СОГЛАСОВАНО:

Заместитель генерального директора по цифровой трансформации

_____ Д.А. Анищенко

«06» 08 2026 г.

УТВЕРЖДАЮ:

Заместитель генерального директора по безопасности

_____ В.В. Катков

«06» 08 2026 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на оказание услуг по актуализации и автоматизации разработки организационно-распорядительной и технической документации и внутренних нормативных документов для систем ИСПДн и ЗОКИИ ПАО «Россети Центр и Приволжье»

1. Общие положения

1.1. Настоящее Техническое задание разработано с целью определения в ПАО «Россети Центр и Приволжье» (далее – Заказчик) состава и содержания услуг по актуализации и автоматизации разработки организационно-распорядительной и технической документации и внутренних нормативных документов для систем ИСПДн и ЗОКИИ.

2. Используемые сокращения

ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ЗОКИИ	Значимый объект критической информационной инфраструктуры
ИС	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
ИСПДн	Информационная система персональных данных
КИИ	Критическая информационная инфраструктура
НПА	Нормативный правовой акт
ОКИИ	Объект критической информационной инфраструктуры
ОРД	Организационно-распорядительная документация
ПДн	Персональные данные
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
УБИ	Угроза безопасности информации
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации

3. Цель и правовые основания оказания услуг

3.1. Целью оказания услуг является актуализация существующей организационно-распорядительной (далее – ОРД) и технической документации и автоматизация разработки организационно-распорядительной и технической документации для систем ИСПДн и ЗОКИИ в соответствии с действующим законодательством Российской Федерации и согласно настоящему Техническому заданию.

3.2. Правовые основания для оказания услуг:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119

«Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений»;
- Постановление Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»;
- Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;
- Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава 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 18.03.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»;

- Приказ ФСБ России от 25.12.2025 № 547 «Об утверждении Порядка информирования ФСБ России о компьютерных атаках и компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации и иных информационных ресурсов Российской Федерации, принадлежащих органам и организациям, на которые возложены обязанности, предусмотренные частью 4 статьи 9 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
- Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;
- Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- Приказ ФСТЭК России от 25.12. 2017 № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- Методический документ «Методика оценки угроз безопасности информации», утвержденный ФСТЭК России 05.02.2021;
- Методический документ «Методика тестирования обновлений безопасности программных, программно-аппаратных средств», утвержденный ФСТЭК России 28.10.2022;
- Методический документ «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств», утвержденный ФСТЭК России 30.06.2025;
- Методический документ «Руководство по организации процесса управления уязвимостями в органе (организации)», утвержденный ФСТЭК России 17.05.2023;
- Методический документ «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденный ФСТЭК России 11.11.2025;
- Методические рекомендации Национального координационного центра по компьютерным инцидентам по разработке Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак,

проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации.

4. Состав, описание и содержание услуг, требования к документированию

4.1. Перечень объектов Заказчика, входящих в рамки услуги, приведен в Таблице 1.

Таблица 1. Перечень объектов Заказчика

№ п/п	Наименование объекта Заказчика	Тип объекта	Адрес
1.	Владимирэнерго	Филиал	600016, г. Владимир, ул. Б. Нижегородская, д.106
2.	Ивэнерго	Филиал	153000, г. Иваново, ул. Крутицкая, д. 8/2
3.	Калугаэнерго	Филиал	248000, г. Калуга, ул. Красная Гора, д. 9/12
4.	Кировэнерго	Филиал	610000, г. Киров, ул. Спасская, д. 51
5.	Мариэнерго	Филиал	424006, Республика Марий Эл, г. Йошкар-Ола, ул. Панфилова, д. 39а
6.	Нижновэнерго	Филиал	603950, г. Нижний Новгород, ул. Рождественская, д. 33
7.	Рязаньэнерго	Филиал	390013, г. Рязань ул. Могэс, д. 12
8.	Тулэнерго	Филиал	300012, г. Тула, ул. Тимирязева, д. 101а
9.	Удмуртэнерго	Филиал	426004, Удмуртская Республика, г. Ижевск, ул. Советская, д. 30

Перечень информационных систем (далее – ИС), входящих в границы оказания услуги приведен в Таблице 2.

Таблица 2. Перечень информационных систем, входящих в границы услуги

№ п/п	Наименование ИС	Тип ИС	Количество экземпляров ИС и ее расположение	Количество необходимых комплектов ОРД
1.	АСДТУ	ЗОКИИ, 2 категория значимости	9, на объектах п. 1 - 9 Табл. 1	9 (девять)
2.	ИВК на базе ПО «Пирамида – Сети»	ЗОКИИ, 2 категория значимости	9, на объектах п. 1 - 9 Табл. 1	9 (девять)
3.	ИВК на базе ПО «Пирамида – Сети»	ИСПДн	9, на объектах п. 1 - 9 Табл. 1	9 (девять)
4.	Система контроля управления доступом (СКУД)	ИСПДн	9 (все объекты Табл. 1)	9 (девять)
5.	ПО КИСУР (Управление персоналом)	ИСПДн	1, на объекте п. 6 Таблицы 1	1 (один)

4.2. Исполнитель обязан оказать услугу в составе и объеме, указанном в Таблице 3.

Таблица 3. Описание услуги

№ п/п	Наименование	Отчетная документация	Начало этапа	Окончание этапа
1	Актуализации разработки организационно-распорядительной и технической документации для систем ИСПДн и ЗОКИИ			

1.1	Экспертный аудит (сбор первичной информации) в объеме, предусмотренном п. 4.3.	-	03.12.2026	07.12.2026
1.2	Разработка и актуализация организационных и технических мер по обеспечению безопасности систем ИСПДн и ЗОКИИ	Комплекты проектов организационно-распорядительной и технической документации по защите информации, в соответствии с п. 4.4	08.12.2026	18.12.2026

Все работы в рамках оказания услуги проводятся в удаленном (дистанционном формате).

4.3. Экспертный аудит проводится Исполнителем с целью получения актуальных объективных качественных и количественных оценок о текущем состоянии информационной безопасности в информационных системах в соответствии с определенными критериями и показателями безопасности (аудит информационной безопасности).

Экспертный аудит информационной безопасности проводится в форме запросов либо интервью с должностными лицами организации Заказчика, полученная информация фиксируется в опросных листах. Инструментальное обследование силами Исполнителя не проводится.

В рамках экспертного аудита Заказчик по запросу Исполнителя предоставляет необходимую документацию в срок не более 2 (двух) рабочих дней.

Экспертный аудит должен состоять из следующих этапов:

– сбор общей информации об организации Заказчика:

- реквизиты, штатное расписание, образец приказа;
- инструкции по делопроизводству, номенклатура дел;
- нормативные документы, регламентирующие деятельность организации Заказчика и обработку защищаемой информации (копия устава, приказы, положения);

– проведение анкетирования сотрудников организации Заказчика, участвующих в процессах обработки и обеспечения безопасности защищаемой информации, определение ответственных лиц;

– сбор документов, необходимых для организационного обеспечения защиты информации, анализ их актуальности;

4.3.1. Заказчик предоставляет Исполнителю следующую информацию в части АРМ и серверов (физических и виртуальных), задействованных в обработке защищаемой информации:

– Сетевое имя;

– Расположение (физический адрес, номер помещения);

– Операционная система;

– Процессор;

– Материнская плата;

– Объем оперативной памяти;

– Модель накопителей (HDD/SSD);

– Модель видеоадаптера;

– Модель монитора;

– Модель клавиатуры;

– Модель манипулятора «мышь»;

– Список установленных СЗИ;

– Перечень программных комплексов.

4.3.2. Заказчик предоставляет Исполнителю следующую информацию в части информационных систем согласно таблице №2 Технического задания:

– сведения о передаче защищаемой информации третьим лицам;

– сведения о коммутационном оборудовании, задействованные в обработке защищаемой информации (наименование, модель, разработчик, место размещения);

– выявление установленных СЗИ/СКЗИ на АРМ и серверах, участвующих в обработке защищаемой информации (с запросом эксплуатационной документации);

– формирование списка сотрудников, имеющих доступ к АРМ и серверам, участвующих в обработке защищаемой информации;

– проведение обследования помещений (документальное): формирование списка помещений, где осуществляется обработка защищаемой информации с помощью средств вычислительной техники (определение границ контролируемой зоны);

– выявление мест хранения защищаемой информации на материальных носителях и формирование списка сотрудников, имеющих доступ к материальным носителям (документальное).

4.3.3. Заказчик обязуется предоставить исполнителю следующие сведения для каждого ОКИИ:

– Точные наименования ОКИИ;

– Техническую документацию на ОКИИ;

– Адреса размещения объекта;

– Архитектура объекта (одноранговая сеть, клиент-серверная система, технология

"тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура);

– Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта;

– Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии);

– Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи

– Наименование оператора связи и (или) провайдера хостинга;

– Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель);

– Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводный), протоколов взаимодействия;

– Наименования программно-аппаратных средств (с указанием моделей и производителей пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество;

– Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии);

– Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (прикладные программы, входящие в состав дистрибутивов операционных систем, не указываются);

– Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) с указанием наименования моделей и производителей средств защиты информации, реквизитов сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки, или сведения об отсутствии средств защиты информации;

– Данные для формирования обоснования показателей категории значимости.

4.3.4. Заказчик должен обеспечить возможность внесения Исполнителем полученной в процессе аудита информации в Программу для ЭВМ (Специализированное ПО) с целью формирования актуального комплекта проектов документов по защите информации, полностью соответствующего требованиям законодательства Российской Федерации в сроки в соответствии с план-графиком оказания услуг (Табл.3). Заказчик обеспечивает доступ Исполнителя к Специализированному ПО для управления процессами и мероприятиями по защите информации со следующим функционалом:

- набор функциональных возможностей, направленный на реализацию мер по обеспечению безопасности ПДн;
- набор функциональных возможностей, направленный на реализацию мер по обеспечению безопасности информации в соответствии с действующим законодательством Российской Федерации в области защиты информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений;
- набор функциональных возможностей, направленный на реализацию мер по категорирование ОКИИ;
- набор функциональных возможностей, направленный на реализацию мер по обеспечению безопасности значимых ОКИИ;
- набор функциональных возможностей, направленный на реализацию мер по планированию и контролю мероприятий по защите информации;
- набор функциональных возможностей, направленный на реализацию мер по регистрации инцидентов информационной безопасности;
- набор функциональных возможностей, направленный на реализацию мер по контролю за деятельностью по защите информации в курируемых организациях.
- набор функциональных возможностей, направленный на реализацию мер по управлению задачами по защите информации.

4.3.5. Предварительными границами экспертного аудита являются ИС, приведенные в Таблице 2.

Границы экспертного аудита уточняются Исполнителем во время оказания услуг и могут быть скорректированы по согласованию с Заказчиком.

4.4. По результатам экспертного аудита Исполнитель должен разработать и/или актуализировать комплекты проектов организационно-распорядительной и технической документации по защите информации. В состав комплекта входят:

4.4.1 Для систем ЗОКИИ:

1) Приказ о назначении заместителя руководителя организации, ответственного за обеспечение информационной безопасности организации;
2) Приказ и Положение о заместителе руководителя организации, ответственного за обеспечение информационной безопасности организации;
3) Приказ о структурном подразделении, осуществляющем функции по обеспечению информационной безопасности;
4) Приказ и Положение о структурном подразделении, осуществляющем функции по обеспечению информационной безопасности организации;
5) Приказ о комиссии по категорированию объектов критической информационной инфраструктуры;
6) Приказ об утверждении Положения о комиссии по категорированию объектов критической информационной инфраструктуры;
7) Приказ об утверждении перечня объектов критической информационной инфраструктуры, подлежащих категорированию;
8) Акт категорирования объекта критической информационной инфраструктуры;
9) Сведения о результатах присвоения объекту критической информационной инфраструктуры категории значимости;
10) Приказ о создании комиссии по контролю состояния обеспечения безопасности КИИ;
11) Приказ о силах обеспечения безопасности значимых объектов критической информационной инфраструктуры (при наличии значимых объектов КИИ);
12) Приказ об установлении контролируемой зоны;
13) Приказ о сотрудниках, ответственных за выявление инцидентов информационной безопасности и реагирование на них;
14) Приказ о сотрудниках, которым разрешены действия по внесению изменений в конфигурацию значимого объекта КИИ;
15) Приказ о назначении администратора безопасности объектов КИИ (при наличии значимых объектов КИИ);
16) Приказ об ответственном за планирование и контроль мероприятий по обеспечению информационной безопасности (при наличии значимых объектов КИИ);
17) Приказ об ответственном за управление (администрирование) подсистемой безопасности (системой защиты информации) (при наличии значимых объектов КИИ);
18) Перечень сотрудников, допущенных до компонентов КИИ;

19) Перечень помещений с компонентами КИИ;
20) Перечень ресурсов сети "Интернет", с которыми могут взаимодействовать значимые объекты, включающего исходящий и входящий сетевые потоки, их характеристики и используемые протоколы (далее – матрица коммуникаций значимых объектов с сетью "Интернет");
21) Определение сетевых адресов, с которыми должно быть обеспечено взаимодействие значимых объектов, формирование списка разрешенных сетевых адресов в условиях реализации атак, направленных на отказ в обслуживании;
22) Политика обеспечения безопасности ЗОКИИ;
23) Регламент идентификации и аутентификации (ИАФ)[1];
24) Регламент управления доступом (УПД) [1];
25) Регламент защиты машинных носителей информации (ЗНИ) [1];
26) Регламент аудита информационной безопасности (АУД) [1];
27) Регламент антивирусной защиты (АВЗ) [1];
28) Регламент обеспечения целостности (ОЦЛ) [1];
29) Регламент обеспечения доступности (ОДТ) [1];
30) Регламент защиты технических средств и систем (ЗТС) [1];
31) Регламент защиты информационной (автоматизированной) системы и ее компонентов (ЗИС) [1];
32) Регламент реагирования на компьютерные инциденты (ИНЦ) [1];
33) Регламент управления конфигурацией информационной (автоматизированной) системы (УКФ) [1];
34) Регламент управления обновлениями программного обеспечения (ОПО) [1];
35) Регламент планирования мероприятий по обеспечению защиты информации (ПЛН) [1];
36) Регламент обеспечения действий в нештатных ситуациях (ДНС) [1];
37) Регламент информирования и обучения персонала (ИПО) [1];
38) Матрица разграничения доступа;
39) План действий в нештатных ситуациях;
40) Должностные инструкции лиц, ответственных за обеспечение безопасности Объекта защиты;

[1] Для формирования регламентов в соответствии с п. 4.1.1. и номерами документов № 23-37 необходимо чтобы Заказчик предоставил Техническое задание на систему защиты ЗОКИИ и документы к Техническому проекту на систему защиту ЗОКИИ.

41) Порядок взаимодействия с провайдером хостинга или организацией, предоставляющей услуги связи;
42) Инструкция (администратора ИБ, пользователей по работе со стационарными и с мобильными АРМ);
43) Приказ о назначение лица ответственного за взаимодействие с НКЦКИ;
44) Регламент взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)/Положение о внешнем взаимодействие при обеспечении безопасности КИИ;
45) План реагирования на КИ и КА;
46) Сопроводительное письмо ФСТЭК с результатами категорирования;
47) Модель угроз безопасности информации;
48) Модель угроз безопасности информации, обрабатываемой в информационной системе с использованием средств криптографической защиты информации;
49) Регламент оценки показателя КЗИ;
50) Акт оценки показателя состояния технической защиты информации и обеспечения безопасности объектов информатизации;
51) Ежегодный план мероприятий по обеспечению безопасности ЗОКИИ (отдельные планы мероприятий в подразделениях).

4.4.2 Для систем ИСПДн:

1) Приказ о допуске сотрудников к обработке ПДн в ИСПДн;
2) Приказ о назначении ответственных (за ЗИ, за организацию работы с ПДн, администраторов, реагирование на инциденты, внесение изменений в конфигурацию и др.);
3) Приказ о порядке доступа в помещения, в которых обрабатывается защищаемая информация ИСПДн (серверные, рабочие помещения);
4) Приказ «О назначении комиссии по определению уровня защищенности информационных систем персональных данных»;
5) Приказ «Об утверждении перечня помещений (мест хранения материальных (бумажных и машинных) носителей защищаемой информации и персональных данных»;
6) Приказ «Об утверждении перечня сотрудников, осуществляющих обработку персональных данных»;
7) Приказ «Об утверждении перечня персональных данных, обрабатываемых в ИСПДн»;

8) Приказ «Об утверждении перечня информационных систем персональных данных»;
9) Приказ «О назначении ответственных за организацию работ по криптографической защите информации»
10) Приказ «Об утверждении Инструкций по организации криптографической защиты информации»;
11) Приказ «Об определении границ контролируемой зоны»;
12) Приказ «Об утверждении Инструкции по организации парольной защиты»;
13) Приказ «Об утверждении Инструкции администратора безопасности информационных систем»;
14) Приказ «Об утверждении Инструкции по обеспечению информационной безопасности»;
15) Приказ «Об утверждении Инструкции по организации антивирусной защиты»;
16) Приказ «Об утверждении перечня лиц, имеющих доступ в помещения, содержащие серверное и телекоммуникационное оборудование»;
17) Приказ «Об утверждении плана внутренних проверок <наименование юридического лица>»;
18) Политика в отношении обработки ПДн;
19) Положение о порядке обработки и защите информации в ИСПДн;
20) Инструкция по организации антивирусной защиты ИСПДн;
21) Инструкция по применению парольной политики в ИСПДн;
22) Инструкция по работе с носителями информации ИСПДн;
23) Инструкция ответственного за организацию обработки ПДн ИСПДн;
24) Инструкция администратора информационной безопасности ИСПДн;
25) Инструкция о порядке реагирования на инциденты информационной безопасности в ИСПДн;
26) Порядок доступа в помещения, где осуществляется обработка ПДн;
27) Порядок внесений изменений в конфигурацию ИСПДн и СЗИ;
28) Регламент разграничения прав доступа на объект информатизации;
29) Журнал инструктажа по защите информации в ИСПДн;
30) Журнал учета СЗИ, СКЗИ и эксплуатационной документации ИСПДн;
31) Журнал учета носителей информации ИСПДн;
32) Журнал учета изменений в конфигурации ИСПДн и СЗИ;
33) Перечень помещений, в которых обрабатывается защищаемая информация ИСПДн, порядок доступа к ним;
34) Перечень лиц, допущенных к обработке ПДн;

35) Перечень защищаемой информации ИСПДн;

36) Акт определения уровня защищенности объекта;

37) Акт оценки вреда субъектам ПДн;

38) Модель угроз безопасности информации;

39) Модель угроз безопасности информации, обрабатываемой в информационной системе с использованием средств криптографической защиты информации;

40) Разрешительная система (матрица) доступа к защищаемым ресурсам ИСПДн;

41) План мероприятий по защите информации в ИСПДн.

Разработка и/или актуализация ОРД и технической документации должна производиться Исполнителем в объеме предоставленных Заказчиком на этапе аудита данных.

Состав комплекта и наименования отдельных документов могут быть изменены по согласованию с Заказчиком. Проекты документов, указанные в п. 4.4, могут быть переданы Заказчику в формате Р7-Офис посредством электронной почты (за исключением документов ограниченного доступа) или на CD/DVD носителе.

5. Требования к организации оказания услуг

5.1. Заказчик на время оказания Услуги обеспечивает доступность следующих Работников Заказчика:

- Работников, ответственных за эксплуатацию ИС и функциональных заказчиков ИС;
- Куратора услуги со стороны Заказчика;

5.2. Исполнитель на время оказания услуги обеспечивает предоставление со своей стороны Сервис-менеджера, являющегося куратором услуги со стороны Исполнителя.

5.3 Исполнитель и Заказчик предоставляют контакты ответственных исполнителей в течение 2 (двух) рабочих дней с момента заключения договора.

5.4 На этапе проведения Экспертного аудита ИС Заказчик обеспечивает доступность и возможность своевременного проведения удаленных собеседований с работниками заказчика, имеющими необходимые права доступа в ИС для сбора информации о текущей конфигурации ИС и особенностях ее эксплуатации и функционала.

6. Сроки оказания услуг

6.1. Начало оказания услуг: с 03.12.2026.

6.2. Окончание оказания услуг: в соответствии с Таблицей 3. Описание услуги, но не позднее 18.12.2026 г.

7. Требования по обеспечению режима конфиденциальности

7.1. В период оказания услуг и после их окончания Исполнитель не должен разглашать и использовать конфиденциальную информацию, принадлежащую Заказчику, перечень которой определен внутренним распорядительным документом Заказчика, которая может стать ему известной в ходе оказания услуг. Исполнитель несет ответственность за соблюдение этого требования в соответствии с Законодательством Российской Федерации.

8. Требования к Исполнителю

8.1. Исполнитель должен обладать действующей лицензией Федеральной службы по техническому и экспортному контролю (ФСТЭК России) на деятельность по технической защите конфиденциальной информации со следующими обязательными видами работ и услуг:

- контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- проектирование средств и систем защиты информации.

8.2. Исполнитель обязан привлечь к работе со Специализированным ПО не менее 3 (трех) специалистов, успешно прошедших обучение по работе с данным программным комплексом. Копии действующих сертификатов специалистов предоставляются Заказчику в течение 3 (трех) рабочих дней с момента заключения Договора, но строго до момента начала оказания услуг.

9. Меры по предоставлению национального режима

Основание: постановление Правительства Российской Федерации от 23.12.2024 № 1875 «О мерах по предоставлению национального режима при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, закупок товаров, работ, услуг отдельными видами юридических лиц».

Предоставление национального режима в соответствии с ПП 1875 от 23.12.2024.	
ОКПД 2	Мера применения национального режима (запрет, ограничение, преимущество)
74.90.20.149	Не применяется*

*Запрет по строке 146 Приложения №1 постановления Правительства Российской Федерации от 23.12.2024 № 1875 устанавливается в отношении Программ для электронной вычислительной машины и (или) баз данных. Настоящая закупка проводится на право заключения договора на оказание услуг по актуализации и автоматизации разработки организационно-распорядительной и технической документации и внутренних нормативных документов для систем ИСПДн и ЗОКИИ ПАО «Россети Центр и Приволжье».

В рамках настоящей закупочной процедуры Программы для электронной вычислительной машины и (или) базы данных не закупаются.