификации (переработке) прикладного программного обеспечения СЭДО. При выполнении работ не должно создаваться новых результатов интеллектуальной деятельности, в том числе программ для ЭВМ.

4.5.9 Требования по стандартизации и унификации

Экранные формы Системы должны проектироваться с учетом требований унификации:

- проводимые работы должны соответствовать требованиям выбора применяемых решений. Преимущество должно отдаваться решениям, основанным на стандартизированных технологиях, т.е. прошедшим процедуру стандартизации и утвержденным в качестве стандарта либо рекомендации каким-либо признанным международным, федеральным, отраслевым, промышленным органом по стандартизации.
- термины, используемые для обозначения типовых операций, а также последовательности действий пользователя, при их выполнении, должны быть унифицированы;
- внешнее поведение сходных элементов интерфейса должно быть реализовано одинаково для однотипных элементов.

4.6 Требования к видам обеспечений

4.6.1 Требования к организационному обеспечению

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

- решения административных вопросов (организация удаленных конференций, предоставление допусков, рассмотрение и согласование документации и т. п.);
- решения инженерно-технических вопросов (согласование технических аспектов реализации и администрирования Системы, определение наличия и размещения технических средств, коммуникаций и т.п.);
- нормативно-методического и информационного обеспечения работ (уточнение функциональных характеристик, предоставление дополнительных сведений).

4.6.2 Требования к методическому обеспечению

Методическое обеспечение включает в себя ознакомление сотрудников Исполнителя с комплектом проектной и рабочей (эксплуатационной) документацией на Систему и другими материалами, связанными с выполнением работ (запрашиваемых Исполнителем и предоставляемых Заказчиком в рабочем порядке).

4.6.3 Требования к лингвистическому обеспечению

Все экранные формы, выходные формы и вся документация разрабатываемая и (или) актуализируемая в рамках настоящих работ должны быть выполнены на русском языке. Исключения могут составлять только системные сообщения Системы не подлежащие русификации и сведения о таких сообщениях, описанные в документации. Набор символов – кириллица. Цифровая информация должна быть отражена арабскими цифрами.

4.6.4 Требования к программному обеспечению

Программное обеспечение СЭДО должно отвечать следующим требованиям:

обеспечивать совместимость программных продуктов в части используемых технических средств, системного программного обеспечения и общесистемной инфраструктуры в пределах требований к техническому обеспечению, а также их информационную совместимость в пределах требований к информационному обмену при размещении в ОЦОД;

Веб-клиент Системы должен функционировать в интернет-браузере Яндекс.Браузер версии 24 и выше;

серверная часть должна функционировать на основе операционных систем, включенных в Реестр отечественного ПО.

4.7 Требования к функциям (задачам) по развитию Системы

По итогам развития Система должна функционировать в соответствии с требованиями к развитию, приведенными в разделе 4.7., без утраты существующего функционала Системы, не затрагиваемого требованиями настоящего ТЗ в части Веб-клиента.

4.7.1 Требования к развитию (адаптации) функционала модуля МЭДО в части обмена данными с глобальным адресным справочником (ГАС)

Исполнитель должен реализовать взаимодействие со справочником ГАС в части обеспечения взаимодействия с участниками ГАС второго уровня.

Исполнитель должен выполнить адаптацию функциональности СЭДО путем интеграции с операторами для обмена документами и уведомлениями в электронном виде между участниками информационного взаимодействия, поддерживающего формат обмена МЭДО и схему обмена для оператора, предусмотренной ГАС.

Система должна обеспечивать обмен с организациями, включенными в ГАС, используя их идентификаторы, полученные из ГАС, в соответствии с форматом МЭДО. Необходимо произвести настройку Системы для обмена документами и уведомлениями между участниками информационного взаимодействия (участники второго уровня), через оператора доставки ГосЭДО, включенного в ГАС.

Исполнитель должен выполнить настройку обмена документами и уведомлениями в электронном виде с использованием МЭДО с организациями-участниками информационного взаимодействия, подключенными к ГИС «ТОР СЭД» (далее – организации-участники ГИС «ТОР СЭД»).

Исполнитель должен выполнить адаптацию СЭДО в части обеспечения отправки документов ДСП адресату на основании данных, полученных из ГАС. Система должна выполнять отправку ДСП документов. При отсутствии у адресата возможности приема документов ДСП, Система не должна выполнять отправку.

Исполнитель должен реализовать вывод уведомления о невозможности передачи ДСП документа адресату в случае, если адресат не принимает ДСП документы через МЭДО.

Возможность приема адресатом документов ДСП, полученных по МЭДО, должно проверяться Системой автоматически.

Полный перечень операций, при выполнении которых Система должна осуществлять проверку возможности приема адресатом документов ДСП, подлежит уточнению на этапе ЧТЗ.

Исполнитель должен выполнить актуализацию справочника контрагентов СЭДО путем приведения сведений о юридических лицах в соответствие со справочником контрагентов ГАС в части наименований (полных и кратких) и адресов. При этом актуализации подлежат только записи о юридических лицах. В рамках выполнения задач по актуализации данных контрагентов не должен быть изменен функционал вывода результатов поиска в поисковых полях.

Исполнитель должен обеспечить обработку Системой входящего технологического транспортного контейнера со сведениями ГАС, поступающего от организатора или оператора межведомственного электронного взаимодействия.

4.7.2 Требования к развитию (адаптации) функционала модуля МЭДО в части поддержки формата обмена данными МЭДО 3.0

Для функционала интеграции с МЭДО должна быть обеспечена адаптация Системы в части возможности работы с форматом МЭДО 3.0.

В рамках адаптации Веб-клиента Исполнитель должен обеспечить:

- реализацию формирования, приема и отправки ТК «Документ в электронном виде» в формате 3.0, в том числе содержащего цифровой документ (при необходимости), и ТК «Цифровой документ ГосЭДО» в формате 3.0. Перечень процессов взаимодействия и видов документов, для которых применяется транспортный контейнер «Цифровой документ ГосЭДО», а также состав транспортного контейнера подлежат уточнению на этапе ЧТЗ;
- реализацию формирования, приема и отправки уведомлений в формате взаимодействия МЭДО 3.0 в составе документов-уведомлений в виде структурированных данных цифрового документа (файла digital.xml). Перечень уведомлений и требований к ним должны быть определены на этапе ЧТЗ;
- реализацию формирования, приема и отправки квитанций о техническом приеме или отказе в приеме электронного сообщения в формате взаимодействия МЭДО 3.0. Требования к квитанциям должны быть уточнены на этапе ЧТЗ;
- реализацию подписания электронной подписью файла структурированных данных цифрового документа при наличии требования о его подписании. Информация о подписании документа должна включаться в состав файла digital.xml в формате XMLDSig. Структура подписи подлежит уточнению на этапе ЧТЗ;
- реализацию формирования файла описания электронного сообщения (message.xml) в формате 3.0 с заполнением обязательных полей, их состав подлежит уточнению на этапе ЧТЗ;
- реализацию формирования файла описания транспортного контейнера (passport.xml) в формате 3.0 с заполнением обязательных полей, их состав подлежит уточнению на этапе ЧТЗ.

Также Исполнитель должен обеспечить создание в СЭДО РК с заполненными обязательными реквизитами на основании входящих транспортных контейнеров формата 3.0. и создание внешней резолюции на основании данных ТК, содержащих событие по ЦП.

4.7.3 Требования к развитию (адаптации) функционала СЭДО в части обмена данными по событиям цифровых поручений второй очереди

Исполнитель должен выполнить адаптацию Веб-клиента для обеспечения поддержки дополнительных событий при взаимодействии с Аппаратом Правительства Российской Федерации в части получения и передачи информации по цифровым поручениям (далее – ЦП) Правительства Российской Федерации в адрес Минэкономразвития России.

Для указанных событий должна быть обеспечена реализация следующего функционала:

1. Пользователь должен иметь возможность направить в Аппарат Правительства Российской Федерации событие «Запрос изменения срока» по пункту ЦП в случае необходимости продления срока выполнения поручения.
2. Пользователь должен иметь возможность направить в Аппарат Правительства Российской Федерации событие «Представление промежуточного доклада» по пункту ЦП в случае необходимости отправки промежуточного ответа на поручение.
3. Прием входящих ТК по событиям «Изменение срока поручения» и «Принятие информации об исполнении». Определение таких пакетов должно осуществляться по наличию в составе ТК структурированного файла digital.xml, содержащего данные событий «Изменение срока поручения» или «Принятие информации об исполнении».

При поступлении вышеуказанных входящих событий в Веб-клиенте должна автоматически формироваться РК входящего документа.

В сформированных РК должен отображаться читаемый файл формата .html, преобразованный из файла структурированных данных digital.xml, для обеспечения возможности просмотра информации по входящим событиям «Изменение срока поручения» или «Принятие информации об исполнении». Сформированные файлы в формате .html должны выводиться в область предпросмотра, область файлов, а также должны быть доступны для загрузки и печати в соответствии с правами доступа на основании ролевой модели Веб-клиента. Макеты экранных форм HTML-файлов подлежат уточнению на этапе ЧТЗ.

4.7.4 Требования к развитию (адаптации) функционала СЭДО интеграции с сайтом Минэкономразвития России в части передачи контактной информации структурного подразделения Министерства по запросу юридического лица

Исполнитель должен подготовить РГ отчет в СЭДО, который будет вызываться интеграционным интерфейсом при создании запроса с официального сайта Минэкономразвития России. Результаты вызова отчета по искомому документу предоставляются в виде согласованного набора данных.

Состав поступающих по запросу данных:

1. номер документа;
2. дата документа.

Состав возвращаемых данных:

1. регистрационный номер входящего документа;
2. дата регистрации документа в СЭДО;
3. корреспондент;
4. наименование структурного подразделения (первого структурного подразделения - ответственного исполнителя по ветке резолюции).

Если по заданным параметрам запросу удовлетворяют несколько документов, то в РГ отчете должны возвращаться данные по всем отобранным в формате согласованного набора данных. Формат представления возвращаемых данных по запросу должен быть уточнен на этапе ЧТЗ.

Исполнитель должен обеспечить консультацию разработчиков официального сайта Минэкономразвития России в части описания доступных методов интеграционного интерфейса для вызова отчета РГ.

4.7.5 Требования к развитию (адаптации) функционала СЭДО в части отправки одного исходящего события по нескольким пунктам цифрового поручения

В рамках адаптации функционала отправки одного исходящего события по нескольким пунктам ЦП в Веб-клиенте должно быть реализовано:

1. Возможность прикрепления одной исходящей РК в реализацию ЦП к нескольким КЗ по пунктам ЦП. К данным исходящим событиям должны относиться:

Представление итогового доклада;
 Представление промежуточного доклада;
 Запрос изменения срока;
 Представление предложения соисполнителя.

2. Формирование единого ТК с одним файлом digital.xml.

При отправке исходящей РК с событием ЦП, прикрепленной к нескольким пунктам ЦП, должен формироваться один контейнер с одним файлом digital.xml, в котором указаны все данные по сопоставленным пунктам ЦП, к которым прикреплена данная исходящая РК;

3. Формирование записей в журнале обмена по каждому пункту ЦП.

После успешной регистрации и передачи исходящей РК получателям в зависимости от типа события ЦП в журнал обмена должны добавляться записи по каждой КЗ, на которую была отправлена исходящая РК.

При возникновении ошибок в ходе передачи ТК с событием ЦП статус записи должен измениться на «Ошибка». Уведомление должно содержать тип сообщения и комментарий, соответствующий событиям ЦП.

Состав событий, по которым формируются записи, карточки, в которых формируются записи, тип сообщений и комментарии к ним должны быть определены на этапе ЧТЗ.

4.7.6 Требования к развитию (адаптации) функционала СЭДО в части автоматической простановки вида контроля «ВК» по пунктам цифрового поручения, где Минэкономразвития России является соисполнителем

Для функционала формирования проекта внешней резолюции по событию «Выдача поручения» для пунктов поручения, в которых Минэкономразвития России является соисполнителем, Исполнитель должен реализовать автоматическую установку вида контроля «ВК».

4.7.7 Требования к развитию (адаптации) функционала СЭДО в части отображения подписанта цифрового поручения в дереве резолюций РК

Для функционала определения подписанта внешней резолюции входящей РК, сформированной по ЦП, Исполнитель должен реализовать вывод ФИО автора ЦП на основании данных digital.xml ЦП в поле «Подписал» внешней резолюции РК.

При создании внешней резолюции ЦП в качестве подписанта должны использоваться сведения об авторе первого по порядку пункта ЦП из digital.xml для текущей организации.

4.7.8 Требования к развитию (адаптации) функционала СЭДО в части изменения последовательности отображения значений в поле «Номер пункта» в резолюциях по событиям Цифровых поручений

Исполнитель должен реализовать в Веб-клиенте отображение номеров пунктов ЦП в формате «разд. 7, п. 4, пп. 2». Указанный формат должен отображаться при создании внешней резолюции в поле «Номер пункта», в дереве резолюции, а также в записях журнала МЭДО по событиям ЦП.

Новый формат должен использоваться только для новых РК ЦП.

4.7.9 Требования к развитию (адаптации) функционала СЭДО в части автоматического указания Министра экономического развития Российской Федерации исполнителем по пунктам цифрового поручения

Исполнителем в Веб-клиенте должна быть выполнена реализация автоматического назначения Министра экономического развития Российской Федерации в качестве исполнителя (с типом исполнения ответственный/соисполнитель) во всех пунктах внешней резолюции, сформированных автоматически на основании цифрового поручения, в которых Минэкономразвития России указан в качестве исполнителя/соисполнителя.

Функционал должен распространяться на взаимодействие в формате МЭДО 3.0.

4.7.10 Требования к развитию (адаптации) функционала СЭДО в части изменения порядка отображения пунктов цифрового поручения

Исполнителем должно быть реализовано отображение пунктов ЦП в автоматически создаваемой внешней резолюции РК и дереве резолюции в порядке возрастания номеров разделов, пунктов и подпунктов.

4.7.11 Требования к развитию (адаптации) функционала СЭДО в части реализации возможности вывода информации в поле «Текст поручения» в пункте внешней резолюции РК

Исполнителем должна быть выполнена реализация отображения расширенного состава сведений о поручении в поле «Текст поручения» пункта внешней резолюции РК, создаваемой по ЦП в Веб-клиенте.

В поле «Текст поручения» пункта внешней резолюции должны отображаться текст пункта ЦП, сведения об исполнителях, соисполнителях, сроке исполнения и авторе поручения, сформированные на основании данных digital.xml ЦП. Порядок и формат вывода информации должны быть уточнены на этапе ЧТЗ.

4.7.12 Требования к развитию (адаптации) функционала СЭДО в части реализации возможности направления исходящего документа по пунктам цифрового поручения, созданным вручную во внешней резолюции

Исполнителем должна быть выполнена адаптация механизма формирования транспортного контейнера исходящих документов по пунктам цифрового поручения, созданным вручную.

При формировании исходящего транспортного контейнера должно выполняться сопоставление пунктов, по которым направляется исходящая РК с пунктами ЦП,

полученными из digital.xml входящей РК. Если пункт исходящей РК отсутствует среди пунктов, содержащихся в digital.xml, такой пункт должен рассматриваться, как созданный вручную.

Для пунктов, созданных вручную, транспортный контейнер ЦП с файлом digital.xml не должен формироваться. По таким пунктам должен формироваться исходящий транспортный контейнер в формате МЭДО 3.0 без файла структурированной информации digital.xml.

Если один исходящий документ связан с несколькими пунктами, созданными вручную, должен формироваться один транспортный контейнер формата МЭДО 3.0.

Если один исходящий документ связан одновременно с пунктами ЦП, созданными автоматически на основании файла digital.xml, и пунктами, созданными вручную, должен формироваться единый исходящий транспортный контейнер ЦП с одним файлом digital.xml. В файл digital.xml должны включаться только данные по пунктам ЦП, присутствующие в digital.xml входящей РК. Для пунктов, созданных вручную, отдельный транспортный контейнер формата МЭДО 3.0 не должен формироваться.

4.7.13 Требования к разработке Частного технического задания на развитие Системы

Частное техническое задание на развитие Автоматизированной информационной системы «Система электронного документооборота Минэкономразвития России» (далее – ЧТЗ, ЧТЗ на развитие Системы) должно быть разработано Исполнителем не позднее 25 ноября 2026 г. и согласовано с Заказчиком.

В ЧТЗ на развитие Системы должны быть учтены требования по размещению Системы в ОЦОД ПК, включая доработку и дополнительную настройку, обеспечивающую готовность к проведению аттестации Системы по требованиям информационной безопасности в соответствии с установленным в Акте классификации системы классом защищенности государственной информационной системы, уровнем защищенности персональных данных, обрабатываемых в Системе. При необходимости внесения корректировок в архитектуру Системы, изменения количества, технических характеристик виртуальных машин, их сетевой связанности должно быть актуализировано и согласовано с Заказчиком и (или) Оператором ОЦОД ПК Техническое решение по размещению Системы в облачной инфраструктуре ОЦОД ПК.

По итогам выполнения данного вида работы и в срок, обозначенный в текущем пункте настоящего ТЗ, Исполнитель формирует документ ЧТЗ на развитие Системы и направляет его

Заказчику официальным письмом для согласования и утверждения, дублируя на адрес электронной почты Заказчика.

Заказчик в срок не более 5 (пяти) рабочих дней с даты получения от Исполнителя ЧТЗ на развитие Системы, утверждает документ, а в случае выявления замечаний, документ направляется Исполнителю на доработку официальным письмом и дублируется на адрес электронной почты Исполнителя.

Исполнитель в срок не более 5 (пяти) рабочих дней с даты получения замечаний к документу, дорабатывает его согласно полученным замечаниям и направляет Заказчику на повторное согласование официальным письмом и дублируя в электронном виде. В случае отсутствия разногласий между Исполнителем и Заказчиком, документ ЧТЗ на развитие Системы утверждается Заказчиком.

4.7.14 Требование к актуализации Модели угроз и Модели нарушителя информационной безопасности Системы

Документ Модель угроз и модель нарушителя безопасности информации (далее - МУиН) должен быть актуализирован с учетом Методики оценки угроз безопасности информации, утвержденной ФСТЭК России 5 февраля 2021 года. В случае, если в период действия контракта ФСТЭК России будут утверждены новые (или актуализированы существующие) материалы, Исполнитель должен их учитывать при актуализации указанного в настоящем пункте документа.

Содержание документа МУиН должно соответствовать, требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утверждёнными приказом ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», Методикой оценки угроз безопасности информации ФСТЭК России от 5 февраля 2021 года, а также учитывать угрозы безопасности информации, актуальные для информационной телекоммуникационной инфраструктуры центра обработки данных (далее – ИТКИ ЦОД).

Должны быть актуализированы угрозы безопасности информации, реализация которых может привести к нарушению безопасности информации в Системе, и разработана на их основе МУиН.

Документ МУиН не должен противоречить требованиям инфраструктурной площадки, на которой размещается Система ТУ ИС ФОИВ ОЦОД ПК.

МУиН подлежит согласованию силами Заказчика с ФСБ России и ФСТЭК России (далее также – уполномоченные органы) в соответствии с требованиями постановления Правительства Российской Федерации от 6 июля 2015 г. № 676.

В случае, если по результатам указанного согласования потребуется доработка документа МУиН в соответствии с замечаниями Заказчика, Исполнитель обязан в срок, установленный Заказчиком и составляющий не менее 10 (десяти) рабочих дней, провести указанную доработку. МУиН должны быть разработаны и (или) актуализированы в соответствии с текущим уровнем значимости и с учетом класса защищенности информационной системы.

МУиН должны быть разработаны и (или) актуализированы Исполнителем с учетом актуализации перечня мер, подлежащих реализации при развитии Системы в целях предотвращения появления и устранения уязвимостей Системы в процессе её жизненного цикла. Выбор и уточнение мер по разработке безопасного СПО должен основываться на результатах проводимого Исполнителем анализа угроз безопасности информации, в результате которого должны быть определены актуальные для среды разработки СПО угрозы безопасности информации.

При определении угроз безопасности информации необходимо использовать банк угроз ФСТЭК России, а также описания векторов (шаблонов) компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.).

4.7.15 Требование к актуализации Частного технического задания на модернизацию системы защиты информации Системы

В случае актуализации модели угроз и модели нарушителя информационной безопасности Системы и (или) в случае, если это обусловлено составом доработок в ЧТЗ на развитие Системы, Исполнителем должно быть актуализировано ЧТЗ на модернизацию системы защиты информации Системы (далее – ЧТЗ на СЗИ), состоящее из комплекта проектной и эксплуатационной документации на систему защиты информации, определяющее в том числе требования к средствам защиты информации (далее – СрЗИ).

Требования к СЗИ должны определяться в зависимости от класса защищенности и актуальных угроз безопасности информации, включенных в модель угроз безопасности информации Системы. Указанные требования включаются в ЧТЗ на СЗИ с учетом требований нормативной правовой базы в области защиты информации государственных информационных систем.

При реализации функций по защите информации должны использоваться:

- встроенные средства защиты информации: возможности и механизмы защиты информации, предоставляемые операционными системами, системами управления базами данных и приложениями;
- средства защиты информации: программно-технические средства, предназначенные для выполнения требований по безопасности информации, не реализуемые встроенными средствами защиты информации.

Применяемые средства защиты информации должны быть сертифицированы по требованиям безопасности информации Российской Федерации. Классы защиты и уровни доверия применяемых при развитии Системы сертифицированных средств защиты информации и средств криптографической защиты информации должны соответствовать классу защищенности Системы.

Не допускается применение СрЗИ, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

При актуализации ЧТЗ на СЗИ Исполнителем должны быть рассмотрены следующие базовые меры защиты информации и адаптированы с учетом определенных для Системы актуальных угроз безопасности (в части развиваемой Системы и в пределах компетенций и ответственности Заказчика и Исполнителя):

- а) идентификация и аутентификация;
- б) управление доступом;
- в) регистрация событий безопасности;
- г) защита виртуализации и облачных вычислений;
- д) защита технологий контейнерных сред и их оркестрации;
- е) защита сервисов электронной почты;
- ж) защита веб-технологий;
- з) защита программных интерфейсов взаимодействия приложений;
- и) защита конечных устройств;
- к) защита мобильных устройств;
- л) защита технологий интернета вещей;
- м) защита точек беспроводного доступа;
- н) антивирусная защита;
- о) обнаружение и предотвращение вторжений на сетевом уровне;
- п) сегментация и межсетевое экранирование;

- р) защита от компьютерных атак, направленных на отказ в обслуживании;
- с) защита каналов передачи данных и сетевого взаимодействия.

При актуализации ЧТЗ на СЗИ Исполнитель должен учитывать требования приказа ФСБ России 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», требования формуляров и оценки влияния среды функционирования на СКЗИ при разработке. Исполнитель обязан неукоснительно соблюдать требования формуляров на средства криптографической защиты информации (далее — СКЗИ), в частности, на требование, касающееся проведения оценки влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований. Проведение работ по оценке влияния среды функционирования СКЗИ на выполнение предъявленных к СКЗИ требований является обязательным условием действия сертификата на СКЗИ, в соответствии с которым СКЗИ обеспечивает заданный уровень информационной безопасности при выполнении требований эксплуатационной документации согласно формуляру, на СКЗИ.

При актуализации ЧТЗ на СЗИ Исполнитель должен учитывать требования Указа Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», Приказа ФСТЭК России от 11 апреля 2025 г. № 117 «Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» в части обеспечения защиты информации при использовании для функционирования информационных систем искусственного интеллекта.

Актуализация ЧТЗ на СЗИ также не должна противоречить требованиям к размещению Системы в ОЦОД ПК. ЧТЗ на СЗИ должно отражать необходимый перечень изменений и дополнительных настроек Системы, обеспечивающих после их реализации беспрепятственное размещение Системы в ОЦОД ПК.

ЧТЗ на СЗИ должно предусматривать требования к разработке (актуализации в случае, если ранее такие документы были разработаны) Исполнителем проектных документов на систему защиты информации Системы, в соответствии с пунктом 8 настоящего ТЗ.

ЧТЗ на СЗИ должно предусматривать требования к разработке и (или) актуализации Исполнителем проектных и эксплуатационных документов на СЗИ. Перечень проектной и эксплуатационной документации на СЗИ уточняется Исполнителем у Заказчика в рабочем порядке в согласованные сроки и предоставляется в каждом отчетном периоде выполнения работ после завершения работ по развитию Системы и перед проведением предварительных испытаний, в соответствии с пунктом 6.1 настоящего ТЗ. В случае наличия замечаний по результатам испытаний Исполнитель должен доработать проектную и эксплуатационную документацию на СЗИ.

ЧТЗ на СЗИ и МУиН направляются Заказчиком на согласование с федеральным органом исполнительной власти, уполномоченным в области безопасности, и с федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий в части, касающейся выполнения установленных требований по защите информации. В случае наличия замечаний к ЧТЗ на СЗИ в процессе согласования, Исполнитель обеспечивает устранение указанных замечаний, в том числе в рамках гарантийных обязательств.

5 Состав и содержание работ по развитию Системы

Сроки выполнения работ и виды отчётной документации приведены в Таблице 6.

Таблица 6 – Сроки выполнения работ и виды отчетной документации

№ п/п	Содержание работ этапов	Сроки	Результаты работ (материалы, предоставляемые Заказчику)
1.	Передача простых (неисключительных) прав на программное обеспечение СЭДО	В течение 7 календарных дней с даты заключения контракта	Лицензионные соглашения и/или лицензионный договор на предоставление простых (неисключительных) лицензий на программное обеспечение СЭДО Акт передачи неисключительных прав
2.	Разработка ЧТЗ, актуализация Модели угроз безопасности информации СЭДО и ЧТЗ ИБ	С даты заключения контракта до 25 ноября 2026 г.	– Частное техническое задание; – Модель угроз безопасности информации СЭДО; – Частное техническое задание на создание системы защиты информации СЭДО
3.	Проведение работ по адаптации и проведение испытаний (тестовый контур)	С даты завершения этапа работ № 2 до 11 декабря 2026 г.	Актуализированная эксплуатационная и программная документация, включая: – Актуализированное руководство администратора; – Актуализированное руководство пользователя. Комплект документации по предварительным испытаниям: – Программа и методика предварительных испытаний; – Протокол проведения предварительных испытаний; – Акт о приемке (готовности) СЭДО к вводу в опытную эксплуатацию. Комплект документации по опытной эксплуатации: – Программа и методика опытной эксплуатации; – Отчет о проведении опытной эксплуатации; – Журнал проведения опытной эксплуатации; – Акт о завершении опытной эксплуатации. Комплект документации по приемочным испытаниям: – Программа и методика приемочных испытаний; – Протокол проведения приемочных испытаний;

			– Акт о приемке (готовности) СЭДО в промышленную эксплуатацию.
4.	Перенос функционала в промышленный контур и аттестационные испытания	С даты завершения этапа работ № 3 по 20 декабря 2026г.	Актуализированная проектная документация на систему защиты информации СЭДО, включая: – Проект акта классификации СЭДО; – Проектные решения системы защиты информации СЭДО Программа и методика аттестационных испытаний; – Протокол аттестационных испытаний; – Заключение по результатам проведения аттестационных испытаний; – Аттестат соответствия требованиям по защите информации СЭДО (при положительном заключении).

Для выполнения работ Исполнитель должен передать Заказчику простые (неисключительные) лицензии на использование программного обеспечения СЭДО в составе, необходимом для выполнения требований настоящего ТЗ и перечисленном в таблице 7.

Исполнитель должен предоставить Заказчику неисключительные права на программное обеспечение в комплекте с лицензионными ключами, передаваемыми на носителе (CD или DVD) и позволяющими точно идентифицировать программное обеспечение, на которое передаются неисключительные права. Исполнителем должен быть в явном виде указан весь перечень передаваемого программного обеспечения и его регистрационные номера в Едином реестре российских программ для ЭВМ и баз данных.

Таблица 7 – Спецификация программного обеспечения

№	Наименование программы для ЭВМ из Единого реестра российских программ для ЭВМ и баз данных	Состав лицензии	Кол-во	Класс программ для электронных вычислительных машин
1	Простая (неисключительная) лицензия на ПО Цифровой КУПОЛ (или эквивалент)	Цифровой КУПОЛ (или эквивалент), Серверный модуль. Бессрочная лицензия. Поддерживаются следующие способы проверки учетных данных: – постоянный пароль,	1	03.01 Средства защиты от несанкционированного доступа к информации

№	Наименование программы для ЭВМ из Единого реестра российских программ для ЭВМ и баз данных	Состав лицензии	Кол -во	Класс программ для электронных вычислительных машин
		– одноразовый пароль (TOTP/sms/e-mail). Поддерживается двухфакторная авторизация с использованием TOTP, sms, e-mail, push, аппаратный токен. Функции управления подключенными информационными системами: – просмотр/ создание/ удаление записи об ИС; – управление парольной политикой для ИС; – управление политикой токенов для ИС. Функции управления пользователями/ учетными записями: – просмотр/ создание/ удаление групп пользователей; – просмотр/ создание/ удаление УЗ пользователя; – настройка групп пользователей – включение/исключение УЗ в группы; – блокировка/разблокировка УЗ; – сброс пароля УЗ; – настройка параметров подключения УЗ, управление факторами авторизации и аутентификации; – настройка утверждений для доступа для УЗ/групп УЗ к ИС. Функции управления доступом к ИС: – предоставления прав доступа к ИС для УЗ/групп УЗ; – программная интеграция ЦК и ИС на уровне ролевой модели ИС (посредством API ЦК). Функции журналирования: – настройка событий, подлежащих регистрации (события		

№	Наименование программы для ЭВМ из Единого реестра российских программ для ЭВМ и баз данных	Состав лицензии	Кол-во	Класс программ для электронных вычислительных машин
		безопасности, события администрирования); – установление срока хранения записей журналов; – журналирование действий пользователей; – возможность выгрузки журналов во внешние системы анализа логов. Функции контроля целостности: – выполнение контроля целостности ЦК (снятия контрольных сумм ПО); – выполнение контроля целостности внешних систем.		
2	Простая (неисключительная) лицензия на ПО Цифровой КУПОЛ (или эквивалент)	Цифровой КУПОЛ (или эквивалент), коннектор, 1 информационная система. Бессрочная лицензия (характеристики в соответствии с пунктом 1).	1	03.01 Средства защиты от несанкционированного доступа к информации
3	Простая (неисключительная) лицензия на ПО Система документационного управления «Приоритет»	Система документационного управления «Приоритет», Корпоративная редакция, Модуль интеграции с МЭДО с поддержкой формата 3.0, Серверная лицензия. Бессрочная лицензия.	1	06.12 Программное обеспечение средств внутреннего электронного документооборота
4	Простая (неисключительная) лицензия на ПО Система документационного управления «Приоритет»	Система документационного управления «Приоритет», Корпоративная редакция, Модуль обмена цифровыми поручениями 1.0, Серверная лицензия, пакет обновлений. Бессрочная лицензия.	1	06.12 Программное обеспечение средств внутреннего электронного документооборота
5	Простая (неисключительная) лицензия на ПО Docsvision	Docsvision 5, Core ECM корпоративная редакция, набор серверных компонентов в составе: Серверная лицензия, 2 серверов в Кластере баз данных, 6 серверов в Кластере Сервера приложений, пакет обновлений. Бессрочная лицензия.	1	06.12 Программное обеспечение средств внутреннего электронного документооборота
6	Простая	Система документационного	1	06.12

№	Наименование программы для ЭВМ из Единого реестра российских программ для ЭВМ и баз данных	Состав лицензии	Кол -во	Класс программ для электронных вычислительных машин
	(неисключительная) лицензия на ПО Система документационного управления «Приоритет»	управления «Приоритет», Корпоративная редакция, Серверный модуль, версия 8.0, пакет обновлений. Бессрочная лицензия.		Программное обеспечение средств внутреннего электронного документооборота
7	Простая (неисключительная) лицензия на ПО Система документационного управления «Приоритет»	Система документационного управления «Приоритет», Корпоративная редакция, АРМ Руководителя, серверная лицензия, версия 8.0, пакет обновлений. Бессрочная лицензия.	1	06.12 Программное обеспечение средств внутреннего электронного документооборота
8	Простая (неисключительная) лицензия на ПО Docsvision	Docsvision 5, Core ECM корпоративная редакция, Универсальный клиент, 1200 пользователей, пакет обновлений. Бессрочная лицензия.	1	06.12 Программное обеспечение средств внутреннего электронного документооборота
9	Простая (неисключительная) лицензия на ПО Система документационного управления «Приоритет»	Система документационного управления «Приоритет», Корпоративная редакция, Универсальный клиент, 1200 пользователей, пакет обновлений. Бессрочная лицензия.	1	06.12 Программное обеспечение средств внутреннего электронного документооборота
10	Простая (неисключительная) лицензия на ПО Docsvision	Docsvision 5, Core ECM корпоративная редакция, Универсальный клиент, 150 пользователей, пакет расширений. Бессрочная лицензия.	1	06.12 Программное обеспечение средств внутреннего электронного документооборота
11	Простая (неисключительная) лицензия на ПО Система документационного управления «Приоритет»	Система документационного управления «Приоритет», Корпоративная редакция, Универсальный клиент, 150 пользователей, пакет расширений. Бессрочная лицензия.	1	06.12 Программное обеспечение средств внутреннего электронного документооборота
12	Простая (неисключительная) лицензия на ПО Система	Система документационного управления «Приоритет», Корпоративная редакция, Модуль автоматической маршрутизации	1	06.12 Программное обеспечение средств

№	Наименование программы для ЭВМ из Единого реестра российских программ для ЭВМ и баз данных	Состав лицензии	Кол-во	Класс программ для электронных вычислительных машин
	документационного управления «Приоритет»	документов, Серверная лицензия, пакет обновлений. Бессрочная лицензия.		внутреннего электронного документооборота
13	Простая (неисключительная) лицензия на Средство криптографической защиты информации «КриптоПро CSP» версии 5.0»	Лицензия на обновление СКЗИ "КриптоПро CSP" до версии 5.0 на сервере. Бессрочная лицензия.	1	03.10 Средства криптографической защиты информации и электронной подписи
14	Простая (неисключительная) лицензия на Программу «КриптоПро .NET»	Лицензия на право использования ПО "КриптоПро .NET" версии 2.0 на одном сервере. Бессрочная лицензия.	1	03.10 Средства криптографической защиты информации и электронной подписи
15	Простая (неисключительная) лицензия на ПО Операционная система специального назначения «Astra Linux Special Edition»	Лицензия на операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры x86-64, со встроенным программным модулем "Защищенная СУБД ОС ALSE", (Лицензия "Защищенная СУБД"), уровень защищенности «Максимальный» («Смоленск»), РУСБ.10015-01 (ФСТЭК), способ передачи электронный, на 1 физическое или виртуальное ядро сервера, сроком на 12 мес. с даты передачи несключительных прав, с включенными обновлениями Тип 1 на 12 мес. OS2101X8618DIGZDBSR02-SO12	164	02.07 Средство управления базами данных

В соответствии с п. 1 ч. 1 ст. 33 Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» возможность поставки «эквивалента» ПО по п. 3-15 не предусмотрена, в связи с необходимостью обеспечения взаимодействия с ПО, используемым Государственным заказчиком.

При необходимости, лицензии на сертифицированную СУБД и иное необходимое для аттестации ПО предоставляет Исполнитель.

6 Порядок контроля и приемки выполненных работ

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

Для приемки адаптированной Системы в промышленную эксплуатацию Исполнитель при участии Заказчика должен провести ее испытания.

Испытания Системы должны быть проведены в следующем порядке:

- Предварительные испытания;
- Опытная эксплуатация;
- Приемочные испытания;
- выполнение квалификационного тестирования СПО в соответствии с ГОСТ Р 56939-2024. Национальный стандарт Российской Федерации. «Защита информации. Разработка безопасного программного обеспечения. Общие требования», ГОСТ Р 71207—2024 «Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Статический анализ программного обеспечения. Общие требования».

Методы проведения всех видов испытаний Системы и сценарии их проведения должны быть определены в соответствующих программах и методиках испытаний, которые должны быть согласованы и утверждены Исполнителем и Заказчиком не позднее 3 (трех) рабочих дней до даты проведения испытаний.

Испытания должны проводиться в присутствии представителей Заказчика и Исполнителя, согласно соответствующему документу Программа и методика испытаний. Порядок устранения замечаний и реализации рекомендаций Заказчика должен быть определен соответственно виду испытания в документах «Программа и методика предварительных испытаний», «Программа и методика опытной эксплуатации» и «Программа и методика приемочных испытаний».

6.1.1 Требования к проведению предварительных испытаний

Предварительные испытания проводят с целью предварительной оценки соответствия СЭДО требованиям ТЗ и ЧТЗ, а также определения работоспособности и готовности СЭДО к вводу в опытную эксплуатацию.

Порядок проведения и методы испытаний должны быть приведены в документе «Программа и методика предварительных испытаний».

При выявлении в ходе испытаний критичных замечаний, исключающих передачу доработанной СЭДО в опытную эксплуатацию, Исполнитель должен устранить замечания в

согласованные с Заказчиком сроки, и предварительные испытания должны быть проведены повторно. Критичными замечаниями считаются выявленные ошибки, после которых СЭДО не может продолжать свою работу.

При выявлении в ходе испытаний некритичных замечаний, не влияющих на решение о передаче СЭДО в опытную эксплуатацию, они устраняются Исполнителем в рамках опытной эксплуатации.

Результаты проведения предварительных испытаний должны быть отражены в Протоколе проведения предварительных испытаний. Протокол проведения предварительных испытаний должен содержать заключение о готовности (неготовности) СЭДО к опытной эксплуатации, а также перечень необходимых доработок (при наличии) и рекомендуемые сроки их выполнения.

В случае успешного проведения предварительных испытаний оформляется Акт о приемке (готовности) СЭДО к вводу в опытную эксплуатацию.

6.1.2 Требования к проведению опытной эксплуатации

По результатам завершения предварительных испытаний (в соответствии с требованиями пункта 6.1.1 настоящего ТЗ) должна быть проведена опытная эксплуатация СЭДО.

Опытную эксплуатацию СЭДО проводят с целью обнаружения и устранения ошибок, допущенных при развитии (адаптации) СЭДО, проверки готовности пользователей к работе в условиях функционирования СЭДО, а также корректировки (при необходимости) документации на СЭДО. Порядок проведения, состав участников и методы испытаний должны быть приведены в документе «Программа и методика опытной эксплуатации».

Опытная эксплуатация проводится в течении 7 (семи) календарных дней. По согласованию с Заказчиком сроки проведения опытной эксплуатации могут быть сокращены.

Пользователи, назначенные Заказчиком для участия в опытной эксплуатации, должны ознакомиться с актуализированной версией Руководства пользователя.

В ходе опытной эксплуатации Исполнителем ведется Журнал проведения опытной эксплуатации, в который заносят сведения о продолжительности функционирования Системы, об отказах, сбоях аварийных ситуациях, изменениях параметров объектов автоматизации, проводимых корректировках документации и программных средств, наладке технических средств, а также замечания и пожелания пользователей по удобству эксплуатации Системы.

При выявлении в ходе опытной эксплуатации критичных замечаний, исключающих передачу доработанной СЭДО на приемочные испытания, срок проведения опытной

эксплуатации продлевается на срок, установленный по согласованию с Заказчиком в целях устранения Исполнителем выявленных замечаний.

При выявлении в ходе опытной эксплуатации не критичных замечаний, не влияющих на решение о передаче СЭДО на приемочные испытания, они устраняются Исполнителем до начала проведения приемочных испытаний. Проверка устранения не критичных замечаний производится в ходе приемочных испытаний.

Результаты проведения опытной эксплуатации должны быть отражены в Отчете о проведении опытной эксплуатации.

Опытная эксплуатация завершается оформлением Акта о завершении опытной эксплуатации.

6.1.3 Требования к проведению приемочных испытаний

По завершении опытной эксплуатации (в соответствии с требованиями пункта 6.1.2 настоящего ТЗ) должны быть проведены приемочные испытания СЭДО. Приемочные испытания должны быть проведены на территории Заказчика.

Приемочные испытания СЭДО проводят для определения соответствия Техническому заданию, оценки качества опытной эксплуатации и решения вопроса о возможности приемки в постоянную эксплуатацию.

Приемочные испытания должны проводиться комиссией, состоящей из уполномоченных представителей Заказчика и Исполнителя.

Порядок проведения и методы испытаний должны быть приведены в документе «Программа и методика приемочных испытаний».

При выявлении в ходе испытаний критичных замечаний, исключающих передачу доработанной СЭДО в промышленную эксплуатацию, Исполнитель должен устранить замечания в согласованные с Заказчиком сроки, и приемочные испытания должны быть проведены повторно. Критичными замечаниями считаются выявленные ошибки, после которых СЭДО не может продолжать свою работу.

При выявлении в ходе испытаний не критичных замечаний, не влияющих на решение о передаче СЭДО в промышленную эксплуатацию, они устраняются Исполнителем не позднее срока завершения работ по развитию СЭДО.

Результаты проведения приемочных испытаний должны быть отражены в Протоколе проведения приемочных испытаний.

По результатам проведения приемочных испытаний оформляется Акт о приемке (готовности) СЭДО в промышленную эксплуатацию».

6.1.4 Требования к мероприятиям по подготовке и проведению аттестационных испытаний Системы

По завершению приемочных испытаний (в соответствии с требованиями пункта 6.1.3 настоящего ТЗ) в объеме выполненных работ по развитию Системы, Исполнителем должны быть проведены мероприятия по подготовке Системы к аттестационным испытаниям, в соответствии с актуальным Комплектом проектной и эксплуатационной, организационно-распорядительной документацией на систему защиты информации.

Исполнитель должен обеспечить:

- контроль проверки выполнения требований к защите ПДн при их обработке в ИСПДн, где результату выполнения работ предоставить Заказчику Проект Акта проверки выполнения требований к защите ПДн при их обработке в ИСПДн;
- поставку СрЗИ (в случае необходимости) в соответствии с Ведомостью покупных изделий, разработанной в рамках ЧТЗ на СЗИ, кроме СрЗИ, поставляемых Оператором ОЦОД ПК;
- установку и настройку СрЗИ, находящихся в зоне ответственности Исполнителя (при необходимости совместно с Заказчиком) после проектирования СЗИ в соответствии с требованиями нормативных правовых документов в области защиты информации и эксплуатационной документацией СрЗИ;
- предоставить Акт установки и настройки средств защиты информации (в случае необходимости), по результату успешной установки и настройки Исполнителем СрЗИ.

По завершении мероприятий по подготовке к аттестационным испытаниям должны быть проведены работы по аттестации СЭДО. В рамках этих мероприятий Исполнитель должен:

- разработать и согласовать с Заказчиком программу и методики аттестационных испытаний СЭДО;
- провести аттестационные испытания на соответствие СЭДО требованиям безопасности информации;
- оформить протокол по результатам аттестационных испытаний СЭДО;
- подготовить заключение о соответствии СЭДО требованиям безопасности информации;
- выдать, в случае положительных результатов аттестационных испытаний, Аттестат соответствия СЭДО требованиям безопасности информации.

Для выполнения работ по аттестации СЭДО Исполнитель вправе привлечь субподрядную организацию, обладающую соответствующими лицензиями.

Исполнитель приступает к разработке программы и методики аттестационных испытаний СЭДО и самим испытаниям после предоставления Заказчиком согласованных ФСБ России и ФСТЭК России модели угроз безопасности информации и частного технического задания на разработку систему защиты информации.

Аттестационные испытания должны проводиться с соблюдением требований следующих документов:

- ГОСТ РО 0043-004-2013. «Аттестация объектов информатизации. Программа и методика аттестационных испытаний»;
- Приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну».

По результатам аттестационных испытаний Исполнитель должен актуализировать комплект организационно-распорядительной документации на СЭДО (состав определяется в ЧТЗ на разработку систему защиты информации).

В случае, если по результатам аттестационных испытаний будут получены отрицательное заключение и вывод о невозможности выдачи Аттестата соответствия требованиям по защите информации на объект информатизации, то Исполнитель обязан в срок, согласованный Заказчиком, провести устранение недостатков и доработку Системы в рамках исполнения гарантийных обязательств выполненных работ. При этом срок действия гарантийных обязательств приостанавливается до даты выдачи Аттестата соответствия требованиям по защите информации на объект информатизации.

7 Объем и сроки гарантий качества

Предметом гарантийного обязательства является функциональность Системы, адаптированной согласно требованиям настоящего Технического задания и Частного технического задания, разработанного Исполнителем в рамках выполнения работ и согласованного с Государственным заказчиком.

Если в период гарантийного срока к материалам выполненных работ будут выявлены замечания со стороны федерального органа исполнительной власти, уполномоченного в области безопасности, и (или) федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам (в пределах их полномочий), то такие замечания подлежат устранению Исполнителем в срок, установленный Заказчиком, и составляющий не более 10 (десяти) рабочих дней.

В случае, если по результатам аттестационных испытаний и аттестации Системы на соответствие требованиям по защите информации будут получены отрицательное заключение вследствие наличия несоответствий (недостатков) системы защиты информации Системы требованиям по защите информации и вывод о невозможности выдачи Аттестата соответствия требованиям по защите информации, то Исполнитель обязан в срок, согласованный Заказчиком, провести устранение недостатков и доработку Системы за свой счет. При этом срок действия гарантийных обязательств приостанавливается до даты выдачи Аттестата соответствия Системы требованиям о защите информации.

На все результаты выполненных Работ устанавливается гарантийный срок 12 (Двенадцать) месяцев с даты подписания документа о приемке по Государственному контракту.

8 Требования к документированию

8.1 Перечень подлежащих разработке документов

Перечень подлежащих разработке и актуализации комплектов и видов документов приведен в разделе 5.

8.2 Требования к эксплуатационной и программной документации

Комплект эксплуатационной и программной документации на Систему должен содержать сведения, обеспечивающие эксплуатацию Системы в соответствии с требованиями к порядку эксплуатации систем, установленным постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

При актуализации документов «Руководство пользователя» и «Руководство администратора» Исполнитель должен отразить в них все изменения в функционировании системы, реализованных в рамках ГК.

По окончании выполнения соответствующих этапов работ, а также по Государственному контракту в целом Исполнитель передает Заказчику отчетные документы, перечисленные в разделе 5.

Исполнитель представляет Заказчику все отчетные документы по итогу выполнения работ по Государственному контракту в электронном варианте на носителе без возможности перезаписи и в 2-х экземплярах в печатном виде.

8.3 Требования по использованию ЕСКД и ЕСПД при разработке документов

При разработке документации дополнительные требования не предъявляются.