

УТВЕРЖДАЮ
Заместитель министра
труда и социального развития
Краснодарского края

_____ Н.А. Киселева

«_____» _____ 20__ г.

Описание объекта закупки
оказание услуг по документальному и техническому обеспечению
деятельности информационных систем персональных данных министерства
труда и социального развития Краснодарского края

№ п/ п	Наименование закупаемых услуг, товаров, работ, входящих в объект закупки	Код по ОКПД2 / Код позиции КТРУ ¹	Требования, установленные к функциональным, техническим характеристикам закупаемых услуг, товаров, работ, входящих в объект закупки	Требования, установленные к качественным характеристикам закупаемых услуг, товаров, работ, входящих в объект закупки	Ед. изм.	Необ ходи мый объе м, коли честв о
1	2	3	4	5	6	7
1.	Услуги по предоставлению сертификата активации сервиса совместной технической поддержки уровень – Расширенный, для защищенной сети ViPNet № 541 ²	62.02.30.000/ -	В соответствии с Приложением № 2 к описанию объекта закупки	В соответствии с Приложением № 2 к описанию объекта закупки	Условн ая единиц а	1
2.	Услуги по предоставлению сертификата активации сервиса совместной	62.02.30.000/ -	В соответствии с Приложением № 2 к	В соответствии с Приложением № 2 к описанию объекта	Условн ая	1

№ п/п	Наименование закупаемых услуг, товаров, работ, входящих в объект закупки	Код по ОКПД2 / Код позиции КТРУ ¹	Требования, установленные к функциональным, техническим характеристикам закупаемых услуг, товаров, работ, входящих в объект закупки	Требования, установленные к качественным характеристикам закупаемых услуг, товаров, работ, входящих в объект закупки	Ед. изм.	Необходимый объем, количество
	технической поддержки уровень – Расширенный, для защищенной сети ViPNet № 986 ²		описанию объекта закупки	закупки	единица	
3.	Услуги по техническому обеспечению защищенной сети	74.90.20.149/ -	В соответствии с Приложением № 1 к описанию объекта закупки	В соответствии с Приложением № 1 к описанию объекта закупки	Месяц	12
4.	Услуги по техническому обеспечению подсистемы защиты от несанкционированного доступа и средств электронной подписи	74.90.20.149/ -	В соответствии с Приложением № 1 к описанию объекта закупки	В соответствии с Приложением № 1 к описанию объекта закупки	Месяц	12
5.	Услуги по регламентному обслуживанию защищенной сети	74.90.20.149/ -	В соответствии с Приложением № 1 к описанию объекта закупки	В соответствии с Приложением № 1 к описанию объекта закупки	Месяц	12
6.	Услуги по актуализации документации, регламентирующей обработку персональных данных	74.90.20.149/ -	В соответствии с Приложением № 1 к описанию объекта закупки	В соответствии с Приложением № 1 к описанию объекта закупки	Условная единица	4
7.	Услуги по аудиту документации, регламентирующей обработку персональных данных	74.90.20.149/ -	В соответствии с Приложением № 1 к описанию объекта закупки	В соответствии с Приложением № 1 к описанию объекта закупки	Условная единица	4
8.	Разработка комплекта организационно-распорядительной документации, регламентирующей защиту информации в соответствии с требованиями Приказа ФСТЭК №117	74.90.20.149/ -	В соответствии с Приложением № 1 к описанию объекта закупки	В соответствии с Приложением № 1 к описанию объекта закупки	Условная единица	1

¹ Общероссийский классификатор продукции по видам экономической деятельности ОК 034-2014 и каталог товаров, работ, услуг для обеспечения государственных и муниципальных нужд, размещенный в единой информационной системе в сфере закупок.

² В описании объекта закупки эквивалентность не указана в целях необходимости обеспечения взаимодействия приобретаемой технической поддержки с программным обеспечением используемым заказчиком (п. 1 ч. 1 ст. 33 Федерального закона от 05.04.2013 № 44-ФЗ), в настоящем извещении указание на товарные знаки не сопровождается словами «или эквивалент».

Перечень принятых сокращений и определений

АРМ	– автоматизированное рабочее место.
ООЗ	– описание объекта закупки.
ГИС	– государственная информационная система.
ИС	– информационная система.
ИСПДн	– информационная система персональных данных.
ПАК	– программно-аппаратный комплекс.
ПК	– программный комплекс.
ПО	– программное обеспечение.
СУ	– сетевой узел.
АП	– абонентский пункт.
ФАПСИ	– Федеральное агентство правительственной связи и информации при Президенте Российской Федерации.
ФСБ России	– Федеральная служба безопасности Российской Федерации.
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю.
Час	– в данном документе часом называется рабочий час, если явно не указано иное.
День	– в данном документе днем называется рабочий день, если явно не указано иное.
Контрольные сроки	нормативные сроки времени решения и времени реакции.
Срок реакции	– время, в течение которого Исполнитель обязуется приступить к работе над обращением Заказчика, способом, предусмотренным в описании объекта закупки.
Время предоставления решения	– определяется как временной интервал, необходимый специалистам Исполнителя для предоставления окончательного, приемлемого для Заказчика решения проблемы.
Время прибытия	– время от момента регистрации заявки до момента физического прибытия инженера на место возникновения инцидента.
Приоритет	– категория, используемая для определения относительной важности инцидента, проблемы или изменения. Приоритет базируется на влиянии и срочности и используется для определения контрольных сроков.

Эскалация	– деятельность, направленная на получение дополнительных ресурсов, когда это необходимо для достижения целевых показателей уровня услуги или удовлетворения ожиданий Заказчика.
Инцидент	– любое событие, не являющееся частью стандартных операций по предоставлению услуги, которое привело или может привести к нарушению или снижению качества этой услуги.
Запрос на обслуживание	– зафиксированное требование Заказчика на потребность в обслуживании в рамках предоставляемой услуги или компонентов, ее образующих, не являющееся инцидентом.
Ответственный представитель Заказчика	– сотрудник Заказчика, назначенный ответственным за информационную безопасность, а также за реагирование на инциденты ИБ, определенный ответственным за эксплуатацию программного обеспечения автоматизации мероприятий по организации обработки и защиты ПДн Заказчика.
Отчетный период	– срок длительностью с первого по последнее число каждого календарного месяца включительно.
Hotfix	– информация, предназначенная для автоматизированного внесения определённых изменений в программное обеспечение.
NAT	– от англ. Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов.
MAJOR	– основной номер версии или поколение продукта ViPNet. Одно поколение от другого может существенно отличаться по функциональным и нефункциональным возможностям, соответствовать разным уровням требований регуляторов рынка.
MINOR	– вспомогательный номер версии продукта ViPNet. Используется для различения версий продукта внутри одного поколения при исправлении выявленных дефектов (hotfix), а также несущественном изменении функциональности (service pack).
VPN	– Virtual private network.
СЗИ от НСД	– Средство защиты информации от несанкционированного доступа.
СКЗИ	– Средство криптографической защиты информации.

1. Общие сведения.

1.1 Полное наименование объекта закупки.

Оказание услуг по документальному и техническому обеспечению деятельности информационных систем персональных данных министерства труда и социального развития Краснодарского края на 2027 год (далее – услуги).

1.2 Заказчик.

Заказчиком услуг выступает министерство труда и социального развития Краснодарского края (далее – министерство).

Юридический адрес заказчика: 350000, г. Краснодар, ул. Чапаева, 58.

Адреса оказания услуг:

г. Краснодар, ул. Чапаева, 58;

г. Краснодар, ул. Зиповская, 5;

г. Краснодар, ул. Индустриальная, 12;

г. Краснодар, ул. Северная, 490;

г. Краснодар, 3-й Тихорецкий проезд, 15.

Министерство является оператором 52 (пятидесяти двух) сегментов государственных информационных систем, информационных систем персональных данных.

2. Состав услуг по документальному и техническому обеспечению.

2.1 Общие требования.

Услуги по документальному и техническому обеспечению включают в себя:

техническое обеспечение защищенной сети министерства;

техническое обеспечение подсистемы защиты от несанкционированного доступа и средств электронной подписи;

регламентное обслуживание защищенной сети;

актуализацию документации, регламентирующей обработку персональных данных;

аудит документации, регламентирующей обработку персональных данных;

разработка комплекта организационно-распорядительной документации, регламентирующей защиту информации в соответствии с требованиями Приказа ФСТЭК № 117.

Услуги включают работы по установке и настройке средств защиты информации, ключевых документов, а также помощь в вводе данных при подаче запроса на создание сертификата электронной подписи в удостоверяющий центр министерства финансов Краснодарского края и помощь в вводе данных при подаче запроса на создание сертификата электронной подписи в удостоверяющий центр Федерального казначейства, необходимых для работы с информационными системами.

2.2 Основания оказания услуг.

Услуги оказываются на основании:

Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

Постановления Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 № 1119;

Приказа ФСБ России «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» от 10.07.2014 № 378;

Постановления Правительства Российской Федерации «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 № 687;

Постановления Правительства Российской Федерации «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» от 21.03.2012 № 211;

Приказа ФАПСИ России «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» от 13.06.2001 № 152;

Сборника руководящих документов по защите информации от несанкционированного доступа, Гостехкомиссия России, 1992 г.;

Приказа ФСТЭК России «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» от 11.04.2025 № 117;

Приказа ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21;

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».

Наличие факта эксплуатации в информационных системах министерства средств защиты информации.

3. Требования к техническому обеспечению.

3.1 . Состав технических и программных средств защиты информации министерства.

3.1.1. Подсистема межсетевого экранирования и защиты каналов связи министерства (далее – подсистема) предназначена для защиты компонентов ИС при взаимодействии со смежными и внешними сетями. Подсистема реализована с помощью компонентов защищенных сетей, построенных по технологии ViPNet (№ 541 и № 986) в следующем составе:

Защищённая сеть ViPNet № 541:

ПО ViPNet Prime – 1 шт.;

ПАК ViPNet Coordinator HW 5 Исполнение HW2000– 1 шт.;

ПАК ViPNet Coordinator HW 5 Исполнение HW1000 – 4 шт.;

ПО ViPNet Client 5 for Windows – 45 шт.;

ПО ViPNet Client 5 for Linux (+BM) – 250 шт.;

ПО ViPNet Client 4U for Android (KC1) – 1 шт.

Защищённая сеть ViPNet № 986:

ПО ViPNet Prime – 1 шт.;

ПАК ViPNet Coordinator HW 5 Исполнение HW2000 – 1 шт.;

ПАК ViPNet Coordinator HW 5 Исполнение HW1000 – 3 шт.;

ПО ViPNet Client 5 for Windows – 10 шт.;

ПО ViPNet Client 5 for Linux (+BM) – 75 шт.

3.1.2. Для защиты каналов связи при работе в государственных информационных системах, не принадлежащих министерству, в подсистеме используется ПО ViPNet Client for Windows 4.x (KC2) защищённых сетей ViPNet № 1274 – 2 шт. и ПО ViPNet Client 4U for Android (KC1) защищённой сети ViPNet № 2467 – 7 шт.

3.1.3. Совместно с подсистемой используются сертифицированные программные VPN-клиенты «Континент-АП» в количестве 2 шт.

3.1.4. Для защиты сетевого трафика, совместно с подсистемой, используется СКЗИ КриптоПро NGate.

3.1.5. Подсистема защиты от несанкционированного доступа реализована с помощью следующих компонентов:

программно-аппаратный комплекс «Соболь» – 156 шт.;

средство защиты от несанкционированного доступа «Secret Net Studio 8» – 100 шт.;

сервер безопасности «Secret Net Studio» – 1 шт.

3.1.6. В качестве средства электронной подписи используется СКЗИ КriptoПро CSP 5 – 260 шт. и СКЗИ «КriptoАРМ ГОСТ» – 10 шт.

3.2 Требования к техническому обеспечению защищенной сети министерства.

Защищенная сеть министерства представлена совокупностью двух объединенных виртуальных сетей, построенных по технологии ViPNet (номера сетей 541 и 986). Техническое обеспечение защищенной сети включает следующие работы:

- генерацию ключевой информации или изменение размещения существующих узлов ViPNet сети по заявкам Заказчика;

- обновление справочников СУ, переиздание сертификатов пользователей, списка отозванных сертификатов;

- настройку связей и задание полномочий для СУ ViPNet, переименование АП;

- настройку автопроцессинга, конфигурирование «Деловой почты защищенной сети»;

- удалённую настройку и изменение правил туннелирования;

- изменение настроек трансляции сетевых адресов (NAT);

- поддержку межсетевых взаимодействий с ViPNet сетями.

Поддержка межсетевых взаимодействий с другими ViPNet сетями включает в себя:

- обработку импорта от смежных ViPNet сетей;

- обновление связей с узлами смежных ViPNet сетей;

- создание ответного экспорта для смежных ViPNet сетей;

- итоговое тестирование СКЗИ ViPNet.

Консультации по вопросам решения проблем функционирования защищенных СУ, в том числе консультации по переустановке программного обеспечения узлов защищенной сети в случае выхода АРМ из строя или программных сбоев по рабочим дням с 9:00 до 18:00 (московское время).

При оказании услуг по техническому обеспечению защищенной сети министерства Заказчик и Исполнитель руководствуются порядком взаимодействия при обработке обращений, определённым разделе 3.5 настоящего приложения к ООЗ.

Исполнитель отражает результаты работ по техническому обеспечению защищенной сети в периодической отчетности. Требования к предоставлению отчетности представлены в разделе 7 настоящего приложения к ООЗ.

На аппаратные и программные решения ViPNet, входящие в состав подсистемы межсетевого экранирования и защиты каналов связи министерства, перечисленные в разделе 3.1.1, предоставлена техническая поддержка производителя уровня «Совместная Расширенная» на следующий день по окончании срока действия имеющейся у Заказчика технической поддержки производителя уровня «Совместная Расширенная», на срок 12 месяцев, подтвержденная сертификатом. Оригиналы сертификатов, выданные производителем, Исполнитель предоставляет Заказчику на следующий день по

окончании срока действия сертификата технической поддержки продуктов ViPNet.

В рамках действия сертификата «Совместной Расширенной» технической поддержки производителя продукции ViPNet, Исполнитель:

предоставляет обновления (hotfix), выпущенных производителем, устраняющие дефекты, выявленные в оборудовании и программном обеспечении центрального узла;

предоставлять обновления (hotfix), а также все изменения, производимые в рамках минорных (MINOR) версий ViPNet, выпущенных производителем для оборудования и программного обеспечения центрального узла;

предоставлять новые версии (изменения мажорной (MAJOR) версии поколения) ViPNet, выпущенных производителем для оборудования и программного обеспечения центрального узла без взимания дополнительной платы (для ПАК – только программные компоненты);

обеспечивать консультации производителя по «горячей» телефонной линии и по электронной почте по рабочим дням с 9:00 до 18:00 (московское время).

Услуга по техническому обеспечению защищенной сети включает в себя следующие работы:

установку и настройку программного обеспечения ViPNet собственных и иных защищенных сетей, используемых министерством, программных и программно-аппаратных средств защиты информации, перечисленных в разделах 3.1.1 - 3.1.4 настоящего приложения к ООЗ, ключевых документов, ПО для установки и настройки предоставляются Заказчиком;

установку сертификатов проверки электронных подписей (не более 500 установок в течение срока оказания услуг);

устранение неполадок в работе средств защиты информации, перечисленных в разделах 3.1.1 - 3.1.4 настоящего приложения к ООЗ по заявкам (дистанционно или с выездом не позднее максимальных сроков, установленных в Таблице 4).

В течение срока действия контракта, при выполнении работ по установке и/или переустановке СКЗИ, а также при оказании помощи в подаче запроса на создание сертификата электронной подписи, Исполнитель обеспечивает внесение в файл учета соответствующих изменений и дополнений в целях актуализации сведений, предусмотренных его структурой.

Исполнитель формирует файл учета, включающий следующие разделы:

1. Учет электронных подписей (ЭП).
2. Учет СКЗИ.

В файле учета в обязательном порядке отражаются следующие сведения:

Таблица 1. Учет электронных подписей (ЭП)

ФИО	Серийный номер сертификата ЭП	Дата получения/подключения	№ токена	Дата запроса	№ запроса	Комментарий

Таблица 2. Учет СКЗИ

Наименование СКЗИ	ФИО пользователя ПЭВМ	Место установки, адрес, кабинет	Серийный номер (инвентарный номер) ПЭВМ/сервера	ПЭВМ опломбирован (номер)	Дата установки	Серийный номер СКЗИ	Номер экземпляра (лицензия)	Регистрационный номер крипто средства (ПАК)	Комментарий
-------------------	-----------------------	---------------------------------	---	---------------------------	----------------	---------------------	-----------------------------	---	-------------

При оказании услуг по техническому обеспечению средств криптографической защиты информации Заказчик и Исполнитель руководствуются порядком взаимодействия сторон при обработке обращений, определённым разделе 3.5 настоящего приложения к ООЗ.

Исполнитель отражает результаты работ по техническому обеспечению средств криптографической защиты информации в периодической отчетности. Требования к предоставлению отчетности представлены в разделе 6 настоящего приложения к ООЗ.

3.3 Требования к техническому обеспечению подсистемы защиты от несанкционированного доступа и средствам электронной подписи.

Техническое обеспечение подсистемы защиты от несанкционированного доступа выполняется Исполнителем и включает в себя следующие услуги:

установку, настройку, диагностику и устранение неполадок с СЗИ от НСД ПАК «Соболь»;

установку, настройку, диагностику и устранение неполадок СЗИ от НСД «Secret Net Studio»;

установку, настройку, диагностику и устранение неполадок СКЗИ «КриптоПРО CSP»;

установку, настройку, диагностику и устранение неполадок СКЗИ «КриптоАРМ ГОСТ»;

устранение неполадок в работе средств защиты информации, перечисленных в разделах 3.1.5 - 3.1.6 настоящего приложения к ООЗ по заявкам (дистанционно или с выездом в согласованные сроки).

Исполнитель отражает результаты работ по техническому обеспечению подсистемы защиты от несанкционированного доступа в периодической отчетности. Требования к предоставлению отчетности представлены в разделе 6 настоящего приложения к ООЗ.

3.4 Требования к регламентному обслуживанию защищенной сети

Исполнитель проводит регламентное обслуживание не менее одного раз в месяц по адресам, указанным в разделе 1.2 настоящего приложения к ООЗ. Комплекс мероприятий предусматривает выполнение следующего объема работ:

Для ПАК ViPNet Coordinator HW 5 Исполнение HW2000/HW1000:

проверка доступности узлов защищенной сети;

проверка логов оборудования;

- проверка работы всех служб;
- анализ журналов аудита, фильтрации трафика и журналов регистрации сетевых пакетов;
- создание резервной копии конфигурации.

Для ViPNet Prime:

- создание снимка, резервных копий конфигурации защищенных сетей ViPNet № 541 и № 986;
- плановые обновления ключей шифрования, справочников и другой служебной информации;
- проверка корректной работы всех компонентов сетей ViPNet № 541 и № 986.

Исполнитель отражает результаты выездов по регламентному профилактическому обслуживанию в периодической отчетности. Требования к предоставлению отчетности представлены в разделе 6 настоящего приложения к ООЗ.

По завершении срока оказания услуг Исполнитель предоставляет Заказчику все резервные копии, конфигурационные файлы в электронном виде на цифровом носителе, собранные в ходе регламентного обслуживания.

3.5 . Требования к порядку постоянного технического обеспечения.

3.5.1. Общие требования.

Исполнитель обеспечивает единую точку контакта для оказания услуг, приема обращений, их обработку и подготовку решений на них на весь срок действия контракта. Интерфейсами взаимодействия единой точки контакта должны выступать:

- дистанционная система формирования и отслеживания выполнения заявок по сопровождению (далее – сервисная система);

- услуга «8-800 Бесплатные звонки»;

- электронная почта.

Исполнитель в течение 1 (одного) рабочего дня с даты заключения контракта предоставляет Заказчику:

- доступ к сервисной системе;

- адрес электронной почты информационно-технического сопровождения;

- номер телефона «горячей» линии.

Сервисная система позволяет Заказчику:

- формировать заявки на техническую поддержку и отслеживать ход их выполнения;

- реализовать возможность создания заявок нескольких типов;

- добавлять к обращению снимки экрана в форматах файлов .jpg, .jpeg, .png;

- организовывать онлайн обмен сообщениями с специалистами

Исполнителя;

- проводить оценку исполнения заявки на информационно-техническое сопровождение.

Минимальные требования к интерфейсу сервисной системы:

наличие формы для создания заявки на оказание информационно-технического сопровождения;

наличие формы выбора типа обращения;

наличие реестра активных заявок на исполнение.

Форма для создания заявки включает поля для ввода темы обращения и описания проблемы.

При обработке заявки на разных этапах (принятие в работу, решение и закрытие заявки), все этапы сопровождаются уведомлениями на адрес электронной почты ответственных представителей со стороны Заказчика, имеющих право подтверждения закрытия заявки.

Исполнить обеспечивает оказание телефонных консультаций пользователей Заказчика с 9:00 до 18:00 (московское время) в рабочие дни.

3.5.2. Требования к приоритетам инцидентов.

В процессе регистрации заявки, Исполнитель классифицирует обращения по типам «Инцидент», «Запрос на обслуживание» и присвоить ему приоритет.

Приоритет обработки Заявок определяется отдельно для каждого типа заявки «Инцидент» и «Запрос на обслуживание».

Заявкам типа «Инцидент» присваивается один из следующих приоритетов:

Критический – сбой подсистемы затронул работу всех пользователей, недоступность несет значительную угрозу непрерывности предоставления министерством государственных услуг.

Высокий – серьезный инцидент, ведущий к высокому риску непрерывности предоставления министерством государственных услуг. Недоступность затрагивает более 10 пользователей.

Стандартный – подсистемы функционируют в штатном режиме, но часть функций работает некорректно. Инцидент не оказывает значительного влияния на выполнение текущих задач министерства.

Низкий – подсистемы функционируют в штатном режиме. Инцидент слабо влияет на выполнение текущих задач министерства.

Приоритет «Запроса на обслуживание» определяется на основе его влияния и срочности с помощью матрицы приоритетов (Таблица 3). Влияние запроса указывает на потенциальный ущерб или эффект, который наносится пользователю (Инициатору запроса). Срочность запроса определяется Инициатором.

Таблица 3. Определение приоритета заявки типа «Запрос на обслуживание»

		Влияние		
		Министерство	Отдел	Персона
Срочность	Критическая	Критический	Критический	Высокий
	Высокая	Критический	Высокий	Средний
	Средняя	Высокий	Средний	Стандартный
	Низкая	Средний	Средний	Стандартный

Заявки обрабатываются Исполнителем с учетом приоритетов:
 в первую очередь обрабатываются заявки с приоритетом «Критический»;
 во вторую очередь обрабатываются Заявки с приоритетом «Высокий»;
 в третью очередь обрабатываются Заявки с приоритетом «Средний»;
 в случае отсутствия в очереди Заявок с приоритетами «Критический», «Высокий», «Средний», обрабатываются заявки с приоритетом «Стандартный».

Если в очереди находятся несколько заявок одинакового приоритета, в первую очередь обрабатывается заявка с ближайшим сроком исполнения. Нормативные сроки исполнения заявок указаны в разделе 3.5.3 настоящего приложения к ООЗ.

3.5.3. Требования к срокам обработки заявок.

При оказании технического сопровождения Исполнитель обеспечивает очередность обработки заявок в соответствии с контрольными сроками, установленными в Таблице 4.

Таблица 4. Контрольные сроки исполнения заявок типа «Инцидент» и «Запрос на обслуживание».

Наименование параметра	Приоритет	Срок реакции, не более	Максимальное время прибытия	Срок решения, не более
Нормативные сроки исполнения Инцидентов	Критический	20 мин.	60 мин.	8 час**
	Высокий	40 мин.	90 мин.	12 час**
	Средний	60 мин.	120 мин.	24 час**
Нормативные сроки исполнения Запросов на обслуживание	Критический	120 мин.	120 мин.*	12 час**
	Высокий	120 мин.	120 мин.*	24 час**
	Средний	120 мин.	120 мин.*	40 час**
	Стандартный	120 мин.	120	40 час**

	й		мин.*	
--	---	--	-------	--

Заказчик вправе потребовать повышения приоритета в случае, если «Инцидент» приоритета уровня «Стандартный» носит повторяющийся характер.

**В случаях, когда Исполнитель не имеет возможности исполнения удаленно, Исполнитель организует экстренный выезд специалистов.*

***В случаях, если для решения проблемы требуется принятие каких-либо действий от третьих лиц (не заказчика и не исполнителя) то контрольные сроки при этом не учитываются до совершения таких действий третьими лицами.*

Если в ходе устранения Инцидента приоритета «Критический» применено обходное решение – приоритет понижается до уровня «Высокий». Обходное решение – уменьшение или устранение влияния инцидента или проблемы, для которых в текущий момент недоступно полное разрешение.

В случае несогласия инициатора с результатами обработки обращения или претензией по качеству, инициатор сообщает об этом в течение 3 (трех) рабочих дней с даты предоставления решения по обращению, после чего существующее обращение открывается повторно, и его обработка продолжается. В случае отсутствия комментариев инициатора по истечении 3 (трех) рабочих дней с даты предоставления решения обращения, текущую заявку Исполнитель окончательно закрывает.

3.5.4. Требования к выезду специалистов.

Решение о необходимости выезда принимается специалистом Исполнителя, ответственным за решение проблемы, на основании данных, полученных от инициатора обращения, либо по результатам проведения предварительного расследования инцидента и согласуется с инициатором заявки.

Исполнитель обеспечивает уровень оперативности выполнения работ по настоящему приложению к ООЗ путем гарантированного прибытия специалиста по адресу проведения работ не позднее максимальных сроков, установленных в Таблице 4.

По результатам проведенных работ составляется Акт о выполнении работ, согласованный с Заказчиком, который подписывается со стороны Исполнителя сотрудником, проводившим работы, а со стороны Заказчика ответственным представителем Заказчика. В Акте фиксируются перечень работ и общее время нахождения специалиста Исполнителя на объекте.

Исполнитель отражает результаты работ по выездам в периодической отчетности. Требования к предоставлению отчетности представлены в разделе 7 настоящего приложения к ООЗ.

4. Требования к актуализации документации, регламентирующей обработку персональных данных.

Ежеквартальные услуги по документальному обеспечению деятельности по защите ПДн Заказчика включают:

ведение и поддержание в актуальном состоянии исходных данных, для формирования локальных нормативно-правовых актов Заказчика по защите ПДн;

проведение классификации ГИС, установление УЗ ИСПДн с выдачей Заказчику исполненных актов классификации ГИС, актов установления уровня защищенности ИСПДн и поддержание их в актуальном состоянии;

разработку и актуализацию технического паспорта информационных систем;

поддержание в актуальном состоянии журнала учета машинных носителей персональных данных;

ведение и поддержание в актуальном состоянии модели угроз безопасности информации и модели нарушителя;

ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

Исполнитель отражает перечень разработанной и актуализированной организационно-распорядительной документации в периодической отчетности. Требования к предоставлению отчетности представлены в разделе 7 настоящего приложения к ООЗ.

5. Требования к аудиту документации, регламентирующей обработку персональных данных.

Аудит документации, регламентирующей обработку персональных данных, проводится специалистами Исполнителя. Продолжительность проведения аудита документального обеспечения деятельности по обработке ПДн не превышает 21 рабочий день.

Аудит документального обеспечения деятельности по обработке ПДн проводится в несколько этапов. На первом этапе специалистами Исполнителя проводятся следующие мероприятия:

планирование работ по защите персональных данных с учетом условий Заказчика;

выявление условий обработки персональных данных и актуализация сведений об обработке персональных данных;

установление и актуализацию информации о распределении полномочий и ответственности за обработку и защиту персональных данных;

анализ корректности и достаточности документации, регламентирующей вопросы обработки ПДн;

сбор сведений об ИТ-инфраструктуре.

На втором этапе, по результатам проведения аудита, Исполнителем проводятся следующие мероприятия:

консультации по вопросам защиты персональных данных и при необходимости подготовка рекомендаций;

разработка аудиторского отчета на соответствие требованиям регуляторов с отражением замечаний и устранением замечаний прошлых проверок.

6. Требования к разработке комплекта организационно-распорядительной документации, регламентирующей защиту информации в соответствии с требованиями Приказа ФСТЭК №117.

Исполнитель 1 раз в период оказания услуг осуществляет сбор сведений об объекте информатизации, включая определение состава защищаемой информации, перечня информационных систем, технических средств и субъектов доступа к защищаемой информации. По результатам проведенного обследования Исполнитель разрабатывает организационно-распорядительную документацию в соответствии с требованиями Приказа ФСТЭК №117 в следующем составе:

1. Проект политики защиты информации.

2. Проект приказа об утверждении внутренних стандартов и регламентов по защите информации, включающий в себя в качестве приложений:

Стандарт идентификации и аутентификации пользователей информационных систем;

Стандарт конфигурирования и настройки программных, программно-аппаратных средств;

Стандарт сетевой безопасности и удаленного доступа;

Стандарт использования и обеспечения эксплуатации пользователями информационных систем;

Стандарт защиты устройств информационных систем;

Стандарт резервного копирования информации, обеспечения непрерывности функционирования и восстановления информационных систем;

Стандарт менеджмента событий безопасности информации и мониторинга информационной безопасности;

Стандарт подключения к информационным системам;

Регламент повышения уровня знаний и информированности по вопросам защиты информации;

Регламент устранения уязвимостей;

Регламент управления обновлениями;

Регламент обращения с информацией ограниченного доступа;

Регламент разработки безопасного программного обеспечения (в случае наличия технологии);

Регламент вывода в контур промышленной эксплуатации сервисов;

Регламент контроля уровня защищенности информации;

Порядок применения мер защиты информационных систем и обрабатываемой ими информации;

План мероприятий по защите информации;

Регламент использования беспроводных сетей (в случае наличия технологии);

Регламент защиты от компьютерных атак, направленных на отказ в обслуживании (в случае наличия технологии);

Регламент применения технологии искусственного интеллекта (в случае наличия технологии);

Регламент оценки состояния защиты информации.

3. Проект приказа об утверждении перечня разрешенного для использования программного обеспечения.

Исполнитель отражает перечень разработанной организационно-распорядительной документации в периодической отчетности. Требования к предоставлению отчетности представлены в разделе 7 настоящего приложения к ООЗ.

7. Требования к предоставлению отчетности по услугам сопровождения.

В результате выполнения услуг Исполнителем предоставляется Заказчику отчетность в соответствии с Таблицей 5.

Таблица 5. Параметры периодической отчетности.

№ п/п	Наименование документа	Требования к содержанию документа	Формат предоставления отчета	Сроки предоставления
1	Отчет об оказанных услугах	Документ, формируемый на основе работ, проведенных специалистами Исполнителя в течение месяца по устранению инцидентов, содержит информацию по оказанным услугам. Отчет по обращениям за технической поддержкой содержит разделы: 1. Детализация обращений, содержащая сведения: номер обращения; статус обращения; дату открытия обращения; информация о заявителе; содержание заявки; дата и время выполнения; краткое описание действий, проведенных специалистами Исполнителя. 2. Выполненные регламентные работы; 3. Раздел по результатам экстренных выездов; 4. Перечень актуализированной, разработанной ОРД; 5. Выводы и рекомендации.	На бумажном носителе, подписанный Исполнителем и Заказчиком.	Не позднее завершения отдельного этапа исполнения Контракта
2	Акт о выполнении работ на территории	Документ содержит описание работ, проведенных на территории Заказчика, в случае выезда специалистов Исполнителя.	На бумажном носителе, подписан	По факту устранения инцидента, но не

	Заказчика		Исполнителем и представителем Заказчика.	позднее контрольных сроков устранения инцидента, приведенных в Таблице Таблица 4.
3	Отчет по аудиту документации, регламентирующей обработку персональных данных	Документ, формируемый на основе работ, проведенных специалистами Исполнителя, отражающий соответствие требованиям регуляторов в области порядка обработки и персональных данных с отражением замечаний и устранением замечаний прошлых проверок	На бумажном носителе, подписан Исполнителем и представителем Заказчика.	Не позднее завершения отдельного этапа исполнения Контракта

Приложение № 2
к описанию объекта
закупки

**Требования,
установленные к функциональным и техническим характеристикам закупаемых
услуг, товаров, работ, входящих в объект закупки**

№ п/п	Наименование закупаемых услуг, товаров, работ, входящих в объект закупки	Требования, установленные к функциональным и техническим характеристикам закупаемых услуг, товаров, работ, входящих в объект закупки	
		Наименование показателя, ед. изм. показателя	Описание, значение
1	2	3	4
1.	Услуги по предоставлению сертификата активации сервиса совместной технической поддержки уровня – Расширенный, для защищенной сети ViPNet № 541 ¹	Приём обращений и консультирование по электронной почте в рабочие дни с 09:00 до 18:00 (московское время)	Соответствие
		Приём обращений и консультирование по телефону горячей линии в рабочие дни с 09:00 до 18:00 (московское время)	Соответствие
		Рекомендации по процессу установки и настройки продукта в объеме эксплуатационной документации	Соответствие
		Исправление ошибок и предоставление релизов с исправлениями в рамках версии	Соответствие
		Предоставление обновлений продуктов при выходе новых версий	Соответствие
		Время реакции на обращения пользователя для Инцидента уровня «Критичный», часов, не более	4
		Время реакции на обращения пользователя для Инцидента уровня «Средний», часов, не более	8
		Время реакции на обращения пользователя для Инцидента уровня «Низкий», часов, не более	12
		Продукты, на которые распространяется техническая поддержка: ПО ViPNet Prime – 1 шт.; ПАК ViPNet Coordinator HW 5 Исполнение HW2000– 1 шт.; ПАК ViPNet Coordinator HW 5 Исполнение HW1000 – 4 шт.; ПО ViPNet Client 5 for Windows – 45 шт.; ПО ViPNet Client 5 for Linux (+BM) – 250 шт.; ПО ViPNet Client 4U for Android (KC1) – 1 шт.	Соответствие
		Возможность функционирования с защищённой сетью передачи данных ViPNet № 541	Соответствие
2.	Услуги по предоставлению сертификата активации	Срок действия, месяцев	12
		Приём обращений и консультирование по электронной почте в рабочие дни с 09:00 до 18:00 (московское время)	Соответствие

№ п/п	Наименование закупаемых услуг, товаров, работ, входящих в объект закупки	Требования, установленные к функциональным и техническим характеристикам закупаемых услуг, товаров, работ, входящих в объект закупки	
		Наименование показателя, ед. изм. показателя	Описание, значение
1	2	3	4
	сервиса совместной технической поддержки уровень – Расширенный, для защищенной сети ViPNet № 986 ¹	Приём обращений и консультирование по телефону горячей линии в рабочие дни с 09:00 до 18:00 (московское время)	Соответствие
		Рекомендации по процессу установки и настройки продукта в объеме эксплуатационной документации	Соответствие
		Исправление ошибок и предоставление релизов с исправлениями в рамках версии	Соответствие
		Предоставление обновлений продуктов при выходе новых версий	Соответствие
		Время реакции на обращения пользователя для Инцидента уровня «Критичный», часов, не более	4
		Время реакции на обращения пользователя для Инцидента уровня «Средний», часов, не более	8
		Время реакции на обращения пользователя для Инцидента уровня «Низкий», часов, не более	12
		Продукты, на которые распространяется техническая поддержка: ПО ViPNet Prime – 1 шт.; ПАК ViPNet Coordinator HW 5 Исполнение HW2000 – 1 шт.; ПАК ViPNet Coordinator HW 5 Исполнение HW1000 – 3 шт.; ПО ViPNet Client 5 for Windows – 10 шт.; ПО ViPNet Client 5 for Linux (+BM) – 75 шт.	Соответствие
		Возможность функционирования с защищённой сетью передачи данных ViPNet № 986	Соответствие
		Срок действия, месяцев	12

¹ В описании объекта закупки эквивалентность не указана в целях необходимости обеспечения взаимодействия приобретаемой технической поддержки с программным обеспечением используемым заказчиком (п. 1 ч. 1 ст. 33 Федерального закона от 05.04.2013 № 44-ФЗ), в настоящем извещении указание на товарные знаки не сопровождается словами «или эквивалент»

Приложение № 3
к описанию объекта
закупки

План
оказания услуг по документальному и техническому обеспечению
деятельности информационных систем персональных данных
министерства труда и социального развития Краснодарского края

Предмет контракта	Этапы оказания услуг	Наименование услуг в каждом этапе	Единица измерения	Количество
Оказание услуг по документальному и техническому обеспечению деятельности информационных систем персональных данных министерства труда и социального развития Краснодарского края	с 01.01.2027 по 31.03.2027	Услуги по техническому обеспечению защищенной сети	месяц	3
		Услуги по техническому обеспечению подсистемы защиты от несанкционированного доступа и средств электронной подписи	месяц	3
		Услуги по регламентному обслуживанию защищенной сети	месяц	3
		Услуги по актуализации документации, регламентирующей обработку персональных данных	усл. ед.	1
		Услуги по аудиту документации, регламентирующей обработку персональных данных	усл. ед.	1
	с 01.04.2027 по 30.06.2027	Услуги по техническому обеспечению защищенной сети	месяц	3
		Услуги по техническому обеспечению подсистемы защиты от несанкционированного доступа и средств электронной подписи	месяц	3
		Услуги по регламентному обслуживанию защищенной сети	месяц	3
		Услуги по актуализации документации, регламентирующей обработку персональных данных	усл. ед.	1
		Услуги по аудиту документации, регламентирующей обработку персональных данных	усл. ед.	1
	с 01.07.2027 по	Услуги по техническому	месяц	3

	30.09.2027	обеспечению защищенной сети		
		Услуги по техническому обеспечению подсистемы защиты от несанкционированного доступа и средств электронной подписи	месяц	3
		Услуги по регламентному обслуживанию защищенной сети	месяц	3
		Услуги по актуализации документации, регламентирующей обработку персональных данных	усл. ед.	1
		Услуги по аудиту документации, регламентирующей обработку персональных данных	усл. ед.	1
	с 01.10.2027 по 30.11.2027	Услуги по предоставлению сертификата активации сервиса совместной технической поддержки уровень – Расширенный, для защищенной сети ViPNet № 541	усл. ед.	1
		Услуги по предоставлению сертификата активации сервиса совместной технической поддержки уровень – Расширенный, для защищенной сети ViPNet № 986	усл. ед.	1
	с 01.10.2027 по 31.12.2027	Услуги по техническому обеспечению защищенной сети	месяц	3
		Услуги по техническому обеспечению подсистемы защиты от несанкционированного доступа и средств электронной подписи	месяц	3
		Услуги по регламентному обслуживанию защищенной сети	месяц	3
		Услуги по актуализации документации, регламентирующей обработку персональных данных	усл. ед.	1
		Услуги по аудиту документации, регламентирующей обработку персональных данных	усл. ед.	1
	с 01.01.2027 по 31.12.2027	Разработка комплекта организационно-распорядительной документации, регламентирующей защиту	усл. ед.	1

		информации в соответствии с требованиями Приказа ФСТЭК №117		
--	--	---	--	--