Приложение № 1 к Контракту
от «31» августа 2023 года
№ 071/23/89

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на оказание государственным и муниципальным образовательным организациям, реализующим образовательные программы общего образования и среднего профессионального образования (далее – образовательные организации), избирательным комиссиям субъектов Российской Федерации и территориальным избирательным комиссиям (далее – избирательные комиссии), расположенным на территориях субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя) (с учетом потребностей указанных пользователей), услуг по предоставлению с использованием единой сети передачи данных доступа к государственным, муниципальным, иным информационным системам и к информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет); по передаче данных при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет; по защите данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет; по обеспечению ограничения доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, причиняющей вред здоровью и (или) развитию детей, содержащейся в сети Интернет, для образовательных организаций; по мониторингу и обеспечению безопасности связи при предоставлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет; по организации подключения к единой сети передачи данных образовательных организаций и избирательных комиссий, по передаче данных при осуществлении доступа к этой сети

СОДЕРЖАНИЕ

1. Термины, определения и сокращения.

1.1. В Контракте, включая настоящее техническое задание (далее – ТЗ) используются следующие термины, определения и сокращения:

Термин	*Определение*
AS	Autonomous System, автономная система, IP сеть, находящаяся под единым административным управлением и имеющая единую политику маршрутизации, характеризуется номером, который выдается официальным интернет-регистратором (например, RIPE)
CE	Customer Edge Router, граничное устройство в локальной вычислительной сети СЗО, Объекта ЦИК, используемое для маршрутизации трафика из сети СЗО, Объекта ЦИК в сеть Исполнителя и обратно
DDoS-атака	Distributed Denial of Service, распределенная атака на отказ в обслуживании, разновидности атак на компьютерные системы и сети связи, связанные с большим количеством запросов (в виде IP-пакетов), посылаемых с большого количества IP-адресов сети Интернет и направленных на IP-адреса оборудования СЗО, Объекта ЦИК.
ICMP	Internet Control Message Protocol - протокол межсетевых управляющих сообщений
IETF RFC	Документ (Reques For Comments) рабочей группы по инженерным проблемам сети Интернет (Internet Engineering Task Force)
IP сеть Исполнителя	Сетевая инфраструктура Исполнителя и привлекаемых Исполнителем субподрядчиков (соисполнителей), состоящая из расположенных на узлах Исполнителя и привлекаемых Исполнителем субподрядчиков (соисполнителей), устройств, обеспечивающих взаимодействие по сетевому протоколу IP (спецификация IETF RFC 791), маршрутизацию, коммутацию и обработку трафика, соединяющих их магистральных каналов и иных средств связи
IP-пакет	Пакет 3 уровня (OSI), маршрутизируемого по протоколу IP
MPLS	Multi Protocol Label Switching, технология коммутации пакетов с использованием меток
MPLS сеть Исполнителя	Построенная по технологии MPLS сетевая инфраструктура Исполнителя и привлекаемых Исполнителем субподрядчиков (соисполнителей), включающая опорные маршрутизаторы (P), граничные маршрутизаторы (PE),

Термин	*Определение*
	соединяющие их магистральные каналы и иные средства связи
RIPE NCC	Региональный Европейский Регистратор Интернет адресов
Service Desk	Система регистрации обращений, управления и решения инцидентов/ запросов
SLA (англ. Service Level Agreement)	Соглашение об уровне предоставления услуг – формальный договор между Заказчиком и Исполнителем, содержащий права и обязанности сторон, а также согласованный уровень качества предоставления данной услуг
SNMP	Simple Network Management Protocol, протокол сетевого управления
WEB	Всемирная паутина – (англ. World Wide Web) — распределенная система, предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключенных к сети Интернет
Аварийная ситуация	Недоступность услуг Исполнителя, вызванная неисправностью оборудования, сети, инженерных систем и инфраструктуры Исполнителя или привлекаемых Исполнителем субподрядчиков (соисполнителей), включая несанкционированные неблагоприятные воздействия на указанные объекты
АРМ	Автоматизированное рабочее место
Вариация задержки	Jitter, отклонение от среднего значения времени прохождения IP-пакетов по участку измерения от передающей стороны к приемной стороне
Владелец ИС	РОИВ, ФОИВ, СЗО, владеющий региональной и/или федеральной информационной системой
Внешние IPv4 адреса	Внешние (публичные) IP адреса из зарегистрированного в базе данных RIPE NCC IP адресов 4 версии протокола IP
Временный белый список	Перечень ресурсов в сети Интернет, доступ к которым разрешен по запросам Потребителей и уполномоченных государственных органов в течение определенного промежутка времени
Время реакции	Срок, в течение которого Исполнитель обязуется приступить к работе над проблемой, обозначенной в запросе Получателя об инциденте, определенный SLA
ВОЛС	Волоконно-оптическая линия связи
ВЧС	Виртуальная частная сеть СЗО, Объекта ЦИК, построенная на базе MPLS сети Исполнителя и привлекаемых Исполнителем субподрядчиков (соисполнителей), путем организации виртуальных каналов между портами на узлах доступа сети Исполнителя, к которым подключен СЗО, Объект ЦИК, и обеспечивающая передачу различных типов трафика с гарантией параметров качества.
Государственный заказчик - Заказчик	Министерство цифрового развития и массовых коммуникаций Российской Федерации.
Доступность услуги	Отношение времени нахождения оказываемых услуг в рабочем состоянии к общей продолжительности интервала наблюдения, выраженное в процентах (доступность за отчетный период).
ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА) — информационная система Российской Федерации, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных информационных системах и иных информационных системах
ЕСПД	Виртуальная частная сеть (сети) Исполнителя, обеспечивающая доступ социально-значимых объектов к информационным системам и к сети

Термин	*Определение*
	Интернет, а также передачу данных при предоставлении доступа к информационным системам и к сети Интернет; обеспечивающая доступ Центральной избирательной комиссии, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий к информационным системам и к сети Интернет.
Задержка	One-way delay, время прохождения IP-пакетов по участку измерения в одну сторону (от передающей стороны к приемной). Определяется согласованными с Потребителем методами и при необходимости рассчитывается как половина временного интервала между моментом отправления сообщения «запрос эхо» передающей стороной и моментом получения сообщения «отклик эхо» от приемной стороны (PING протокола ICMP).
Заявка	Надлежащим образом оформленное по форме (Приложение №1) обращение Заказчика к Исполнителю с указанием дат и перечня объектов, для которых необходимо оказывать Услуги связи.
Иная технология	Технологии линий связи, отличные от технологий волоконно-оптической связи и спутниковой технологии. Используется в случае невозможности использования ВОЛС с обеспечением наибольшей скорости подключения.
ИС	Государственная, региональная, муниципальная и иная информационная система, класс криптозащиты которой соответствует классу защиты ЕСПД, к которой предоставляется доступ с использованием единой сети передачи данных Исполнителя.
Исполнитель	Оператор связи, с которым заключен Государственный контракт на оказание Услуг связи
Канал L2	Канал связи от СЗО, Объекта ЦИК до Точки присоединения ЕСПД
Класс трафика	Набор требований к эксплуатационным параметрам, соблюдаемым Исполнителем при передаче по сети применительно ко всем IP-пакетам, принадлежащим данному типу
Контракт	Государственный контракт на оказание государственным и муниципальным образовательным организациям, реализующим образовательные программы общего образования и среднего профессионального образования (далее – образовательные организации), избирательным комиссиям субъектов Российской Федерации и территориальным избирательным комиссиям (далее – избирательные комиссии), расположенным на территориях субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя) (с учетом потребностей указанных пользователей), услуг по предоставлению с использованием единой сети передачи данных доступа к государственным, муниципальным, иным информационным системам и к информационно-телекоммуникационной сети «Интернет» (далее – сеть Интернет); по передаче данных при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет; по защите данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет; по обеспечению ограничения доступа к информации , распространение которой в Российской Федерации запрещено, и к информации, причиняющей вред здоровью и (или) развитию детей, содержащейся в сети Интернет, для образовательных организаций; по мониторингу и обеспечению безопасности связи при предоставлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет; по организации подключения к единой сети передачи данных образовательных организаций и избирательных комиссий, по передаче данных при осуществлении доступа к этой сети
Компонент	Составляющая Услуг связи, определяющая одну из основных потребностей, удовлетворяемых с помощью оказываемых Услуг

Термин	*Определение*
КСА	Комплекс средств автоматизации
Коэффициент готовности сети	Параметр, выражающий вероятность того, что точка присоединения ЕСПД окажется в работоспособном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых предоставление сервисов не предусматривается
Коэффициент потери пакетов	Максимальная потеря пакетов – отношение общего количества недоставленных пакетов к общему количеству переданных пакетов, выражаемая в процентах потерянных пакетов
КФ	Контентная фильтрация
Личный кабинет	Персональная страница для Потребителя, организованная на ресурсе сайта Исполнителя, доступ на которую осуществляется через ЕСИА
МСЭ	Межсетевое экранирование
Нежелательный Интернет-трафик	Интернет-трафик, поступающий на оборудование СЗО, Объекта ЦИК, наличие которого может быть обусловлено наличием DDoS-атаки, либо другими нежелательными для Потребителя факторами
Образовательная организация	Государственная или муниципальная образовательная организация, реализующая программы общего образования и (или) среднего профессионального образования
Объект	Совокупность технических средств, средств вычислительной техники и программного обеспечения, расположенных по одному адресу
Объекты ЦИК	Центральная избирательная комиссия Российской Федерации или избирательные комиссии субъекта Российской Федерации или территориальные избирательные комиссии.
Отчетный период	Период времени оказания Услуг связи, по окончании которого производится сдача-приемка Услуг связи и их оплата
Оператор СКЗИ	Оператор связи, оказывающий услугу по компоненту «Защита данных» на участке от СЗО до Точки присоединения ЕСПД на момент исполнения Контракта
Пакет	Форматированный блок информации, передаваемый по сети связи, функционирующей посредством технологии коммутации пакетов
ПД	Передача данных
Потребитель	Пользователь Услуг связи или ее Компонентов на СЗО, Объекте ЦИК.
Порт	Логический интерфейс ВЧС Потребителя на узлах доступа сети Исполнителя
Постоянный белый список	Перечень ресурсов в сети Интернет, доступ к которым разрешен по запросам Потребителей и уполномоченных государственных органов на постоянной основе
Представитель СЗО	Руководитель социально значимого объекта, в интересах которого Исполнитель оказывает услуги в соответствии с Государственным контрактом, или лицо, уполномоченное в установленном порядке на взаимодействие с Исполнителем при оказании Услуг.
Представитель объекта ЦИК	Руководитель объекта ЦИК, в интересах которого Исполнитель оказывает услуги в соответствии с Государственным контрактом, или лицо, уполномоченное в установленном порядке на взаимодействие с Исполнителем при оказании Услуг связи.
Процент потерянных пакетов	IP packet loss ratio, отношение разности количества отправленных в конечную точку участка измерения IP-пакетов и количества принятых в этой точке IP-пакетов, к количеству отправленных в конечную точку IP-пакетов
РОИВ	Региональный орган исполнительной власти
Сеть Интернет	Информационно-телекоммуникационная сеть «Интернет»

Термин	*Определение*
СЗО - Социально значимый объект	Образовательная организация.
СКЗИ	Средства криптографической защиты информации
Служба технической поддержки Заказчика	Организуемая Заказчиком служба технической поддержки Потребителя, которая осуществляет контроль оказания Услуг связи по обращениям Потребителей или Заказчика в соответствии с Регламентом технической поддержки при оказании Услуг
СМЭВ	Система межведомственного электронного взаимодействия
СОРМ	Системы технических средств для обеспечения функций оперативно-розыскных мероприятий
Спутниковая технология	Один из видов космической радиосвязи, основанный на использовании в качестве ретрансляторов искусственных спутников Земли - специализированных спутников связи
	Сеть связи общего пользования
ССОП Стоп-фактор	Признак состояния Объекта, при котором Исполнитель не может оказать Услуги связи в соответствии с условиями Контракта
Субъект РФ	Территориальная единица верхнего уровня в Российской Федерации.
ТЗ	Настоящее техническое задание
Точки присоединения ЕСПД	Средства связи, входящие в состав сети электросвязи Исполнителя, с помощью которых осуществляется подключение и доступ СЗО, Объектов ЦИК к ЕСПД
Трафик	Совокупность IP-пакетов, переданных по сети передачи данных
Услуги связи	Оказание Исполнителем Услуг связи для СЗО и Объектов ЦИК, расположенным на территориях субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя) по: передаче данных при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (Компонент Услуги связи «Передача данных») в составе услуг: по защите данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (Компонент «Защита данных»); по обеспечению ограничения доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, причиняющей вред здоровью и (или) развитию детей, содержащейся в сети Интернет для образовательных организаций (Компонент «Ограничение доступа к информации»); по мониторингу и обеспечению безопасности связи при предоставлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (Компонент «Мониторинг и обеспечение безопасности связи»); по предоставлению с использованием ЕСПД доступа к государственным, муниципальным, иным информационным системам и к информационно - телекоммуникационной сети «Интернет» (Компонент «Предоставление доступа»). Оказание Исполнителем Услуг связи для СЗО и Объектов ЦИК, расположенных на территориях субъектов Российской Федерации

Термин	*Определение*
	(за исключением Республики Крым и г. Севастополя) по: организации подключения к ЕСПД (Компонент «Организация канала L2»); передаче данных при осуществлении доступа к ЕСПД (Компонент «Передача данных L2»)
ФОИВ	Федеральный орган исполнительной власти
ФСБ	Федеральная служба безопасности Российской Федерации
ЦИК России	Центральная избирательная комиссия Российской Федерации
ЦОД	Центр обработки и хранения данных
Черный список	Перечень ресурсов в сети Интернет, доступ к которым заблокирован на уровне КФ по запросам Потребителей и уполномоченных государственных органов

2. Общие сведения.

2.1. Основания оказания Услуг связи:

2.1.1. Постановление Правительства РФ от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации «Информационное общество»;

2.1.2. Подпункт «б» пункта 2 Перечня поручений по реализации Послания Президента Российской Федерации Федеральному Собранию Российской Федерации от 26 февраля 2019 г. № Пр-294 по вопросу подключения общеобразовательных организаций к сети Интернет.

2.1.3. Подпункт «в» пункта 1 Перечня поручений по итогам совещания Президента Российской Федерации с членами Правительства Российской Федерации от 23 апреля 2021 г. № Пр-676 о принятии дополнительных мер, направленных на недопущение случаев неоправданного завышения стоимости услуг по подключению общеобразовательных организаций к высокоскоростному Интернету;

2.1.4. Распоряжения Правительства Российской Федерации от 28 июля 2017 г. № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»;

2.1.5. Федеральный проект «Информационная инфраструктура» национального программа «Цифровая экономика Российской Федерации»,

утвержденный протоколом заседания президиума правительственной комиссии по цифровому развитию, использованию цифровых технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 06 мая 2019 г. № 8.

2.1.6. Положение о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденное постановлением Правительства Российской Федерации от 02 июня 2008 г. № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации».

2.1.7. Оказание Услуг связи должно соответствовать:

— Федеральному закону от 07 июля 2003 г. № 126-ФЗ «О связи»;

— Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

— Федеральному закону от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

— Федеральному закону от 06 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;

— Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

— Федеральному закону от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;

— Указу Президента РФ от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;

— Постановлению Правительства РФ от 31 декабря 2021 № 2606 "Об утверждении Правил оказания услуг связи по передаче данных";

— Постановлению Правительства РФ от 31 декабря 2021 № 2607 "Об утверждении Правил оказания телематических услуг связи";

— Постановлению Правительства Российской Федерации от 30 декабря 2020 г. № 2385 «О лицензировании деятельности в области оказания услуг связи

и признании утратившими силу некоторых актов Правительства Российской Федерации»;

— Постановлению Правительства РФ от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность»;

— Приказу Минцифры России от 18 февраля 2022 N 132 "Об утверждении Требований к порядку ввода сетей связи в эксплуатацию";

— Приказу ФСБ России от 10 июля 2014 г. № 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»;

— Приказу Министерства связи и массовых коммуникаций РФ от 16 апреля 2014 г. № 83 «Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий»;

— Приказу Министерства связи и массовых коммуникаций РФ от 16 января 2008 г. № 6 «Об утверждении требований к сетям электросвязи для проведения оперативно-розыскных мероприятий Часть 1. Общие требования»;

— Требованиям к подключению и доступу, включая требования к передаче данных, государственных и муниципальных образовательных организаций,

реализующих программы общего и среднего профессионального образования, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий к единой сети передачи данных, утвержденным приказом Минцифры России № 417, Минпросвещения России от 30 апреля 2021 г. № 221 «Об утверждении требований к подключению и доступу, включая требования к передаче данных, государственных и муниципальных образовательных организаций, реализующих программы общего и среднего профессионального образования, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий к единой сети передачи данных»;

— Техническим нормам в соответствии с «РД 45.129-2000. Руководящий документ отрасли. Телематические службы», утвержденным приказом Минсвязи России от 23 июля 2001 г. № 175 «Об утверждении Руководящего документа отрасли "Телематические службы»;

— Национальному стандарту РФ ГОСТ Р 59853-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения»;

— Межгосударственному стандарту ГОСТ 34.201-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

— ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

— Межгосударственному стандарту ГОСТ 34.602-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

— Национальному стандарту РФ ГОСТ Р 59792-2021 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды испытаний автоматизированных систем»;

— ГОСТ 27049-86 Защита оборудования проводной связи и обслуживающего персонала от атмосферных разрядов;

— ГОСТ 28439-90 «Аппаратура волоконно-оптических систем передачи по линиям электропередач цифровая. Общие технические требования»;

— ГОСТ 5238-81 «Установки проводной связи. Схемы защиты от опасных напряжений и токов, возникающих на линиях. Технические требования»;

— ГОСТ Р 50799-95 «Совместимость технических средств электромагнитная. Устойчивость технических средств радиосвязи к электростатическим разрядам, импульсным помехам и динамическим изменениям напряжения сети электропитания. Требования и методы испытаний»;

— ГОСТ Р 53724-2009 «Качество услуг связи. Общие положения»;

— ГОСТ Р 53731-2009 «Качество услуг связи. Термины и определения»;

— ГОСТ Р 53728-2009 «Качество услуги «Передача данных». Показатели качества»;

— ГОСТ Р 53729-2009 «Качество услуги «Предоставление виртуальной частной сети (VPN)». Показатели качества»;

— Межгосударственному стандарту ГОСТ 34.12-2018 «Информационная технология. Криптографическая защита информации. Блочные шифры»;

— Межгосударственному стандарту ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»;

— ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры».

2.2. Срок оказания Услуг связи: с 1 сентября по 31 декабря 2023 года включительно.

Услуги связи оказываются непрерывно, круглосуточно и ежедневно в соответствии с условиями ТЗ.

2.3. Оказание Услуг связи для СЗО и Объектов ЦИК осуществляется

в соответствии с Заявками Заказчика и Ценами единиц Услуги связи (Приложение № 2 к государственному контракту).

2.3.1 Услуги связи, согласно направляемым Заказчиком Заявкам, включают в себя:

2.3.1.1 Оказание Исполнителем услуг связи для СЗО и Объектов ЦИК, расположенных на территориях субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя) по:

1) передаче данных при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (**Компонент «Передача данных»**) в составе услуг:

- по защите данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (**Компонент «Защита данных»**);
- по обеспечению ограничения доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, причиняющей вред здоровью и (или) развитию детей, содержащейся в сети Интернет для образовательных организаций (**Компонент «Ограничение доступа к информации»**);
- по мониторингу и обеспечению безопасности связи при предоставлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (**Компонент «Мониторинг и обеспечение безопасности связи»**);

2) по предоставлению с использованием ЕСПД доступа к государственным, муниципальным, иным информационным системам и к информационно - телекоммуникационной сети Интернет (**Компонент**

«Предоставление доступа»).

3) организации подключения к ЕСПД (**Компонент «Организация канала L2»**);

4) передаче данных при осуществлении доступа к ЕСПД (**Компонент «Передача данных L2»**).

2.3.2 С целью своевременной поставки товаров (выполнения работ, оказания услуг) Исполнитель вправе совершать юридически значимые действия, не противоречащие законодательству Российской Федерации, в том числе привлекать к исполнению своих обязательств по настоящему Контракту исполнителей (соисполнителей), оставаясь ответственным перед Заказчиком за их действия, в том числе по договорам (контрактам, соглашениям), заключенным с поставщиками, подрядчиками, исполнителями на поставку товаров, выполнение работ, оказание услуг, необходимых для поставки товаров (выполнения работ, оказания услуг) по Контракту, до заключения настоящего Контракта, а также оплачивать поставленный товар, выполненные работы, оказанные услуги.

2.4. Место оказания Услуг связи:

Субъекты Российской Федерации (за исключением Республики Крым и г. Севастополя), по месту нахождения точек присоединения к единой сети передачи данных, по месту нахождения государственных и муниципальных образовательных организаций, реализующих образовательные программы общего образования и среднего профессионального образования, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий,

по месту нахождения Исполнителя.

2.5. Исходные данные.

При оказании Услуг связи Исполнитель должен руководствоваться следующими исходными данными:

– настоящим ТЗ;

– перечнем Точек присоединения ЕСПД;

– Заявками на оказание Услуг связи.

2.6. Результаты оказания Услуг связи.

2.6.1 Исполнителем оказаны услуги связи для СЗО и Объектов ЦИК, расположенных на территориях субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя) по:

1) передаче данных при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (**Компонент «Передача данных»**) в составе услуг:

— по защите данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (**Компонент «Защита данных»**);

— по обеспечению ограничения доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, причиняющей вред здоровью и (или) развитию детей, содержащейся в сети Интернет для образовательных организаций (**Компонент «Ограничение доступа к информации»**);

— по мониторингу и обеспечению безопасности связи при предоставлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (**Компонент «Мониторинг и обеспечение безопасности связи»**);

2) предоставлению с использованием ЕСПД доступа к государственным, муниципальным, иным информационным системам и к информационно - телекоммуникационной сети «Интернет» (**Компонент**

«Предоставление доступа»).

3) организации подключения к ЕСПД (**Компонент «Организация канала L2»**);

4) передаче данных при осуществлении доступа к ЕСПД (**Компонент «Передача данных L2»**).

2.7. Требования к Исполнителю.

Исполнитель должен соответствовать требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим оказание услуг связи, позволяющим на протяжении действия Государственного контракта оказывать следующие услуги:

– услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации;

– телематические услуги связи;

– услуги по защите информации.

2.7.1. Исполнитель для соответствующих видов работ должны иметь лицензии, действующие на территории Российской Федерации на следующие виды деятельности:

– лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации в части следующих работ и услуг, утвержденных постановлением Правительства Российской Федерации
от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»:

– контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;

– установка, монтаж, испытания, ремонт средств защиты информации (программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки

информации, программных (программно-технических) средств контроля защищенности информации);

– лицензии Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций:

– на оказание услуг связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации;

– на оказание телематических услуг связи;

– лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания 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)» в части следующих работ и услуг:

– монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств (п.12 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств);

– монтаж, установка (инсталляция), наладка защищенных с использованием шифровальных (криптографических) средств информационных систем (п.13 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств);

– работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства (за исключением случая, если указанные работы проводятся для обеспечения собственных нужд) (п.20 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств);

– передача шифровальных (криптографических) средств (п.21 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств);

– передача защищенных с использованием шифровальных (криптографических) средств информационных систем (п.22 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств);

– передача средств изготовления ключевых документов (п.24 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств);

Для подтверждения соответствия указанным требованиям Исполнитель должен предоставить выписку из реестра лицензий о наличии у Исполнителя соответствующих лицензий или копии соответствующих лицензий в установленном законодательством Российской Федерации порядке.

2.8. Время оказания Услуг связи.

Услуги связи должны оказываться 24 (двадцать четыре) часа в сутки 7 (семь) дней в неделю.

2.9. Услуги связи должны предоставляться посредством сети передачи данных Исполнителя.

2.10. ЕСПД должна быть организована по принципу полносвязной, защищенной сети связи, изолированной от сети Интернет и сетей других пользователей на логическом уровне, и поддерживающей обмен данными (трафиком) через узлы ЕСПД на уровне субъектов РФ (за исключением

Республики Крым и г. Севастополя).

2.11. Для оказания Услуг связи СЗО и Объектам ЦИК в составе ЕСПД организуются каналы передачи данных и Точки присоединения ЕСПД.

2.12. Для оказания Услуг связи Исполнитель должен использовать телекоммуникационное оборудование, страной происхождения которого является Российская Федерация, и сведения, о котором содержатся в перечне телекоммуникационного оборудования российского происхождения, который формируется приказами Министерства промышленности и торговли Российской Федерации, или в Едином реестре российской радиоэлектронной продукции, сформированном Министерством промышленности и торговли Российской Федерации.

2.13. При отсутствии телекоммуникационного оборудования, которому присвоен статус телекоммуникационного оборудования российского происхождения, обладающего характеристиками, необходимыми для оказания Услуги связи, а также в случае, если производитель такого телекоммуникационного оборудования не в состоянии обеспечить его наличие в достаточном количестве для начала оказания Услуг связи или в течении срока их оказания, Исполнитель вправе приобретать и использовать для оказания Услуг связи иное телекоммуникационное оборудование только после согласования его использования с Заказчиком.

2.14. Заказчик согласовывает использование иного телекоммуникационного оборудования, предусмотренного п. 2.13 ТЗ, в следующих случаях:

— отсутствие телекоммуникационного оборудования, которому присвоен статус телекоммуникационного оборудования российского происхождения, обладающего характеристиками, необходимыми для оказания Услуги связи;

— представлением Исполнителем Заказчику заверенных копий запроса, направленного производителю телекоммуникационного оборудования, которому присвоен статус телекоммуникационного оборудования российского происхождения, о возможности обеспечения его наличия в срок и в количестве,

которые необходимы для оказания Услуг связи, а также предоставления ответа производителя, подтверждающего невозможность такого обеспечения.

2.15. Исполнитель обеспечивает присоединение канала связи между СЗО, Объектами ЦИК и ЕСПД в Точках присоединения ЕСПД.

2.16. Требования к оборудованию Точек присоединения ЕСПД для **СЗО**:

1) Точкой присоединения ЕСПД является комплект оборудования Исполнителя, в состав которого входит оборудование, с сетевыми интерфейсами для подключения Каналов L2 между СЗО и ЕСПД. Количество интерфейсов для подключения оборудования канала связи между СЗО и ЕСПД должно обеспечить оказание Услуг связи;

2) Состав оборудования Точек присоединения ЕСПД должен быть определен Исполнителем с учетом требований ТЗ;

3) Исполнитель обеспечивает установку необходимого оборудования в Точке присоединения ЕСПД своими силами и за свой счет;

4) Адреса размещения Точек присоединения ЕСПД предоставляются на утверждение по форме в соответствии с Приложением № 4 к Техническому заданию Исполнителем Заказчику в срок, указанный в п. 7.1 ТЗ.

2.17. Требования к оборудованию Точек присоединения ЕСПД для Объектов **ЦИК:**

1) Исполнитель обеспечивает установку необходимого оборудования в Точке присоединения ЕСПД своими силами и за свой счет;

2) Точкой присоединения ЕСПД является комплект оборудования Исполнителя или привлеченного Исполнителем соисполнителя, в состав которого входит оборудование с сетевыми интерфейсами для подключения оборудования Объектов ЦИК. Количество интерфейсов для подключения оборудования Объектов ЦИК должно обеспечить оказание Услуг связи;

3) Оборудование Точки присоединения ЕСПД должно обеспечивать достаточное количество интерфейсов для подключения к ЕСПД оборудования Объекта ЦИК и располагаться на Объекте ЦИК в месте, согласованном Представителем объекта ЦИК.

2.18. Доступ к сети Интернет из ЕСПД должен осуществляться на уровне административных центров субъектов РФ, в которых расположены СЗО и Объекты ЦИК. Осуществление доступа к сети Интернет вне административных центров субъектов РФ согласовывается с Заказчиком.

2.19. Количество Точек присоединения ЕСПД для Объектов ЦИК должно соответствовать количеству Объектов ЦИК, указанных в Заявках, и находиться по их фактическим адресам. По согласованию с Представителями объектов ЦИК допускается организация одной Точки присоединения ЕСПД для нескольких Объектов ЦИК при условии их нахождения в одном здании (помещении).

2.20. Для Объектов ЦИК, которые будут добавляться дополнительно, линии связи от средств связи, входящих в состав сети электросвязи Исполнителя, до Точек присоединения ЕСПД на Объектах ЦИК должны использовать ВОЛС. Использование спутниковых каналов связи при организации Точек присоединения ЕСПД в труднодоступных населенных пунктах допускается только при обосновании данной необходимости Исполнителем и по согласованию с Заказчиком.

2.21. В каждом субъекте Российской Федерации должно быть не менее одной Точки присоединения ЕСПД с возможностью оказания Услуг связи (за исключением Республики Крым и г. Севастополя).

2.22. Точки присоединения ЕСПД должны обеспечивать достаточное количество интерфейсов для подключения к ЕСПД Каналов L2. Типы абонентских физических интерфейсов, которые могут использоваться при присоединении Каналов L2 включают в том числе следующие:

- 802.3ab 1000BASE-T (10/100/1000 Ethernet over copper);
- 1000 Base-LX (одномодовое оптическое волокно);
- 1000 Base-LH (одномодовое оптическое волокно);
- 10G Base-LR (одномодовое оптическое волокно);
- 100GBASE-LR4 (одномодовое оптическое волокно).

2.23. Каналы связи ЕСПД между Точками присоединения ЕСПД для СЗО, задействованные в оказании Услуг связи, должны использовать ВОЛС.

2.24. Линии связи, используемые для предоставления Услуг связи, должны находиться в пределах границ Российской Федерации, за исключением тех, которые используются для обеспечения функционирования Точек присоединения ЕСПД и Объектов ЦИК Калининградской области.

2.25. Не допускается организация каналов связи, использующихся для оказания Услуг связи СЗО и Объектам ЦИК, через сеть Интернет.

2.26. **Для СЗО** в составе ЕСПД организуются следующие отдельные виртуальные сети включая, но не ограничиваясь следующими:

– передачи данных образовательных организаций при доступе к информационным системам и в сеть Интернет.

2.27. **Для Объектов ЦИК** в составе ЕСПД организуются следующие отдельные виртуальные сети включая, но не ограничиваясь следующими:

- передачи данных ЦИК, ИК СРФ, ТИК для ГАС «Выборы»;

- передачи данных ИК СРФ, ТИК при предоставлении доступа в сеть Интернет.

2.28. Трафик, предназначенный для отдельных виртуальных сетей, не должен перемешиваться.

2.29. Точки присоединения ЕСПД **для СЗО** должны соответствовать следующим параметрам:

– количество Точек присоединения ЕСПД не менее 83;

– в административном центре каждого субъекта Российской Федерации (за исключением Донецкой Народной Республики, Республики Крым, Луганской Народной Республики, Запорожской области, Херсонской области и г. Севастополя) должно быть не менее одной Точки присоединения ЕСПД;

– полоса пропускания на одну Точку присоединения ЕСПД должна обеспечивать гарантированное выполнение параметров качества передачи данных, соответствующих требованиям подключения для каждого СЗО, подключенного
к ЕСПД;

– процент потери IP-пакетов, задержка передачи IP-пакетов и вариация

времени задержки IP-пакетов должны соответствовать требованиям ТЗ;

– другим требованиям, изложенным в ТЗ.

2.30. Точки присоединения ЕСПД **для Объектов ЦИК** должны соответствовать следующим параметрам:

– количество Точек присоединения ЕСПД для Объектов ЦИК определяется в соответствии с количеством Объектов ЦИК, указанных в Заявках, при этом допускается организация одной Точки присоединения ЕСПД для нескольких Объектов ЦИК, расположенных в одном здании, помещении;

– увеличение/уменьшение Точек присоединения ЕСПД происходит при формировании новых Объектов ЦИК России или их сокращении после получения Заявки;

– полоса пропускания на одну Точку присоединения ЕСПД должна обеспечивать гарантированное выполнение параметров качества передачи данных, соответствующих требованиям подключения для каждого Объекта ЦИК;

– коэффициент готовности сети Кг общий не менее 0,99 за расчетный период (календарный месяц), расчет которого осуществляется в Системном проекте;

– процент потери IP-пакетов, задержка передачи IP-пакетов и вариация времени задержки IP-пакетов должны соответствовать требованиям ТЗ;

– другим требованиям, изложенным в ТЗ.

2.31. Исполнитель обязан оказывать Услуги связи для СЗО и Объектов ЦИК без ограничения объема передачи (безлимитно).

2.32. Исполнитель самостоятельно присоединяет к ЕСПД ИС, на основании запросов от Заказчика.

2.33. Исполнитель обязан произвести присоединение ИС к ЕСПД в течение 30 (тридцати) дней с даты получения запроса от Заказчика или запросов от Владельцев ИС или ЦИК, при условии готовности Владельцев ИС или ЦИК согласовать и реализовать техническое решение по подключению в указанный срок, а также при назначении со стороны ИС или ЦИК лиц, ответственных за диагностику и устранение проблем, возникающих между ЕСПД и ИС

(контакты ответственных передаются Исполнителю письмом). В случае неготовности Владельцев ИС или ЦИК исполнять указанные требования – Исполнитель проводит эскалацию Заказчику для согласования новых сроков подключения.

2.34. Исполнитель за свой счет проводит все необходимые работы по присоединению ИС к ЕСПД в том числе и доработку ИС в части обеспечения оборудованием для обеспечения криптографической защиты передаваемых данных между пользователями и ИС.

2.35. Исполнитель присоединяет к ЕСПД региональные и муниципальные сети передачи данных субъектов Российской Федерации, по обращению субъектов Российской Федерации. Присоединение региональных и муниципальных сетей передачи данных субъектов Российской Федерации производится после согласования с Заказчиком.

2.36. Исполнитель обеспечивает маршрутизацию трафика и доступность ИС для СЗО, подключенных к региональным сетям субъектов Российской Федерации, в своей зоне ответственности.

2.37. Исполнитель, для обеспечения Услуг связи, при подключении объекта к ЕСПД единоразово оказывает содействие СЗО по настройке всех АРМ, имеющих техническую возможность подключения к ЕСПД. Последующее содействие

по подключению новых АРМ после первичной организации услуги в СЗО оказываются путем предоставления необходимых инструкций и консультационной поддержки.

2.38. При оказании Услуг связи, в том числе в части обеспечения функционирования ГАС «Выборы», Объектам ЦИК Исполнитель обязан выполнять Технические требования «На оказание Услуг связи территориальным избирательным комиссиям и избирательным комиссиям субъектов Российской Федерации для обеспечения функционирования ГАС «Выборы» (Приложение № 7), если иное не установлено действующим законодательством.

2.39. Организация Канала L2 от СЗО до Точки присоединения ЕСПД

проводится в границах одного субъекта Российской Федерации. При отсутствии экономической и технической целесообразности подключения Канала L2 к ЕСПД в границах одного субъекта Российской Федерации, подключение СЗО может быть выполнено к Точке присоединения ЕСПД соседнего субъекта Российской Федерации, при этом данное решение согласовывается Исполнителем с Заказчиком.

2.40. Подключение Канала L2 от СЗО, Объекта ЦИК к Точке присоединения ЕСПД проводится силами Исполнителя.

2.41. Требования к взаимодействию между Исполнителем и Представителем **СЗО** при предоставлении Услуг связи:

2.41.1. Исполнитель предоставляет и устанавливает для всех СЗО, присоединяемых (подключаемых) к ЕСПД, криптомаршрутизаторы. Установка криптомаршрутизаторов осуществляется в телекоммуникационные шкафы. В случае отсутствия на объекте СЗО телекоммуникационного шкафа Исполнитель осуществляет его установку.

2.41.2. Установка криптомаршрутизатора Исполнителем не требуется в случае, если на участке сети от СЗО до Точки присоединения к ЕСПД защита данных обеспечивается сторонним оператором СКЗИ в соответствии с требованиями ТЗ.

2.41.3. Исполнитель в течение всего срока оказания Услуг связи обеспечивает за свой счет настройку, включая изменение настроек в соответствии с запросами Заказчика, техническое обслуживание и ремонт оборудования, в том числе криптомаршрутизаторов, установленных Исполнителем в СЗО. При этом сроки

и порядок выполнения регламентных и ремонтных работ устанавливаются Регламентом технической поддержки при оказании Услуги связи, утвержденным Заказчиком.

2.42. Требования к взаимодействию между Исполнителем и Представителем **ЦИК** при предоставлении Услуг связи:

2.42.1. Исполнитель предоставляет и устанавливает для всех объектов

ЦИК, присоединяемых (подключаемых) к ЕСПД, криптомаршрутизаторы или маршрутизаторы на основании Заявок. Установка оборудования осуществляется в телекоммуникационные шкафы. В случае отсутствия на объекте ЦИК телекоммуникационного шкафа Исполнитель осуществляет его установку.

2.42.2. Компонент «Предоставление доступа» для избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий, расположенных на территориях субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя) в соответствии с запросами ЦИК РФ без установки СКЗИ (для новых Объектов ЦИК, ранее не подключенных к ЕСПД) – включает в себя установку маршрутизатора на объекте ЦИК.

2.42.3. Исполнитель в течение всего срока оказания Услуг связи обеспечивает за свой счет настройку, включая изменение настроек в соответствии с запросами Заказчика, техническое обслуживание и ремонт оборудования, в том числе криптомаршрутизаторов и маршрутизаторов, установленных Исполнителем в СЗО в рамках оказания услуг в соответствии с настоящим ТЗ. При этом сроки и порядок выполнения регламентных и ремонтных работ устанавливаются Регламентом технической поддержки при оказании Услуги связи, утвержденным Заказчиком.

2.42.4. Требования к средствам маршрутизации:

2.42.4.1. Средства маршрутизации должны выполнять функций Firewall и QoS, а также должны:

- обеспечивать возможность мониторинга состояния по протоколу SNMP;
- поддерживать статическую и динамическую маршрутизацию IPv4 и IPv6 по протоколу BGPv4 (спецификация IETF RFC 1771), OSPFv2, RIPv2;
- обладать механизмами фильтрации трафика по TCP/UDP портам;
- поддерживать протоколы резервирования VRRP;
- поддерживать механизм NAT;

– обеспечивать поддержку не менее 3 (трех) классов обслуживания трафика модели DiffServ;
– обеспечивать возможность работы в качестве DHCP relay агента, клиента, сервера;
– обеспечивать возможность работы в качестве DNS (клиента, proxy, сервера), NTP (клиента, сервера);
– обеспечивать возможность поддержки создания VPN туннелей.

2.42.4.2. Режим работы средств маршрутизации – круглосуточный необслуживаемый, по схеме 24 часа в сутки, 7 дней в неделю.

2.43. Требования к модульности Услуг связи:

1) Услуги связи должны обладать модульностью;

2) Модульность должна обеспечивать возможность добавлять и комбинировать Компоненты в рамках предоставления Услуг связи;

3) Каждый Компонент должен обеспечивать выполнение своей функции.

2.44. Требования к масштабируемости Услуг связи:

1) Исполнитель должен обеспечить техническую готовность сети передачи данных Исполнителя к оказанию Услуг связи СЗО в соответствии с полученными от Заказчика Заявками;

2) Услуги связи должны обеспечивать масштабируемость, достаточную для работы самих Услуг связи, а также всех Компонентов в ее составе без дополнительных затрат Заказчика;

3) Масштабируемость Услуг связи может достигаться путем модернизации программного и/или аппаратного обеспечения, подключения дополнительных систем к ЕСПД и расширением пропускной способности каналов связи;

4) Расширение каналов связи не должно приводить к ухудшению параметров качества Услуг связи и не должно оказывать влияние на Компоненты;

5) Исполнитель во время исполнения государственного контракта самостоятельно или по требованию Заказчика определяет необходимость масштабирования Услуг.

2.45. Требования к отказоустойчивости Услуг:

1) Услуги связи должны обеспечивать отказоустойчивость в целом и отказоустойчивость Компонентов в частности. В случае возникновения сбоев или аварий Услуги связи должны предоставлять возможность изменения алгоритмов работы, для обеспечения сохранения работоспособности Услуг связи в полном объеме;

2) Отказоустойчивость подключения при оказании Услуг связи должна обеспечиваться следующими решениями, но не исключительно:

– использование резервных каналов связи на магистральных линиях ЕСПД;

– использование на сегментах MPLS-сети Исполнителя отказоустойчивых конфигураций оборудования и программного обеспечения, по схемам N+1 или N+N;

– использование источников бесперебойного питания на Точках присоединения для защиты от потери электропитания;

– дублирование ключевых компонентов;

– использование резервных каналов связи в магистральной составляющей ЕСПД между Точками присоединения ЕСПД, позволяющих перенаправлять трафик в обход отказавшего пути;

– маршрутизацию трафика с применением протоколов статической или динамической маршрутизации;

3) В случае прекращения энергоснабжающей организацией подачи электропитания на Точку присоединения ЕСПД, Исполнитель обязан продолжить предоставление Услуг связи в течение 4 часов. Более длительные перерывы в электроснабжении, подтвержденные со стороны энергоснабжающих организаций, считаются форс-мажором.

2.45.1. Требования к отказоустойчивости Компонента «Мониторинг и обеспечение безопасности связи» в части Элемента межсетевого экранирования (МСЭ):

1) Отказоустойчивость МСЭ должно обеспечиваться следующими

решениями:

– использование отказоустойчивых конфигураций аппаратного и программного обеспечения;

– резервирование настроек средств защиты.

2.45.2. Требования к отказоустойчивости Компонента «Мониторинг и обеспечение безопасности связи» в части Элемента «защиты от DDoS»:

1) Отказоустойчивость средств защиты от DDOS должно обеспечиваться следующими решениями:

– использование отказоустойчивых конфигураций аппаратного и программного обеспечения;

– использование резервных каналов связи в магистрали, позволяющих перенаправлять трафик в обход отказавшего пути;

– резервирование настроек средств защиты.

2.46. Требования к реализации Системы технических средств для обеспечения функций оперативно-розыскных мероприятий (СОРМ).

Обеспечить реализацию функций СОРМ (СОРМ 2 и СОРМ 3), в соответствии с требованиями нормативно-правовых актов:

1) Требования к сетям электросвязи для проведения оперативно-розыскных мероприятий Часть 1. Общие требования (утв. приказом Министерства информационных технологий и связи РФ от 16 января 2008 г. № 6);

2) Правила оказания телематических услуг связи (утв. постановлением Правительства РФ от 31 декабря 2021 № 2607 "Об утверждении Правил оказания телематических услуг связи");

3) Постановление Правительства РФ от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность»;

4) Приказ Министерства связи и массовых коммуникаций РФ от 16 апреля 2014 г. № 83 «Об утверждении Правил применения оборудования систем

коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть III. Правила применения оборудования коммутации и маршрутизации пакетов информации сетей передачи данных, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий»;

5) Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 29 октября 2018 г. № 573 «Об утверждении Требований к техническим и программным средствам информационных систем, содержащих базы данных абонентов оператора связи и предоставленных им услугах связи, а также информацию о пользователях услугами связи и о предоставленных им услугах связи, обеспечивающих выполнение установленных действий при проведении оперативно-розыскных мероприятий»;

6) Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

2.47. Требования к хранению передаваемого трафика и созданию систем хранения данных.

Обеспечить реализацию функций по хранению передаваемого трафика и созданию систем хранения данных в соответствии с требованиями нормативно-правовых актов и выполнения действующего согласованного плана мероприятий по реализации требований Федерального закона от 06 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

2.48. Требования к системному проекту.

Не позднее 90 календарных дней с момента подписания Контракта, Исполнитель должен предоставить Заказчику системный проект, описывающий вопросы предоставления Услуг связи, включая:

2.48.1. Модель угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей программных модулей, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз и модели нарушителя безопасности информации применяются методические документы, разработанные и утвержденные ФСТЭК России, учитывается информация из Банка данных угроз безопасности ФСТЭК России (https://bdu.fstec.ru/), Приказ ФСБ России от 10 июля 2014 г. № 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».

Требования к Компоненту «Защита данных» определяются:
- в зависимости от класса защищенности и угроз безопасности информации, включенных в модель угроз безопасности информации;
- с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, в части определения:

-целей и задач обеспечения защиты информации;

-класса защищенности;

-перечня нормативных правовых актов, методических документов и национальных стандартов, которым должны соответствовать Компонент «Защита данных»;

-требований к защите информации при информационном взаимодействии с ИС и информационно-телекоммуникационными сетями, в том числе с ИС ФОИВ, РОИВ.

2.48.2. Реализацию СОРМ.

2.48.3. Мероприятия по реализации требований Федерального закона от 06 июля 2016 года № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму».

2.48.4. Обеспечение выполнения требований к оказанию Компонента «Предоставление доступа».

2.48.5. Обеспечение выполнения требований по оказанию Компонента «Ограничение доступа к информации.

2.48.6. Обеспечение выполнения требований по оказанию Компонента «Мониторинг и обеспечение безопасности связи».

2.48.7. Общие принципы построения сетевой инфраструктуры для оказания Услуг связи.

2.48.8. Инженерно-технические решения по организации оказания Услуг связи для СЗО на базе ЕСПД.

2.48.9. Инженерно-технические решения по организации оказания Услуг связи для СЗО на базе спутниковой сети связи.

2.48.10. Описание и структурные схемы построения ЕСПД по субъектам Российской Федерации.

При построении инфраструктуры для оказания Компонента «Защита данных», провести оценку в соответствующем порядке, установленном ФЗ №187 «О безопасности критической информационной для инфраструктуры Российской федерации» от 26.07.2017 г.

2.49. Требования к технической поддержке Исполнителя при оказании Услуг связи:

2.49.1. В период оказания Услуг связи Исполнитель обязан осуществлять техническую поддержку Потребителей (далее - Техническая

поддержка) по вопросам оказания Услуг связи в соответствие с Регламентом технической поддержки при оказании Услуги связи (утвержденным Заказчиком в соответствии п. 7.1. ТЗ).

2.49.2. В целях оказания дополнительной консультационной поддержки Потребителей по вопросам, связанным с оказанием Услуг связи, а также в целях обеспечения возможности управления Услугами связи со стороны Потребителей, Исполнитель должен создать ресурс в сети Интернет, разместить на нем инструкции и дополнительные материалы для Потребителей и создать Личный кабинет.

2.49.3. Техническая поддержка должна осуществляться круглосуточно и ежедневно в соответствии с Регламентом технической поддержки при оказании Услуги связи, утвержденным Заказчиком. Для Объектов ЦИК Регламент разрабатывается отдельно и должен быть согласован с ЦИК России. После утверждения Регламента Заказчиком, он должен быть размещен Исполнителем на ресурсе, созданном в соответствии с п. 2.50.2 ТЗ, и направлен для ознакомления
в адрес всех Потребителей, указанных в Заявках Заказчика на оказание Услуги связи.

2.49.4. Обращения в техническую поддержку должны регистрироваться посредством следующих способов:

– по единому бесплатному контактному номеру телефона;

– посредством отправки сообщений электронной почты на единый почтовый ящик;

– посредством личного кабинета;

– автоматическое заведение инцидентов на основании событий, полученных в ходе оказания Компонента «Мониторинг и обеспечение безопасности связи» (Элемент «Мониторинг параметров качества предоставляемых услуг»).

2.49.5. Профилактические работы:

1) При проведении профилактических работ допускается перерыв

в оказании Услуг связи.

2) Проведение указанных видов работ должно осуществляться в часы наименьшей нагрузки и информирование представителя СЗО должно быть произведено заранее не менее чем за 3 рабочих дня до начала работ по телефону или электронной почте.

2.49.6. Приоритеты и время восстановления работоспособности Услуг связи для Объектов ЦИК определяется требованиями Приложения №7.

2.49.7. Приоритеты и время восстановления работоспособности Услуг связи для Образовательных организаций:

1) Неисправности подразделяются на четыре приоритета по степени срочности их устранения:

1-ый приоритет – Критичный:

– сопровождаемая услуга не доступна (авария);
– массовые (более десяти обращений в течение тридцати минут от различных СЗО в отдельном субъекте Российской Федерации) обращений в техническую поддержку Исполнителя, связанные с нарушением работоспособности Услуг связи, относящиеся к одному событию;

2-ой приоритет – Высокий:

– наблюдается массовая деградация производительности или периодическое прерывание услуги в не менее 5 процентов общего числа СЗО в регионе;
– фиксируются периодические прерывания или деградация (снижение скорости относительно заявленной) в работе услуги в одном СЗО;

3-й приоритет – Средний:

– нарушение вспомогательной функциональности Услуг связи;
– запрос на обслуживание или изменение настроек;
– запрос на изменение конфигурации или функциональности Услуг связи;

4-й приоритет – Низкий:

– проблемы без утраты способности Услуг связи;
– запросы по оказанию информационной поддержки;
– представителю СЗО требуется консультация.

Показатель	Норматив времени реакции
Режим регистрации обращений	24 часа 7 дней в неделю
Время решения инцидентов первого приоритета	10* часов рабочего времени (с 08:00 до 18:00 местного времени по рабочим дням) с момента регистрации обращения. В периоды проведения избирательных компаний различного уровня и периоды проведения единого государственного экзамена- круглосуточно
Время решения инцидентов второго приоритета	14 * часов рабочего времени (с 08:00 до 18:00 местного времени по рабочим дням) с момента регистрации обращения. В период проведения избирательных компаний различного уровня и периоды проведения единого государственного экзамена - круглосуточно
Время решения инцидентов третьего приоритета	20* часа рабочего времени (с 08:00 до 18:00 местного времени по рабочим дням). В период проведения избирательных компаний различного уровня- круглосуточно
Время решения инцидентов четвертого приоритета	24* часа рабочего времени (с 08:00 до 18:00 местного времени по рабочим дням) В период проведения избирательных компаний различного уровня- круглосуточно

*) Указано время устранения неисправности, не требующее выезда. Для восстановления магистральной кабельной инфраструктуры, работ на узловом и магистральном оборудовании, замены оборудования/восстановления кабельной инфраструктуры Исполнителя и иных работ, требующих выезда в СЗО, нормативные сроки решения инцидента увеличиваются на 48 часов. Указано

время для восстановительных работ инфраструктуры Исполнителя, без учета времени восстановительных работ оборудования СЗО, инфраструктуры информационных систем, а также наличия СЗО в труднодоступном населенном пункте.

Для объектов, расположенных в труднодоступных населенных пунктах (труднодоступный населенный пункт - это населенный пункт, который в силу погодных, природных, техногенных и иных обстоятельств и (или) отсутствия элементов инфраструктуры становится недоступным или труднодостижимым для транспортных средств) срок решения инцидента для восстановления кабельной инфраструктуры Исполнителя, замены оборудования Исполнителя и иных работ, требующих выезда на объект СЗО, а также для восстановления магистральной кабельной инфраструктуры, работ на узловом и магистральном оборудовании, увеличивается до 10 рабочих дней.

Регламент технической поддержки при оказании Услуги связи должен предусматривать порядок взаимодействия между Потребителем, Исполнителем и Заказчиком, в том числе:

- порядок регистрации, открытия, обработки и закрытия обращений Потребителей по вопросам предоставления Услуг связи Службой технической поддержки Заказчика и Службой технической поддержки Исполнителя;
- порядок регистрации, открытия, обработки и закрытия обращений, созданных на основании событий, полученных в ходе оказания Компонента «Мониторинг и обеспечение безопасности связи» (Элемент «Мониторинг параметров качества предоставляемых услуг»);
- порядок взаимодействия Потребителей, Службой технической поддержки Заказчика и Службой технической поддержки Исполнителя при планировании и проведении технологических перерывов;
- порядок формирования и предоставления Заказчику отчетности по обращениям Потребителей и отчетности о качестве услуг связи Компонента «Мониторинг и обеспечение безопасности связи» (Элемент «Мониторинг параметров качества предоставляемых услуг»);
- порядок регистрации, открытия, обработки и закрытия обращений Потребителей, направленных через Личный кабинет.

Примечания:

1) В случаях, если для решения заявки требуется дополнительная информация от Потребителя или проверка работоспособности с его стороны, время простоя не учитывается, до получения запрошенной информации.

2) Отключения (перерывы), вызванные любой из перечисленных ниже причин, не классифицируются как недоступность или неисправность:

- проведение плановых профилактических работ (далее – ППР) с уведомлением представителей Заказчика и/или Потребителей в срок не менее трех рабочих дней до времени проведения работ;
- работа на оборудовании Исполнителя по запросу Потребителя;
- тестирование Услуг связи по запросу Потребителя в случае, когда не было выявлено никакой неисправности или недоступности;
- неисправности или дефекты оборудования Потребителей;
- перерывы в предоставлении Услуг связи, вызванные умышленными или неумышленными действиями Потребителей;
- форс-мажор, в том числе действия, впрямую или косвенно влияющие на сроки организации работ или соблюдение Исполнителем обязательств в рамках ТЗ.

2.49.8. Исполнитель в течение всего срока оказания Услуг связи предоставляет Заказчику доступ через оборудование криптозащиты, к системе регистрации обращений, управления и решения инцидентов/запросов Исполнителя (Service Desk).

2.49.9. Исполнитель в течение всего срока оказания Услуг связи предоставляет выделенный многоканальный телефонный номер в коде доступа к услуге электросвязи «800» для регистрации обращений Потребителей Службой технической поддержки Заказчика, а также предоставляет Заказчику возможность автоматического распределения вызовов. Вызовы Потребителей на выделенный телефонный номер Исполнителя должны осуществляться без взимания платы за исходящее соединение на всей территории Российской Федерации.

3. Состав Услуг связи.

Оказание Исполнителем Услуг связи для СЗО и Объектов ЦИК осуществляется на территориях субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя)(Далее – **Услуги связи**) и состоит из следующих Компонентов:

3.1. Компонент «Предоставление доступа» обеспечивает предоставление

доступа СЗО, Объектам ЦИК, расположенным на территории субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя) к ЕСПД в случае его отсутствия (Далее - **Предоставление доступа**).

3.2. Компонент «Передача данных» обеспечивает передачу данных при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети Интернет (Далее - **Передача данных**) в составе:

— Компонент «Защита данных» обеспечивает защиту данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным и иным информационным системам, а также к сети Интернет (Далее - **Защита данных**);

— Компонент «Ограничение доступа к информации» обеспечивает ограничение доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, наносящей вред здоровью и развитию детей, содержащейся в сети Интернет для образовательных организаций (Далее - **Ограничение доступа к информации**);

— Компонент «Мониторинг и обеспечение безопасности связи» обеспечивает мониторинг и обеспечение безопасности связи при предоставлении доступа к государственным, муниципальным и иным информационным системам, а также к сети Интернет (Далее - **Мониторинг и обеспечение безопасности связи**).

3.3. Компонент «Организация канала L2» обеспечивает организацию канала связи, включая его создание или модернизацию в случае возможности улучшения параметров канала связи в соответствии с ТЗ, для СЗО, Объектов ЦИК, расположенных на территории субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя) с целью подключения к ЕСПД (Далее - **Организация канала L2**).

3.4. Компонент «Передача данных L2» обеспечивает передачу данных между СЗО, Объектом ЦИК, расположенными на территории субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя)

и ЕСПД (Далее - **Передача данных L2**).

4. Требования к Услугам связи.

4.1. Услуги связи должны представлять собой совокупность Компонентов с возможностью их комбинации и изменений. Основными принципами обеспечения Услуг связи должны являться универсальность, управляемость и масштабируемость.

4.2. Управление Услугами связи.

Исполнитель должен осуществлять управление изменениями, которые могут включать изменения параметров Услуг связи:

– интерфейсы оборудования Точек присоединения ЕСПД, к которому подключается Канал L2;

– интерфейсы оборудования Точек присоединения ЕСПД, к которым подключается оборудование КСА Объектов ЦИК;

– топология ЕСПД;

– IP адреса и подсети;

– протоколы маршрутизации;

– профили портов доступа;

– пропускная способность передачи трафика разных типов по предоставляемым каналам связи между СЗО, Объектами ЦИК в зоне ответственности Исполнителя;

– параметры качества передачи IP-пакетов и Ethernet кадров СЗО между СЗО в зоне ответственности Исполнителя;

– подключение СЗО к сети Исполнителя при изменении количества СЗО, адреса месторасположения СЗО в зоне ответственности Исполнителя;

– параметры качества передачи IP-пакетов между СЗО, Объектами ЦИК в зоне ответственности Исполнителя;

– подключение Объектов ЦИК к ЕСПД при изменении количества Объектов ЦИК, адреса месторасположения Объекта ЦИК в зоне ответственности

Исполнителя (по дополнительному согласованию с Заказчиком);

– приостановление или возобновление оказания Услуг связи;

– оказание Услуг связи для СЗО, Объектов ЦИК по согласованию между Заказчиком и Исполнителем;

– прекращение оказания Услуг связи;

– иные согласованные Исполнителем и Заказчиком параметры Услуг связи.

4.3. Требования к производительности Услуг связи:

1) Производительность Услуг связи должна быть достаточной для выполнения возложенных на нее задач. В случае необходимости увеличения производительности Исполнитель должен предусмотреть такую возможность без дополнительных капитальных затрат.

2) Увеличение производительности Услуг связи должно достигаться следующими способами:

– замена или модернизация аппаратного обеспечения;

– замена или модернизация программного обеспечения;

– увеличение пропускной способности каналов связи.

5. Требования к Компонентам.

5.1. Услуги связи должны представлять собой набор следующих компонентов и элементов:

1) Компонент «Предоставление доступа».

2) Компонент «Передача данных»:

- Элемент «Передача данных в ВЧС с заданными параметрами качества»;
- Элемент «Передача данных в сеть Интернет.

3) Компонент «Защита данных»:

- Элемент «Криптографическая защита каналов связи».

4) Компонент «Ограничение доступа к информации»:

- Элемент «Контентная фильтрация».

5) Компонент «Мониторинг и обеспечение безопасности связи»:
   - Элемент «Мониторинг параметров качества предоставляемых услуг»;
   - Элемент «Защита от DDoS атак»;
   - Элемент «Межсетевое экранирование».
6) Компонент «Организация канала L2».
7) Компонент «Передача данных L2».

5.2. **Компонент «Предоставление доступа».**

Компонент «Предоставление доступа» должен являться универсальным, управляемым и масштабируемым.

5.2.1. Требования к архитектуре Компонента «Предоставление доступа».

Архитектура Компонента «Предоставление доступа» приведена на рисунках 1 и 2.

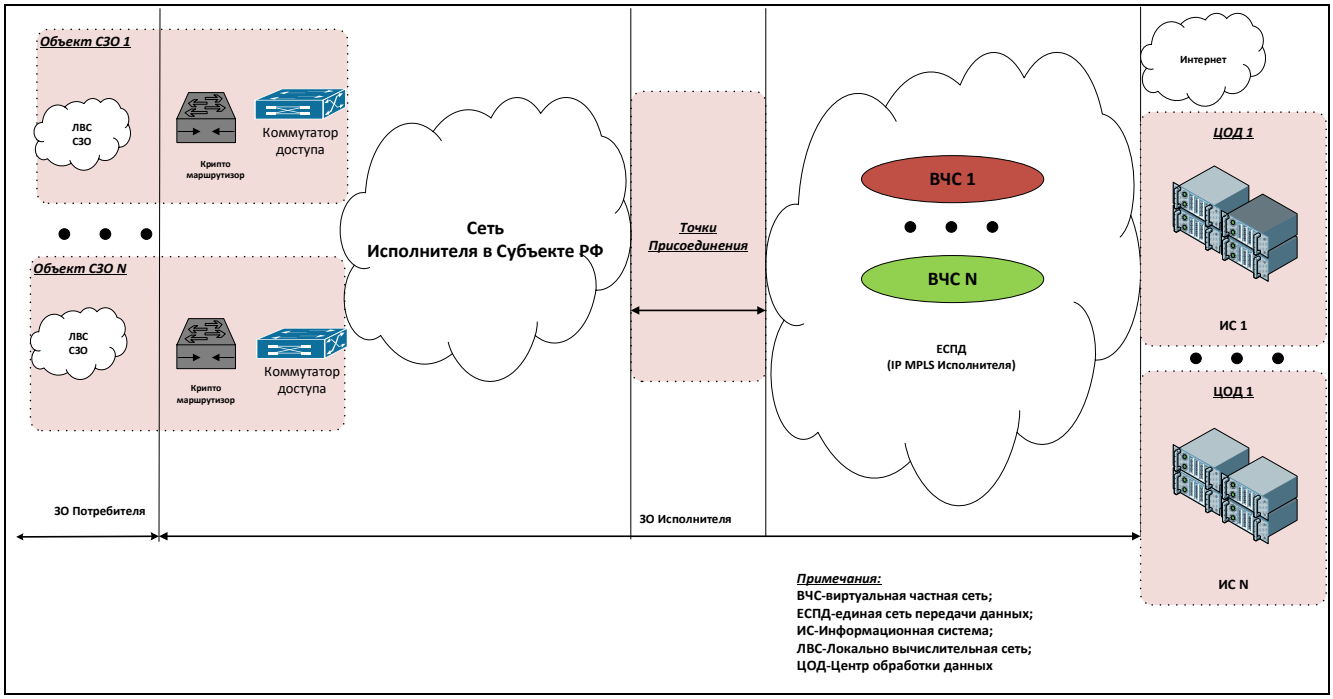

Рис.1.Архитектура Компонента «Предоставление доступа» для СЗО

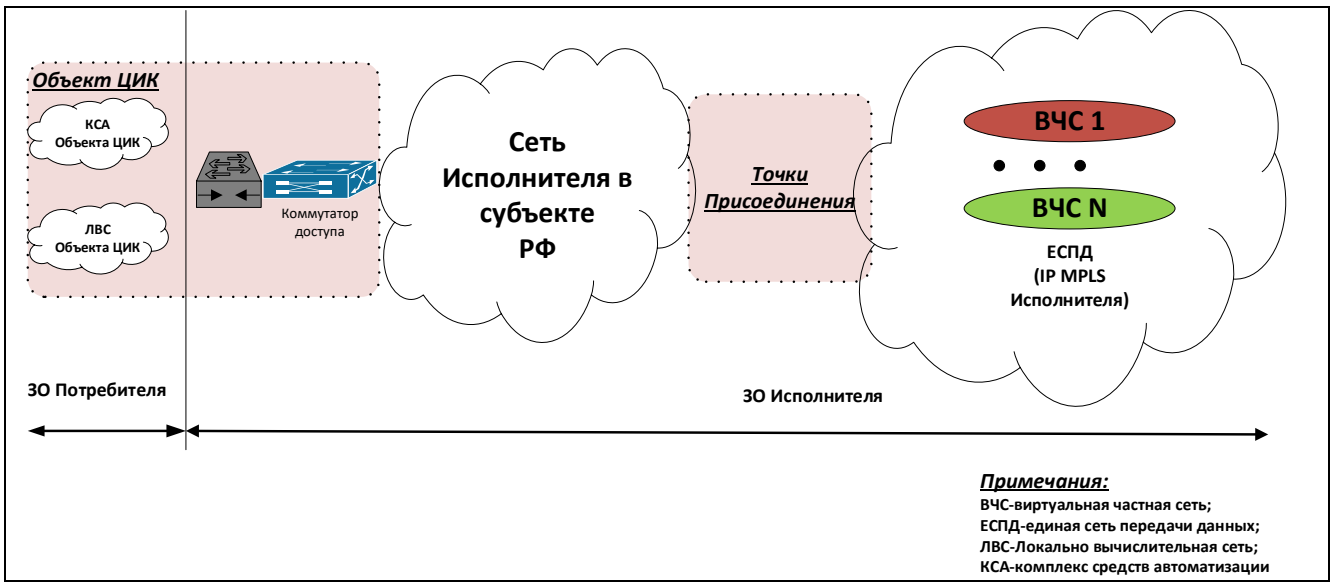

Рис.2.Архитектура Компонента «Предоставление доступа» для Объектов ЦИК.

5.2.2. Технические средства реализации Компонента Услуг «Предоставление доступа».

Подключение Канала L2 к Точке присоединения ЕСПД, Объектов ЦИК к Точке присоединения ЕСПД осуществляется в соответствии с требованиями ТЗ.

5.2.3. Управление Компонентом «Предоставление доступа».

Для указанных Заказчиком СЗО, Объектов ЦИК Исполнитель должен осуществлять управление изменениями, которые могут включать изменения параметров оказания Услуг связи:

– интерфейс на оборудовании Исполнителя, к которому подключается Канал L2;

– интерфейс на оборудовании Исполнителя, к которому подключается оборудование КСА Объекта ЦИК;

– топология ЕСПД;

– IP адреса и подсети;

– протоколы маршрутизации;

– профили портов доступа;

– пропускная способность передачи трафика разных типов

по предоставляемым каналам связи между СЗО, Объектами ЦИК в зоне ответственности Исполнителя;

– параметры качества передачи IP-пакетов и Ethernet кадров СЗО между СЗО в зоне ответственности Исполнителя;

– подключение СЗО к сети Исполнителя при изменении адреса месторасположения СЗО в зоне ответственности Исполнителя;

– приостановление или возобновление оказания Услуги связи;

– пропускная способность передачи трафика разных типов по предоставляемым каналам связи между Объектами ЦИК в зоне ответственности Исполнителя;

– подключение Объекта ЦИК к ЕСПД при изменении адреса месторасположения Объекта ЦИК в зоне ответственности Исполнителя;

– оказание Услуг связи для новых СЗО, Объектов ЦИК в зоне ответственности Исполнителя по согласованию между Заказчиком и Исполнителем;

– прекращение оказания Услуг связи по предоставлению доступа;

– иные согласованные Исполнителем и Заказчиком параметры Услуг связи.

5.2.4. Требования к дополнительному функционалу и сопряжению со смежными системами:

1) Компонент должен иметь возможность расширять функционал посредством подключения к информационным ресурсам и системам, без снижения уровня информационной безопасности, емкости Услуг связи и производительности.

2) К смежным системам относятся:

– сеть Интернет;

– внешние центры обработки данных Исполнителя и/или Владельцев ИС.

5.2.5. Требования к производительности.

Производительность должна быть достаточной для выполнения возложенных на нее задач. В случае необходимости увеличения

производительности Исполнитель должен предусмотреть такую возможность.

5.2.6. Компонент «Предоставление доступа» должен обеспечить совокупную пропускную способность из расчета необходимости обеспечения каждому подключенному СЗО, в соответствии с Заявками, следующих параметров:

– находящиеся в городских поселениях – не менее 100 (ста) Мбит/с по направлению «от»/«к» СЗО;
– находящиеся в сельских поселениях – не менее 50 (пятидесяти) Мбит/с по направлению «от»/«к» СЗО;
– находящиеся в труднодоступных населенных пунктах, подключенные по спутниковым каналам связи – не менее 1 (одного) Мбит/с по направлению «от»/«к» СЗО.

Для СЗО, подключенному по иной технологии отличной от волоконно-оптической и спутниковой технологии допускается асимметричность канала связи.

5.2.7. Компонент «Предоставление доступа» должен обеспечить совокупную пропускную способность из расчета необходимости обеспечения каждому подключенному Объекту ЦИК следующих параметров:

– ТИК – не менее 60 (шестьдесят) Мбит/с по направлениям «от»/«к» ТИК, с учетом (включая) требования к скорости передачи данных для доступа к ГАС «Выборы», указанных в Приложении № 7 к ТЗ (за исключением ТИК расположенных в удаленных и труднодоступных населенных пунктах);
– ИК СРФ – не менее 140 (сто сорок) Мбит/с по направлениям «от»/«к» ИК СРФ, с учетом (включая) требования к скорости передачи данных для доступа к ГАС «Выборы», указанных в Приложении № 7 к ТЗ (за исключением ИК СРФ расположенных в удаленных и труднодоступных населенных пунктах);

– ЦИК России – не менее 40 000 (сорок тысяч) Мбит/с по направлениям «от»/«к» ЦИК России, с учетом (включая) требования к скорости передачи данных для доступа к ГАС «Выборы», указанных в Приложении № 7 к ТЗ;

– Для Объектов ЦИК, расположенных в удаленных и труднодоступных населенных пунктах - не менее 1 (одного) Мбит/с «от»/«к» Объекту ЦИК с учетом (включая) требования к скорости передачи данных для доступа к ГАС «Выборы», указанных в Приложении № 7 к ТЗ.

5.2.8. Увеличение производительности Компонента «Предоставление доступа» должно достигаться следующими способами:

– замена или модернизация аппаратного обеспечения;

– замена или модернизация программного обеспечения;

– увеличение пропускной способности каналов связи, магистральных и на уровне сетей доступа.

5.2.9. Компонент «Предоставление доступа» должен обеспечивать доступ к сети Интернет и возможность доступа СЗО к ИС, должен обеспечивать доступ к сети Интернет и доступ Объектов ЦИК к ГАС «Выборы» в соответствии с требованиями ТЗ.

5.2.10. Назначение Компонента «Предоставление доступа».

Компонент Услуг связи «Предоставление доступа» предназначен для организации подключения СЗО, Объектов ЦИК через Канал L2 к Точкам присоединения ЕСПД, Объектов ЦИК к Точкам присоединения к ЕСПД для Объектов ЦИК.

5.2.11. Требование к Компоненту «Предоставление доступа»:

1) ЕСПД должна представлять собой выделенную сеть, построенную на оборудовании Исполнителя и использующую собственные каналы связи Исполнителя, исключающую организацию каналов поверх сети Интернет.

2) ЕСПД должна быть построена с использованием технологии многопротокольной коммутации по меткам IP/MPLS и иметь возможность обеспечения сервисов L2/L3 MPLS VPN.

3) ЕСПД должна поддерживать статическую и динамическую маршрутизацию по протоколу BGPv4 (спецификация IETF RFC 1771).

4) Исполнитель должен предоставить маршрутизируемую виртуальную частную сеть 3-го уровня согласно классификации ГОСТ Р ИСО/МЭК 7498-1-99, при этом указанная сеть должна обеспечивать передачу информации по протоколу IP согласно спецификации IETF RFC 791 и обеспечивать прохождение между интерфейсами доступа оборудования Потребителей IP-пакетов размером до 1514 байт включительно (MTU) без их фрагментации.

5) ЕСПД должна позволять создание несколько выделенных ВЧС, каждый из которых изолирован друг от друга на логическом уровне.

6) ЕСПД должна иметь возможность организовать, как минимум, следующие ВЧС:

– ВЧС для взаимодействия между образовательными организациями и централизованного доступа в сеть Интернет (на уровне субъекта Российской Федерации), а также с возможностью доступа к ИС на федеральном и региональном уровнях.

– ВЧС для ЦИК, ИК СРФ, ТИК для передачи данных ГАС «Выборы»,

– ВЧС для ИК СРФ, ТИК для доступа в сеть Интернет.

5.2.12. Требования к топологии сети:

1) В ЕСПД Исполнитель должен организовать Точки присоединения ЕСПД в административных центрах субъектов РФ (за исключением Республики Крым и г. Севастополя).

2) Точка присоединения ЕСПД должна быть подключена к магистральной сети Исполнителя при помощи ВОЛС. Предпочтительно подключение Точек присоединения ЕСПД к магистральной сети Исполнителя при помощи резервированных каналов.

3) ЕСПД должна обладать возможностью организации следующих типов связей для ВЧС:

– «каждый с каждым» (Full mesh) – между любой парой СЕ пакет проходит по оптимальному с точки зрения сети Исполнителя маршруту;

– «звезда» или «частичная связность» (hub & spoke) – реализуется связность таким образом, что узлы сети, определенные как spoke получают маршрутную информацию только от hub, hub получает маршруты от всех spoke. Это означает, что трафик от spoke может быть направлен только в сторону hub. После получения и обработки Трафика hub может направлять трафик на другой spoke, тем самым замыкая весь Трафик в ВЧС на себя; задачи маршрутизации трафика, проходящего через hub, берет на себя Заказчик;

– «произвольная связность» – другие варианты топологии виртуальной частной сети, необходимые Заказчику; для реализации данного варианта в каждом конкретном случае разрабатывается схема организации услуги.

5.2.13. Общие принципы формирования адресного пространства:

1) Формирование адресного пространства в ЕСПД должна основываться на рекомендациях документа RFC 1918 «Address Allocation for Private Internets» (распределение адресов в частных IP-сетях), а также должно учитывать рекомендации RFC 6890 «Special-Purpose IP Address Registries» и RFC 2544 «Benchmarking Methodology for Network Interconnect Devices».

2) В ВЧС ЕСПД должны использоваться сети класса А из диапазона, разрешенного к применению в частных IP-сетях 10.0.0.0/8. Использование иных сетей согласовывается с Заказчиком.

3) Кроме основного адресного пространства, в виде исключения, могут использоваться дополнительно диапазоны IP-сетей и отдельных адресов.

4) Трансляция сетевых адресов в режиме «один к многим» при взаимодействии между Потребителями должна отсутствовать. Трансляция адресов в режиме «1 к 1» возможна по согласованию с Исполнителем. Пересечение адресных пространств исключается использованием легитимных (выданных централизованно Исполнителем) адресных пулов.

5.2.14. Требования к качеству обслуживания:

1) ЕСПД должна предоставлять как минимум 3 класса качества обслуживания трафика модели DiffServ. По согласованию с Заказчиком допускается использование моделей качества обслуживания с большим или

меньшим количеством классов.

2) В рамках модели с 3 классами обслуживания при передаче трафика между Потребителями ЕСПД должна поддерживать:

– Класс 1 – трафик приложений реального времени (голос, видео), критичный к потерям пакетов, задержкам и колебаниям задержки;
– Класс 2 – трафик корпоративных информационных систем, критичный к задержкам и потерям;
– Класс 3 – трафик, некритичный к задержкам (Интернет, различные сетевые службы).

3) Классификация трафика должна осуществляться для каждого IP-пакета в отдельности, передаваемого в IP/MPLS сеть Исполнителя, в соответствии со значением его поля DSCP, как указано в следующей таблице:

Тип трафика	Значение DSCP заголовка
Класс 1	CS4
Класс 2	AF21
Класс 3	Default (любые значения, отличные от классов 1 и 2)

Примечания:

– При передаче данных через IP/MPLS сеть Исполнителя заголовки IP-пакетов меняться не должны.

– При превышении трафиком Класса 1 пропускной способности, установленной на порту для Класса 1, должен производиться сброс IP-пакетов с качеством Класса 3; при превышении трафиком Класса 2, пропускной способности, установленной на порту для Класса 2, – сброс IP-пакетов с качеством Класса 3; при превышении трафиком Класса 3 пропускной способности порта – сброс IP-пакетов.

5.3. Компонент «Передача данных».

5.3.1. Требования к архитектуре Компонента «Передача данных».

Архитектура Компонента «Передача данных» приведена

на рисунках 3 и 4.

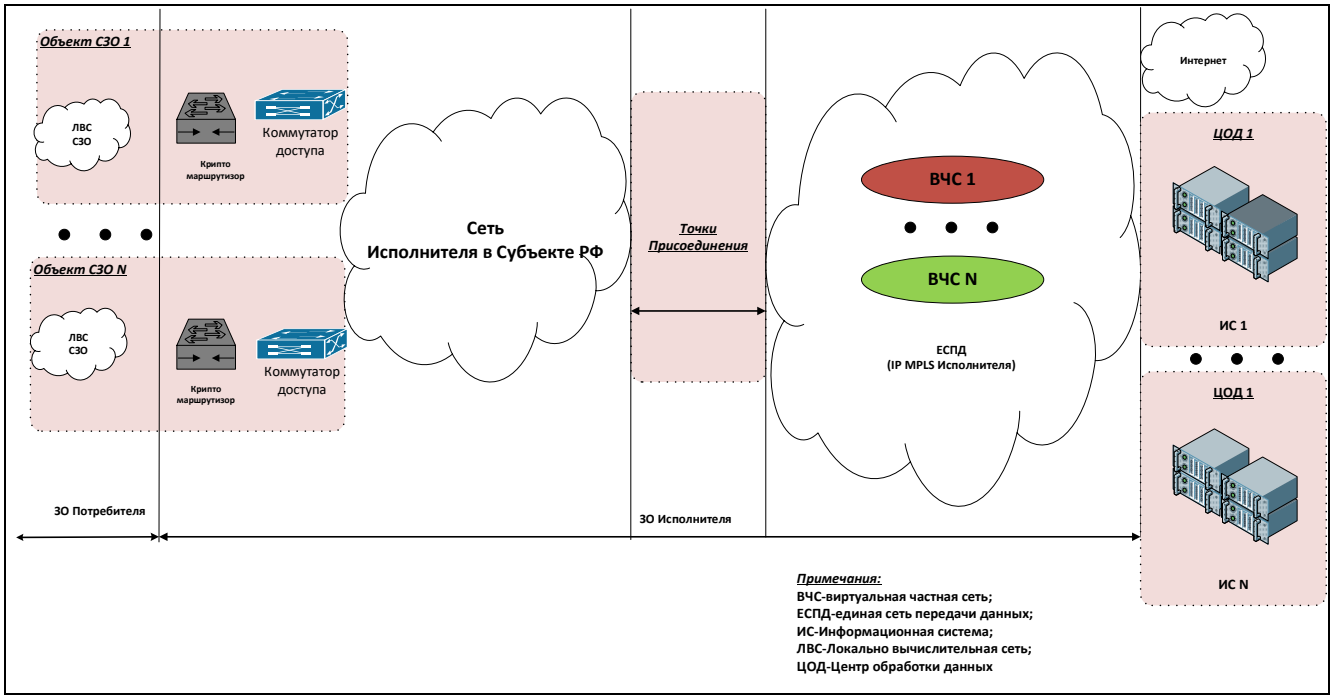

Рис.3.Архитектура Компонента «Передача данных».

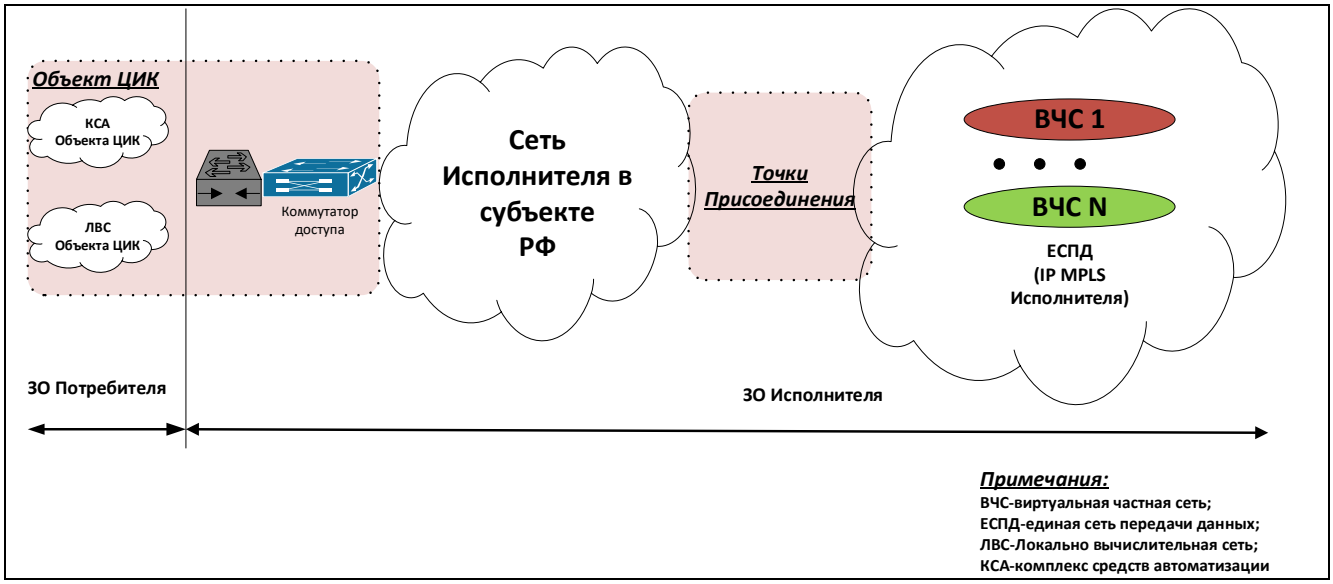

Рис.4.Архитектура Компонента «Передача данных» для Объектов ЦИК.

5.3.2. Элемент «Передача данных в частной виртуальной сети с заданными параметрами качества**» (далее – Элемент ПД в ВЧС).**

5.3.2.1.Назначение Элемента ПД в ВЧС.

Элемент ПД в ВЧС предназначен для передачи данных посредством ЕСПД между Точками присоединения ЕСПД, при осуществлении доступа СЗО к государственным, муниципальным и иным информационным системам, и сети Интернет.

Элемент ПД в ВЧС предназначен для передачи данных по ЕСПД между Точками присоединения ЕСПД при осуществлении доступа Объектов ЦИК к ГАС «Выборы».

5.3.2.2. Требования к пропускной способности.

ПД в ВЧС должна осуществляться с учетом следующих скоростных параметров подключения **СЗО** к ЕСПД, в соответствии с Заявками:

	Скорость доступа к сети Интернет
Для образовательных организаций, находящихся в городских поселениях	Не менее 100 Мбит/с
Для образовательных организаций, находящихся в сельских поселениях	Не менее 50 Мбит/с
Для образовательных организаций, подключаемых с использованием иных линий связи (в том числе спутниковых) в случае невозможности использования ВОЛС	Не менее 1 Мбит/с

ПД в ВЧС должна осуществляться с учетом следующих скоростных параметров подключения объектов **ЦИК** к ЕСПД:

	Скорость доступа к сети	
	Интернет	ГАС «Выборы»
Для Центральной избирательной комиссии Российской Федерации	-	40 Гб/с
Для Избирательных комиссий субъектов Российской Федерации	100 Мбит/с	40 Мбит/с
Для Территориальных избирательных комиссий	50 Мбит/с	10 Мбит/с
Для объекты ЦИК, расположенных в труднодоступных населенных пунктах и подключенных с использованием спутниковых линий связи	512 кбит/с	512 кбит/с

5.3.2.3. Требования к качеству обслуживания.

1) Элемент ПД в ВЧС должен предоставлять как минимум 3 класса качества обслуживания трафика модели DiffServ. По согласованию с Заказчиком допускается использование моделей качества обслуживания с большим или меньшим количеством классов.

2) В рамках модели с 3 классами обслуживания при передаче трафика между СЗО ЕСПД должна поддерживать:

- Класс 1 – трафик приложений реального времени (голос, видео), критичный к потерям пакетов, задержкам и колебаниям задержки;
- Класс 2 – трафик корпоративных информационных систем, критичный к задержкам и потерям;
- Класс 3 – трафик, некритичный к задержкам (Интернет, различные сетевые службы).

3) Классификация трафика должна осуществляться для каждого IP-пакета в отдельности, передаваемого в IP/MPLS сеть Исполнителя, в соответствии со значением его поля DSCP, как указано в следующей таблице:

Тип трафика	Значение DSCP заголовка
Класс 1	CS4
Класс 2	AF21
Класс 3	Default (любые значения, отличные от классов 1 и 2)

Примечания:

- При передаче данных через IP/MPLS сеть Исполнителя заголовки IP-пакетов меняться не должны;
- При превышении трафиком Класса 1 пропускной способности, установленной на порту для Класса 1, должен производиться сброс IP-пакетов с качеством Класса 3; при превышении трафиком Класса 2, пропускной способности, установленной на порту для Класса 2, – сброс IP-пакетов с качеством Класса 3; при превышении трафиком Класса 3 пропускной способности порта – сброс IP-пакетов.

5.3.2.4. Требования к качеству Элемента ПД в ВЧС.

1) При оказании Элемента ПД в ВЧС Исполнитель должен осуществлять маршрутизацию IP-пакетов с данными СЗО и обеспечивать передачу IP-пакетов с данными СЗО между подключенными к сети СЗО, между СЗО и другими подключенными к ЕСПД сетями и объектами, а также между сетью Интернет;

2) При оказании Элемента ПД в ВЧС Исполнитель должен осуществлять маршрутизацию IP-пакетов с данными объектов ЦИК и обеспечивать передачу IP-пакетов с данными объектов ЦИК между подключенными к сети объектами ЦИК;

3) Пропускная способность передачи данных между любыми двумя СЗО, Объектами ЦИК по каналам через ЕСПД в зоне ответственности Исполнителя, должна определяться как наименьшее значение из пропускных способностей подключений данных объектов к ЕСПД;

4) Гарантии качества передачи IP-пакетов с данными Потребителя между любыми Точками присоединения ЕСПД должны удовлетворять следующим требованиям:

Значения параметров качества передачи данных на проводных каналах между Точками присоединения, удаленными друг от друга на расстояние по прямой на карте не более 4000 км:

Тип трафика	Процент потерянных IP-пакетов, не более	Задержка передачи IP-пакетов в одну сторону, не более	Вариация задержки, не более
Класс 1	0,2%	75 мс	50 мс
Класс 2	0,2%	100 мс	не нормируется
Класс 3	5%	125 мс	не нормируется

Значения параметров качества передачи данных на проводных каналах между Точками присоединения, удаленными друг от друга на расстояние по прямой на карте более 4000 км:

Тип трафика	Процент потерянных IP-пакетов, в не более	Задержка передачи IP-пакетов в одну сторону, не более	Вариация задержки, не более
Класс 1	0,2%	100 мс	50 мс

Класс 2	0,2%	150 мс	не нормируется
Класс 3	5%	200 мс	не нормируется

5.3.3. Элемент «Передача данных в сеть Интернет» **(далее –Элемент ПД в Интернет).**

5.3.3.1. Требования к Элементу ПД в Интернет:

1) Передача данных в сеть Интернет из ЕСПД должна осуществляться на ресурсах Исполнителя, с использованием частной адресации оборудования СЗО и использованием функции сетевой трансляции адресов (NAT);

2) Элемент ПД в Интернет должен быть централизован на уровне инфраструктуры Исполнителя в административных центрах субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя), в соответствии
с требованиями ТЗ. Элемент ПД в Интернет должен предоставляться в географических точках субъектов Российской Федерации (за исключением Республики Крым и г. Севастополя), наиболее близко расположенных к Точкам присоединения ЕСПД, из которых инициируется такой доступ;

3) Перед началом оказания ПД в Интернет для СЗО, Объектов ЦИК, указанных Заявках, Исполнителем должен предоставляться выделенный симметричный дуплексный доступ к сети Интернет с пропускной способностью, соответствующей требованиям ТЗ. При этом для СЗО, подключенных с использованием иных технологий, допускается предоставление асимметричного доступа по согласованию с Заказчиком;

4) Исполнитель для оказания ПД в Интернет должен зарезервировать достаточное количество внешних IPv4 адресов из зарегистрированного за Исполнителем в базе данных RIPE NCC пространства IPv4 адресов. Объем (количество) IPv4 адресов Исполнителя должно быть достаточным для взаимодействия пользователей ЕСПД с информационными системами, размещенными в сети Интернет, в т.ч. с системами, имеющими жесткие

ограничения по количеству сессий, устанавливаемых с одного IPv4-адреса;

5) Исполнитель должен обеспечить следующие пороговые значения параметров качества передачи данных в зоне ответственности Исполнителя по каналу связи между Точкой присоединения ЕСПД и ресурсами сети Интернет, Точкой присоединения ЕСПД для Объекта ЦИК и ресурсами сети Интернет, непосредственно подключенными к IP сети Исполнителя:

– процент потерянных пакетов – не более 5%;

– задержка передачи пакетов:

- по проводным каналам – не более 250 мс;

- на составных каналах с учетом наличия одного беспроводного участка (одного спутникового скачка) – не более 1000 мс.

5.4. Компонент «Защита данных».

5.4.1. Назначение Компонента «Защита данных».

Компонент «Защита данных» предназначен для защиты данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным, иным информационным системам, требующих защиты передачи данных, размещаемым в региональных или федеральном ЦОД Владельцев ИС.

Для достижения целей по защите данных Исполнитель должен выполнить следующие задачи:

– Заказчик согласовывает, а Исполнитель осуществляет размещение оборудования криптографической защиты информации на территории федеральных, региональных и (или) муниципальных площадках Владельцев ИС;

– разместить оборудование криптографической защиты информации ЕСПД на федеральных, региональных и муниципальных площадках Владельцев ИС и обеспечить его подключение к ЕСПД самостоятельно и за свой счет.

– организовать криптографическую защиту передаваемых данных от пользователей СЗО до федеральных, региональных или муниципальных ИС;

– организовать связность криптографических средств между собой

в заданной конфигурации.

5.4.2. Требования к архитектуре Компонента.

Архитектура Компонента «Защита данных» определяется Исполнителем.

Для СЗО Компонент должен обеспечивать защищенный доступ от СЗО до ИС, расположенных в федеральном, региональном или муниципальном ЦОД Владельцев ИС, в соответствии с требованиями ТЗ. Компонент «Защита данных» должен использовать ЕСПД в качестве транспорта для защищаемых криптографическими средствами данных.

Для Объектов ЦИК Компонента «Защита данных» используется в случае если необходимо обеспечивать защищенный доступ из Объектов ЦИК до ИС, расположенных в федеральном и региональном или муниципальном ЦОД Владельцев ИС, в соответствии с требованиями ТЗ. Компонент «Защита данных» должен использовать ЕСПД в качестве транспорта для защищаемых криптографическими средствами данных.

5.4.3. Управление Компонентом «Защита данных».

Для указанных Заказчиком СЗО, Объектов ЦИК Исполнитель должен осуществлять управление изменениями, которые могут включать изменения следующих параметров:

- интерфейса на оборудовании Исполнителя, к которому подключается оборудование СЗО, Объектов ЦИК;
- топология криптографической сети;
- IP адреса и подсети;
- протоколы маршрутизации;
- профили портов доступа;
- точки присоединения к криптографической сети;
- параметры качества передачи IP-пакетов и Ethernet кадров СЗО между СЗО;
- подключение СЗО к сети Исполнителя при изменении адреса месторасположения СЗО;
- параметры качества передачи IP-пакетов и Ethernet кадров Объектов

ЦИК между Объектами ЦИК;

- подключение Объектов ЦИК к сети Исполнителя при изменении адреса месторасположения Объектов ЦИК;
- приостановление или возобновление оказания услуги;
- оказание услуги для новых СЗО по согласованию между Заказчиком и Исполнителем;
- прекращение оказания услуги;
- иные согласованные Исполнителем и Заказчиком параметры услуги.

5.4.4. Требования к производительности Компонента Услуг «Защита данных».

5.4.4.1. Производительность Компонента «Защита данных» должна быть достаточной, для выполнения возложенных на нее задач. В случае необходимости увеличения производительности. Увеличение производительности Компонента должно достигаться следующими способами:

- замена или модернизация аппаратного обеспечения;
- замена или модернизация программного обеспечения;
- увеличение пропускной способности каналов связи, магистральных и сети доступа.

5.4.5. **Элемент «Криптографическая защита каналов связи»** (далее – Элемент «Криптозащита»).

5.4.5.1. Назначение Элемента «Криптозащита».

Элемент «Криптозащита» предназначен для обеспечения поддержки шифрования с использованием российских алгоритмов для защиты данных, передаваемых по каналам связи, не предназначенным для сети Интернет. Используемые средства криптографической защиты должны иметь сертификат соответствия требованиям ФСБ России к шифровальным (криптографическим) средствам класса не ниже КС3 и ФСТЭК России.

5.4.5.2. Требования к Элементу «Криптозащита»:

1) Элемент «Криптозащита» реализуется на основе программно-аппаратных средств;

2) Шифрование должно обеспечивать возможность подключения СЗО к ИС, требующим защиты данных, размещаемым во внешних региональных и федеральных ЦОД;

3) Шифрование реализуется на основе криптомаршрутизаторов, соответствующих требованиям ТЗ;

4) Шифрование должно обеспечивать функцию защиты трафика при передаче персональных данных;

5) Обязательно наличие действующих сертификатов соответствия требованиям ФСБ России к средствам криптографической защиты класса КС3 и ФСТЭК России;

6) Шифрование должно обеспечивать передачу требующих защиты данных Объектов ЦИК;

7) Шифрование должно обеспечивать функцию защиты трафика при передаче персональных данных, за исключением данных ГАС «Выборы».

5.4.6. Средства криптозащиты информации должны выполнять:

- шифрование данных, передаваемых по открытым каналам связи между защищенными сегментами сети L3VPN;
- скрытие внутренней структуры локальных вычислительных сетей;
- прием и передачу IP-пакетов по протоколам семейства TCP/IP;
- централизованное управление защитой сети;
- прием и передача IP-пакетов по протоколам семейства TCP/IP;
- криптографическое преобразование передаваемых и принимаемых IP-пакетов должны соответствовать требованиям: ГОСТ 34.13-2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» и ГОСТ Р 34.12-2015 "Информационная технология. Криптографическая защита информации. Блочные шифры";
- шифрование информации на сетевом уровне;
- увеличение размера пакета с учетом дополнительного IP-заголовка не должно превышать 60 байт;

- возможность мониторинга состояния криптомаршрутизатора из защищенных сетей по протоколу SNMP;
- режим работы криптомаршрутизатора – круглосуточный необслуживаемый, по схеме 24 часа в сутки, 7 дней в неделю;
- поддерживать статическую и динамическую маршрутизацию по протоколу BGPv4 (спецификация IETF RFC 1771);
- обеспечивать поддержку не менее 3 (трех) классов обслуживания трафика модели DiffServ;
- обеспечивать поддержку маркировки входящего трафика на основе IP адреса получателя;
- обеспечивать поддержку маркировки входящего трафика на основе IP адреса источника;
- обеспечивать поддержку маркировки шифрованного трафика;
- сегментирование и разграничение информационных потоков;
- Интеграция с SIEM-системами, регистрация и отправка событий информационной безопасности, регламентированных технической и нормативной документацией;
- Возможность интеграции с системами мониторинга трафика по протоколам Netflow, IPFIX.

5.4.7. Дополнительные требования к функциональности средств криптозащиты информации, установленных в центральном ЦОД Исполнителя, а также в региональных ЦОД Исполнителя для связи с СЗО, Объектами ЦИК и внешними ИС:

- возможность «горячего» резервирования (в режиме отказоустойчивого активно-пассивного кластера или с помощью протоколов сетевой доступности и виртуализации);
- возможность обеспечивать производительность шифрования не менее 2,5 Гбит/с;
- каждый объект этого типа является центральным кластером отдельной защищенной сети; центр управления данной сети будет располагаться

на площадке Исполнителя.

5.4.8. Дополнительные требования к функциональности средств криптозащиты информации, установленных в региональных ЦОД Исполнителя для связи центральным ЦОД Исполнителя:

– возможность «горячего» резервирования (в режиме отказоустойчивого активно-пассивного кластера);
– возможность обеспечивать производительность шифрования не менее 100, 200, 300, 500, 1000 Мбит/с.

5.4.9. Дополнительные требования к функциональности средств криптозащиты информации, установленных в СЗО:

– возможность «холодного» резервирования;
– возможность обеспечивать производительность шифрования не менее 50 Мбит/с, но в соответствии с пропускной способностью каналов связи, указанной в Заявке.

5.5. **Компонент «Ограничение доступа к информации»**.

5.5.1. Компонент «Ограничение доступа к информации» должен обеспечивать блокирование доступа к Интернет-ресурсам в соответствии с п.2 ст.5 Федерального закона № 436-ФЗ от 29 декабря 2010 г. «О защите детей от информации, причиняющей вред их здоровью и развитию», где определены виды информации, запрещенной для распространения среди детей, а также с использованием положений методических рекомендаций по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, утверждённых Министерством просвещения Российской Федерации 28 апреля 2014 г.

В рамках Ограничения доступа к информации должно осуществляться регулярное (не реже одного раза в день) обновление баз данных, запрещенных Интернет-ресурсов.

В рамках Ограничения доступа к информации должна быть реализована функция анализа содержимого веб страниц для определения необходимости блокировки по контенту, включая веб ресурсы использующие средства шифрования передаваемого трафика SSL/TLS.

Компонент не должен распространяться на АРМ административно-хозяйственного и педагогического состава СЗО.

5.5.2. Требования к архитектуре Компонента:

- Ограничение доступа к информации должно быть обеспечено на основе программных и аппаратных компонентов, размещенных на объектах Исполнителя.

- Предусмотреть возможность создания двух физически разделенных сегментов сети в СЗО для раздельного доступа в сеть Интернет для учащихся и педагогического, а также административно-хозяйственного состава СЗО.

5.5.3. Управление Компонентом.

Для указанных Заказчиком СЗО Исполнитель должен осуществлять управление изменениями, которые могут включать изменения следующих параметров к Компоненту:

- IP адреса и подсети;
- правила фильтрации;
- ключевые слова и словосочетания для организации правил контент фильтрации;
- списки ресурсов ограниченного доступа;
- подключение СЗО к сети Исполнителя при изменении адреса расположения СЗО;
- приостановление или возобновление оказания услуги;
- оказание услуги для новых СЗО по согласованию между Заказчиком и Исполнителем;
- подключение Объектов ЦИК к сети Исполнителя при изменении адреса расположения Объектов ЦИК;
- оказание Услуг связи для новых Объектов ЦИК по согласованию

между Заказчиком и Исполнителем;

– прекращение оказания услуги и иные согласованные Исполнителем и Заказчиком параметры Компонента.

5.5.4. Требования к дополнительным функционалу и сопряжению со смежными подсистемами и Элементами:

1) Компонент должен иметь возможность расширять функционал посредством подключения к информационным ресурсам и смежным подсистемам, без снижения уровня информационной безопасности, емкости и производительности;

2) К смежным подсистемам относятся следующие:

– дополнительные источники списков фильтрации;

– внешние ЦОД Исполнителя;

3) Данные функциональные возможности Компонента должны быть использованы для размещения ресурсов, необходимых для обеспечения Компонентов, а также для получения дополнительной информации по фильтрации.

5.5.5. Требования к производительности Компонента:

1) Производительность Компонента должна быть достаточной, для выполнения возложенных на нее задач. В случае необходимости увеличения производительности Исполнитель должен предусмотреть такую возможность без дополнительных капитальных затрат;

2) Увеличение производительности Компонента должно достигаться следующими способами:

– замена или модернизация аппаратного обеспечения;

– замена или модернизация программного обеспечения;

– увеличение пропускной способности каналов связи, магистральных и сети доступа.

5.5.6. **Элемент «Контентная фильтрация» (далее - Элемент).**

5.5.6.1. Требования к архитектуре Элемента.

Архитектура решений по контентной фильтрации в рамках ЕСПД

представлена на рисунке 5.

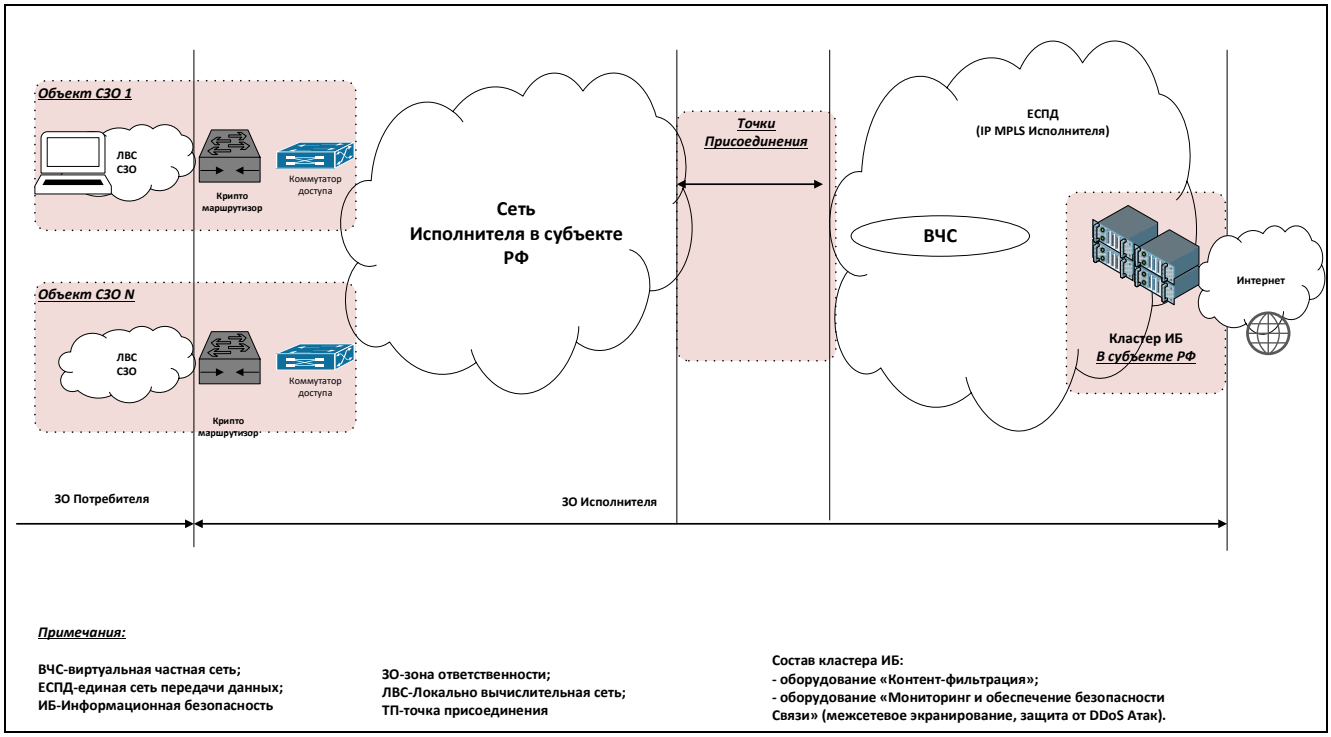

Рис. 5. Общая архитектура решений по контентной фильтрации.

Оборудование КФ должно располагаться в административных центрах субъектов РФ в соответствии с требованиями ТЗ. (за исключением Республики Крым и г. Севастополя).

Элемент Услуг связи «Контентная фильтрация» для Объектов ЦИК предоставляется только по дополнительному запросу ЦИК России.

5.5.6.2. Требования к Элементу.

Контентная фильтрация должна поддерживать следующие функции:

– контроль веб-трафика по протоколам HTTP, HTTPS;

– блокировка злонамеренных интернет-ресурсов;

– поддержка черных и белых списков интернет-ресурсов;

– блокировка вредоносного ПО и нежелательной рекламы;

– обеспечение антивирусной защиты пользователей СЗО при взаимодействии с ресурсами сети Интернет (веб антивирус), включая анализ содержимого веб-ресурсов и получаемых/передаваемых вложений;

– принудительное включение безопасного поиска для поисковых систем

Google, Yandex, Yahoo, Bing, Rambler, Ask и портала YouTube для блокировки нежелательного контента;

– журналирование поисковых запросов пользователей на срок до 6 месяцев;

– блокировка приложений популярных социальных сетей, с возможностью открытия доступа, по запросу Потребителя в соответствии с запрашиваемыми действиями для страниц каждой отдельно взятой социальной сети, при условии поддержки социальной сетью разграничения действий внутри сервиса;

– ограничение по объему использования веб-трафика;

– централизованное распространение политик безопасности на все узлы КФ;

– ведение досье на СЗО, с возможностью привязки трафика по посещаемым СЗО ресурсам/категориям ресурсов, и объему использованного интернет-трафика за период до 6 месяцев;

– добавление ресурсов в список для контентной фильтрации по запросу Заказчика;

– добавление сервисов в обход контентной фильтрации по запросу Заказчика.

Контентная фильтрация должна обеспечивать:

– гибкую фильтрацию HTTP трафика;

– фильтрацию HTTPS трафика с точностью до имени запрашиваемого ресурса на основании значения SNI;

– гибкую фильтрацию HTTPS трафика средствами анализа контента, размещенного на веб ресурсе на предмет запрещенных материалов и (или) ключевых фраз;

– гибкую фильтрацию HTTPS трафика, в случае установки на клиентские устройства сертификата Исполнителя;

– гибкую фильтрацию HTTPS трафика на мобильных устройствах, в случае установки на мобильные устройства WEB-браузера Исполнителя;

– гибкую фильтрацию HTTPS трафика на мобильных устройствах в приложениях, согласованных с Заказчиком, в рамках реализации проектов Министерства образования.

5.5.6.3. Требования к применяемым техническим решениям:

– КФ должна быть реализована с использованием программно-аппаратных комплексов;

– возможность, по запросу от Потребителя, автоматизации процессов, связанных с предоставлением услуги «Ограничение доступа к информации» посредством элемента «Контентная фильтрация».

5.5.6.4. Требования к автоматизации.

Средства контроля доступа в сеть Интернет и фильтрации трафика сети Интернет должны обеспечивать выполнение следующих функций:

– обеспечение и контроль доступа пользователей в сеть Интернет с фильтрацией входящего и исходящего Интернет-трафика по протоколам HTTP/HTTPS;

– управление доступом к сайтам сети Интернет на основе «черных» и «белых» списков, составленных с использованием категоризации сайтов. Функционал настройки фильтрации входящего и исходящего трафика должен позволять указывать в качестве фильтра маску или регулярное выражение. Списки категорий сайтов должны предоставляться производителем средств контроля доступа в сеть Интернет. Для администраторов программного обеспечения должна быть реализована функция внесения корректировок в данные списки, а также создания собственных категорий. Списки должны формироваться путем внесения не только одиночных сайтов, но и их списков (в формате текстовых файлов с разделителями);

– отключение функционала контроля доступа в сеть «Интернет» и фильтрации трафика сети Интернет для конкретных IP-адресов и конкретных пользователей, прошедших авторизацию в ЕСИА;

– управление доступом пользователей к различным типам информации

в сети Интернет (видео, аудио, изображения и т.д.);

– управление доступом пользователей к возможности передачи в сеть Интернет информации различных типов (видео, аудио, изображения и т.д.);

– уведомление в окне браузера пользователя сети Интернет о блокировании доступа к запрашиваемому пользователем web-ресурсу в случае нарушения требований информационной безопасности, а также на основании наличия потенциально опасного кода (с функцией правки кода и текста уведомления);

– автоматическое или ручное обновление программных компонентов с сайта производителя;

– управление доступом к средствам контроля доступа в сеть Интернет и фильтрации трафика сети Интернет с использованием ролевой модели;

– протоколирование действий администраторов системы;

– обеспечение отказоустойчивости программно-аппаратных компонентов системы.

Не позднее **60** календарных дней с даты заключения Контракта Исполнитель в Личном кабинете, созданном в соответствии с п. 2.49.2 ТЗ, обеспечивает выполнение следующих функций:

– возможность доступа к Личному кабинету путем авторизации с использованием ЕСИА работников СЗО, а также федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, осуществляющих функции в сфере общего образования и среднего профессионального образования;

– возможность подачи заявок на включение (блокировку) ресурсов сети Интернет в Белый список, Временный белый список, Черный список;

– возможность отслеживания статусов выполнения поданных заявок;

– возможность оценки качества исполнения поданных заявок;

– возможность формирования отчетности для контроля перечня ресурсов сети Интернет, включенных в Белый список, Временный белый список, Черный список;

– возможность быстрой проверки текущего статуса доступности в ЕСПД ресурса сети Интернет.

5.6. **Компонент «Мониторинг и обеспечение безопасности связи».**

5.6.1. Элемент «Мониторинг параметров качества предоставляемых услуг».

5.6.1.1. Требования к функционалу средств мониторинга и отчетности.

Средства мониторинга функционирования и формирования отчетности должны обеспечивать выполнение следующих функций:

1) Объективный контроль работоспособности средств связи и соблюдение требуемого качества и доступности услуг связи, целостности и устойчивости функционирования сетей передачи данных, а также безопасности связи при подключении и предоставлении доступа для СЗО к государственным, муниципальным, иным информационным системам и сети Интернет с возможностью формирования Инцидентов в автоматизированном режиме посредством использования программно-аппаратного комплекса;

2) Протоколирование действий пользователей и администраторов системы;

3) Формирование отчетности с предоставлением функционала:

– отображение информации о состоянии объектов в режиме реального времени в цвето-графическом виде;
– задания фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности;
– задания формата отчетов;

4) Компонент должен обеспечивать сбор и формирование данных по утилизации трафика в разрезе пиковых значений, среднего входящего /исходящего, а также среднее по объему входящего/исходящего потребления данных (в Мбайт) по каждому Объекту (протокол snmp) с глубиной хранения данных 12 месяцев;

5) Компонент должен обеспечивать сбор и формирование данных по недоступности Услуг связи по причинам, находящимся в зоне ответственности Потребителя (электропитание в момент возникновения события, функция Dying

gasp), а также по причинам в зоне ответственности Исполнителя (ППР, проблемы с канальной, сетевой частью как на объекте, так и на магистральной части) с глубиной хранения данных 12 месяцев;

6) Компонент должен обеспечивать возможность присвоения признаков «стоп-факторов» лежащих в зоне ответственности пользователя (ремонт и другие работы на продолжительный период связанные с отключением услуги, но не приводящие к исключению объекта из заявки к ГК) с глубиной хранения данных 12 месяцев;

7) Компонент должен представлять собой совокупность Элементов с возможностью их комбинации и изменений;

8) Основными принципами мониторинга и обеспечения безопасности связи должны являться универсальность, управляемость и масштабируемость;

9) Компонент должен позволять запуск дополнительных Элементов по требованию Заказчика и Потребителя без дополнительных затрат;

10) Технические программно-аппаратные средства, используемые при оказании Компонента, должны соответствовать требованиям государственной метрологической измерительной системы национального уровня, за счет выполнения следующих требований:

- использования средств измерения, внесенных в Федеральный информационный фонд по обеспечению единства измерений, а также своевременно прошедших поверку в соответствии с требованиями статьи 13 Федерального закона от 26 июня 2008 г. № 102-ФЗ «Об обеспечении единства измерений»;
- соответствия всех программно-аппаратных средства требованиям к измерениям, относящимся к сфере государственного регулирования обеспечения единства измерений и выполняемым при обеспечении целостности

и устойчивости функционирования сети связи общего пользования, а именно, в соответствии с постановлением Правительства Российской Федерации от 16 ноября 2020 г. № 1847 «Об утверждении перечня измерений, относящихся

к сфере государственного регулирования обеспечения единства измерений»;

- сертификация оборудования в соответствии с постановлением Правительства Российской Федерации от 04 февраля 2022 г. № 113 «Об утверждении перечня средств связи, подлежащих обязательной сертификации».

5.6.1.2. Требования к архитектуре Компонента.

Архитектура должна строиться на принципах модульности и масштабируемости, на программных и аппаратных компонентах.

Технические решения, применяемые в рамках оказания Компонента, должны представлять собой иерархическую систему с возможностью горизонтального и вертикального масштабирования.

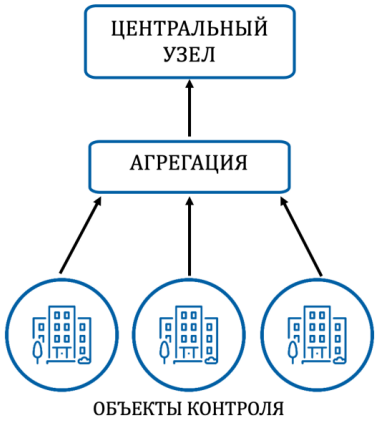

Рис. 6. Общая архитектура Компонента «Мониторинг и обеспечение безопасности связи».

Центральным узлом технических решений, применяемых в рамках оказания Компонента, должен являться отказоустойчивый кластер серверов. Уровнем агрегации должны являться зонды уровня агрегации, размещаемые в зоне ответственности Исполнителя, объектами контроля должны являться оказываемые СЗО в соответствии с Заявками услуги связи с использованием зондов, размещаемых на указанных СЗО.

Технические решения, применяемые для оказания Компонента, должны использовать только программно-аппаратные зонды для получения исходных данных о работоспособности средств связи и соблюдению требуемого качества

предоставления услуг связи. Использование иных способов получения исходных данных о работоспособности средств связи и соблюдению требуемого качества предоставления услуг связи не предусматривается.

5.6.1.3. Управление Компонентом.

Для указанных Заказчиком СЗО, Объектов ЦИК Исполнитель должен осуществлять управление изменениями, которые могут включать изменения следующих параметров оказания мониторинга и обеспечения безопасности связи:

- период опроса оборудования;
- расписание мониторинга;
- количество оцениваемых параметров качества услуги;
- параметры для оценки качества услуг;
- объем параметров оценки качества;
- IP адреса и подсети;
- профили портов доступа;
- пропускная способность передачи трафика разных типов по предоставляемым каналам связи между СЗО, Объекта ЦИК;
- IP адрес для защиты от DDoS атак;
- подключение СЗО, Объекта ЦИК к сети Исполнителя при изменении адреса их месторасположения;
- приостановление или возобновление оказания мониторинга и обеспечения безопасности связи;
- Мониторинг и обеспечение безопасности связи для новых СЗО, Объекта ЦИК по согласованию между Заказчиком и Исполнителем;
- прекращение мониторинга и обеспечения безопасности связи;
- иные согласованные Исполнителем и Заказчиком параметры мониторинга и обеспечения безопасности связи.

5.6.1.4. Требования к дополнительным функционалу и сопряжения со смежными системами и Элементами:

1) Компонент должен иметь возможность расширять функционал посредством подключения к информационных ресурсам и системам, без

снижения уровня информационной безопасности, емкости и производительности;

2) Данные функциональные возможности Компонента должны быть использованы для мониторинга параметров качества предоставляемых услуг.

5.6.1.5. Требования к производительности Компонента:

1) Производительность Компонента должна быть достаточной, для выполнения возложенных на нее задач. В случае необходимости увеличения производительности Исполнитель должен предусмотреть такую возможность;

2) Увеличение производительности Компонента должно достигаться следующими способами:

– замена или модернизация аппаратного обеспечения;

– замена или модернизация программного обеспечения;

– увеличение пропускной способности каналов связи, магистральных и сети доступа.

5.6.1.6. Требования к наличию отчетов.

Компонент должен обеспечивать по каждому СЗО, в соответствии с Заявками, формирование в электронном виде (за исключением случаев содержания в отчетах сведений, составляющих государственную тайну, или сведений ограниченного доступа («Для служебного пользования»)) по запросу уполномоченного представителя Заказчика и в автоматическом режиме предопределенной (регламентированной) статистической и аналитической отчетности о качестве услуг связи:

— формирование периодических статистических и аналитических отчетов о качестве услуг связи по предоставленным Заказчиком предопределенным формам и их автоматизированную рассылку средствами электронной почты (за исключением случаев содержания в отчетах сведений, составляющих государственную тайну, или сведений ограниченного доступа («Для служебного пользования»)) уполномоченным представителям Заказчика;

— формирование в электронном виде (за исключением случаев

содержания в отчетах сведений, составляющих государственную тайну, или сведений ограниченного доступа («Для служебного пользования»)) оперативных отчетов за произвольный период времени о качестве конкретной услуги связи для конкретного СЗО при самостоятельном обращении Заказчика к Компоненте;

5.6.2. **Элемент «Защита от DDoS атак»** (далее – Элемент).

5.6.2.1. Назначение Элемента.

Элемент предназначен для обеспечения защиты от распределенных атак типа «отказ в обслуживании». В составе Элемента «Защита от DDoS атак» Исполнитель должен оказывать телематические услуги связи.

5.6.2.2. Требования к Элементу:

1) элемент должен предоставляться для всех IP сетей СЗО, Объектов ЦИК которые используются оконечными пользовательскими устройствами Потребителей;

2) должен проводиться анализ-трафика следующих видов:

– статический – на основании сравнений фактических параметров Интернет-трафика с соответствующими значениями индивидуально установленных граничных значений;

– динамический – выявление отклонений реального объема всего Интернет-трафика пользователей (PPS и BPS) от статистически обычных значений;

3) должен проводиться анализ Интернет-трафика с учетом следующих признаков Интернет-трафика:

– диапазон IP-адресов отправителя/получателя Интернет-трафика;

– диапазон адресов портов TCP/UDP отправителя/получателя Интернет-трафика;

– наименования и параметры протоколов IP, DNS, TCP, UDP, ICMP, AH, GRE, ESP (например, значения TCP-флагов для протокола TCP/IP);

4) должен проводиться анализ Интернет-трафика по следующим параметрам:

– характеристики Интернет-трафика (распределение по протоколам);

– количество пакетов Интернет-трафика в секунду (PPS);

– количество байт Интернет-трафика в секунду (BPS).

5) необходимо оповещать Потребителя о наличии нежелательного Интернет-трафика при его появлении из сети Потребителя;

6) В течение 30 минут после обнаружения аномалий необходимо направлять Интернет-трафик Потребителя на программно-аппаратный комплекс Исполнителя, выполняющий с помощью вероятностных методов очистку поступающего на него Интернет-трафика в целях фильтрации нежелательного Интернет-трафика.

5.6.2.3. Исполнитель должен обеспечивать защиту от DoS/DDoS-атак на оборудовании Исполнителя.

1) Защита от DoS/DDoS атак средствами Исполнителя должна обеспечиваться от следующих типов атак:

– атаки на переполнение каналов связи (Volumetric Attacks);

– атаки на сетевую инфраструктуру (State Exhaustion Attacks);

– атаки уровня приложений (Application Attacks).

2) Фильтрация трафика должна осуществляться по следующим критериям:

– по географическому признаку;

– по «черным» и «белым» спискам IP адресов;

– протоколам;

– портам;

– с помощью регулярных выражений основных характеристик протоколов;

– с помощью регулярных выражений различных характеристик приложений;

– с применением challenge/response контрмер, для удостоверения хостов источника;

– с отслеживанием соединений на наличие медленных атак.

3) Оборудование Исполнителя, обеспечивающее защиту от DoS/DDoS, должно иметь техническую возможность:

– подавлять атаки до уровня приложения семиуровневой модели OSI емкостью не менее 150 Гбит/сек;

– подавлять атаки до транспортного уровня семиуровневой модели OSI до 2 Тбит/с;

– при необходимости и возможности взаимодействовать с системой защиты от DoS/DDoS Потребителя в целях обработки автоматических запросов активации дополнительной очистки трафика и подавления атак;

– в автоматическом режиме загружать и применять «белые» и «черные» списки IP адресов сети «Интернет» для точек подключения Потребителя, в которых оказывается услуга по защите от DoS/DDoS.

4) Решение защиты от DoS/DDoS должно поддерживать включение режима очистки трафика перечисленными ниже способами:

– в автоматическом режиме при получении сведений от оборудования площадки Потребителя, где оказывается Услуга связи;

– в автоматическом режиме при обнаружении оборудованием Исполнителя аномалии в трафике Потребителя;

– вручную, путем обращения Потребителем в службу технической поддержки Участника;

– вручную Исполнителем при обнаружении оборудованием Исполнителя аномалии в трафике Потребителя.

5.6.3. **Элемент «Межсетевое экранирование»** (далее – Элемент).

5.6.3.1. Назначение Элемента.

Элемент предназначен для обеспечения информационной безопасности при доступе в сеть Интернет, а также при обмене трафиком между ЕСПД и подключаемыми к ЕСПД Каналами L2, для предотвращения несанкционированного доступа к внутренним сегментам ЕСПД и попыток взлома.

Элемент предназначен для обеспечения информационной безопасности при доступе в сеть Интернет, а также при обмене трафиком между ЕСПД

и Объектами ЦИК, для предотвращения несанкционированного доступа к внутренним сегментам ЕСПД и попыток взлома.

5.6.3.2. Требования к Элементу:

1) Элемент должен обеспечивать:

– разграничение информационных потоков, сетевого взаимодействия между сегментами;

– блокировку запрещенных типов взаимодействий;

– журналирование или подсчет числа попыток осуществления запрещенных взаимодействий;

– блокировку обращений к известным серверам злоумышленников;

– поддержку функции выявления вредоносного трафика на основании сигнатур;

– возможность создания отказоустойчивого кластера (типов active-passive или active-active);

2) Межсетевые экраны должны обеспечивать защиту от несанкционированного доступа из сети Интернет или внешней сети по отношению к ЕСПД, а также контроль и регулировку доступа пользователей внутренней сети к ресурсам сети Интернет и выделенным сегментам инфраструктуры Потребителя. Межсетевой экран должен обеспечивать контроль всего проходящего трафика и быть устойчивым к воздействию внешних атак;

3) При выборе МСЭ определенного класса защиты для обеспечения безопасности в информационных системах соответствующего класса защищенности необходимо руководствоваться нормативными правовыми актами ФСТЭК России;

4) Выбор сертифицированных на соответствие требованиям по безопасности информации МСЭ, должен производиться с учетом совместимости с информационными технологиями и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы;

5) Для обеспечения необходимого уровня информационной

безопасности необходимо применять в качестве ключевой настройки межсетевого экрана принцип «запрещено все». Открываться на МСЭ должны только те услуги, хосты, сети и протоколы, которые нужны для обеспечения работы систем Потребителя. Все неиспользуемые адреса, сети, протоколы и услуги на МСЭ должны быть запрещены;

6) МСЭ должен содержать средства, обеспечивающие контроль за целостностью своей программной и информационной части. Межсетевой экран должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которая должна обеспечивать восстановление свойств межсетевого экрана. В межсетевом экране должна обеспечиваться возможность регламентного тестирования;

7) В журналах или log-файлах в обязательном порядке должны регистрироваться все события о соединениях, устанавливаемых через МСЭ и храниться Исполнителем в течение 12 месяцев;

8) При возможности должна быть обеспечена автоматическая регистрация следующих событий информационной безопасности:

– любые попытки входа/выхода субъектов доступа в систему/из системы;
– изменение прав и системных привилегий учетных записей пользователей;
– изменение настроек МСЭ;

9) Защита на основе МСЭ должна реализовывать следующие возможности:

– фильтрация на основе сетевых адресов отправителя получателя;
– локальная сигнализация попыток нарушения правил фильтрации;

10) МСЭ должен быть использован для:

– ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети Интернет;
– ограничения доступа внешних пользователей к внутренним ресурсам корпоративной сети;
– поддержки преобразования сетевых адресов (NAT), что позволяет

использование во внутренней сети приватных IP адресов;

11) Для обеспечения информационной безопасности при обмене информацией между внутренними подсетями ЕСПД должны устанавливаться МСЭ на стыке узлов сети, создавая при этом дополнительные точки контроля доступа, которые должны обеспечивать ограничение способов взаимодействия между сегментами сети.

5.7. **Компонент «Организация канала L2»**.

5.7.1. Назначение Компонента.

Компонент Услуг связи должен обеспечивать организацию канала связи от СЗО, Объектов ЦИК к Точкам присоединения ЕСПД по сети MPLS Исполнителя.

5.7.2. Требования к Компоненту:

1) Организованные каналы связи должны представлять собой выделенную сеть, построенную на оборудовании Исполнителя**;**

2) Организованные каналы связи должны быть созданы с использованием технологий:

- ВОЛС;
- спутниковый канал связи;
- иные технологии, обеспечивающие наибольшую гарантированную скорость подключения.

Приоритетной технологией подключения объектов является ВОЛС.

Подключение объектов по спутниковой технологии или иным технологиям, отличным от ВОЛС, должно быть согласовано Исполнителем с Заказчиком;

3) Организованные каналы связи начинаются на оборудовании Исполнителя в СЗО, Объектах ЦИК и заканчиваются в Точке присоединения ЕСПД;

4) Организованные каналы могут быть частично организованы через сети третьих операторов, при этом точки сопряжения сетей Исполнителя и третьих операторов могут не совпадать с Точками присоединения ЕСПД;

5) Организованные каналы связи могут быть предоставлены в виде:

a. выделенных каналов для одного СЗО, Объекта ЦИК;

b. ВЧС объединяющих несколько СЗО, Объектов ЦИК. В рамках таких ВЧС должно быть исключено взаимодействие СЗО, Объектов ЦИК, минуя ЕСПД;

6) Организованные каналы связи (ВЧС) могут быть реализованы на втором или третьем уровне сетевой модели OSI при условии соблюдения всех прочих требований настоящего ТЗ;

7) Организованные для доступа к ЕСПД каналы не предназначены для передачи видео-трафика;

8) Надежность организованных каналов связи не должна быть ниже доступности услуги ЕСПД в целом, определенной ТЗ;

9) Организованные с использованием ВОЛС каналы должны обеспечивать прохождение пакетов размером до 1500 байт включительно (MTU) без их фрагментации;

10) Организованные каналы должны предоставлять как минимум 3 класса качества обслуживания трафика. По согласованию с Заказчиком допускается использование моделей качества обслуживания с большим или меньшим количеством классов.

5.7.3. Требования к пропускной способности.

Организованные каналы должны обеспечивать следующую скорость передачи данных, в соответствии с Заявками:

Для СЗО:

	Скорость доступа
Для образовательных организаций, находящихся в городских поселениях	Не менее 100 Мбит/с
Для образовательных организаций, находящихся в сельских поселениях	Не менее 50 Мбит/с
Для образовательных организаций, подключаемых с использованием иных линий связи (в том числе спутниковых) в случае невозможности использования ВОЛС	Не менее 1 Мбит/с

Для Объектов ЦИК:

	Скорость доступа к сети	
	Интернет	ГАС «Выборы»
Для Центральной избирательной комиссии Российской Федерации	-	40 Гб/с
Для Избирательных комиссий субъектов Российской Федерации	100 Мбит/с	40 Мбит/с
Для Территориальных избирательных комиссии	50 Мбит/с	10 Мбит/с
Для объектов ЦИК, расположенных в труднодоступных населенных пунктах и подключенных по спутниковым каналам связи	512 кбит/с	512 кбит/с

5.8. **Компонент «Передача данных L2»**.

5.8.1. Назначение Компонента.

Компонент должен обеспечивать передачу данных от СЗО, Объектов ЦИК к Точкам присоединения ЕСПД.

5.8.2. Требования к пропускной способности.

Организованные каналы должны обеспечивать следующую скорость передачи данных, в соответствии с Заявками:

Для СЗО

	Скорость доступа
Для образовательных организаций, находящихся в городских поселениях	Не менее 100 Мбит/с
Для образовательных организаций, находящихся в сельских поселениях	Не менее 50 Мбит/с
Для образовательных организаций, подключаемых с использованием иных линий связи (в том числе спутниковых) в случае невозможности использования ВОЛС	Не менее 1 Мбит/с

Для Объектов ЦИК:

	Скорость доступа к сети	
	Интернет	ГАС «Выборы»
Для Центральной избирательной комиссии Российской Федерации	-	40 Гб/с
Для Избирательных комиссий субъектов Российской Федерации	100 Мбит/с	40 Мбит/с
Для Территориальных избирательных комиссии	50 Мбит/с	10 Мбит/с
Для объектов ЦИК, расположенных в труднодоступных населенных пунктах и подключенных по спутниковым каналам связи	512 кбит/с	512 кбит/с

5.8.3. Требования к качеству обслуживания.

В рамках модели с 3 классами обслуживания при передаче трафика между СЗО и узлом Исполнителя должна поддерживать:

– Класс 1 – трафик приложений реального времени (голос, видео), критичный к потерям пакетов, задержкам и колебаниям задержки;
– Класс 2 – трафик корпоративных информационных систем, критичный к задержкам и потерям;
– Класс 3 – трафик, некритичный к задержкам (Интернет, различные сетевые службы).

Классификация трафика должна осуществляться для каждого L2-пакета в отдельности, в соответствии со значением его заголовков 802.1p, как указано в следующей таблице:

Тип трафика	Значение заголовка
Класс 1	5 (VO)
Класс 2	3 (CA)
Класс 3	Default (любые значения, отличные от классов 1 и 2)

Примечания:

– При передаче данных через канал связи заголовок 802.1p не должен

изменяться.

– При превышении трафиком Класса 1 пропускной способности, установленной на порту для Класса 1, должен производиться сброс пакетов с качеством Класса 3; при превышении трафиком Класса 2, пропускной способности, установленной на порту для Класса 2, – сброс пакетов с качеством Класса 3; при превышении трафиком Класса 3 пропускной способности порта – сброс пакетов.

– Параметры качества передачи L2-пакетов через канал связи должны удовлетворять следующим требованиям:

Гарантированные значения параметров качества передачи данных по каналам связи от СЗО, Объектов ЦИК к Точкам присоединения ЕСПД, организованным по ВОЛС:

Тип трафика	Процент потерянных L2-пакетов, не более	Задержка передачи L2-пакетов в одну сторону, не более	Вариация задержки, не более
Класс 1	0,2%	15 мс	10 мс
Класс 2	0,2%	20 мс	не нормируется
Класс 3	5%	25 мс	не нормируется

Среднестатистические целевые значения параметров качества передачи данных по каналам связи от СЗО, Объектов ЦИК к Точкам присоединения ЕСПД, организованным с использованием спутниковых линий связи:

Тип трафика	Процент потерянных L2-пакетов, не более	Задержка передачи L2-пакетов в одну сторону, не более	Вариация задержки, не более
Класс 1	0,5%	500 мс	50 мс
Класс 2	1%	550 мс	не нормируется
Класс 3	5%	600 мс	не нормируется

Среднестатистические целевые значения параметров качества передачи данных по каналам связи от СЗО, Объектов ЦИК к Точкам присоединения ЕСПД, организованным по Иным технологиям

Тип трафика	Процент потерянных L2-пакетов, не более	Задержка передачи L2-пакетов в одну сторону, не более	Вариация задержки, не более
Класс 1	0,5%	100 мс	50 мс
Класс 2	1%	200 мс	не нормируется
Класс 3	5%	300 мс	не нормируется

6. Порядок взаимодействия Сторон в рамках оказания Услуг связи.

6.1. Оказание Услуг связи Исполнителем осуществляется на основании заявок Заказчика по форме Заявки (Приложение № 1).

6.2. Состав заявки должен включать следующую информацию:

— Номер;

— Содержание;

— Состав компонентов;

— Параметры Услуг связи;

— Срок оказания Услуг связи;

— Стоимость согласно Ценам единиц Услуги (Приложение № 2 к государственному контракту) и объему Услуг связи;

— Адресный перечень СЗО.

6.3. Заявка формируется Заказчиком в электронной форме (за исключением случаев содержания в заявке сведений, составляющих государственную тайну, или сведений ограниченного доступа («Для служебного пользования»), которые формируются на бумажном носителе) и направляется в адрес Исполнителя. В части Компонента «Предоставление доступа» не менее чем за 15 рабочих дней, для Компонента «Организация канала L2» Заявки направляются в срок не менее

чем за 30 рабочих дней до даты начала оказания Услуг связи, установленной Заявкой.

6.4. Заявка должна быть подписана уполномоченным лицом Заказчика в электронной форме (за исключением случаев содержания в заявке сведений, составляющих государственную тайну, или сведений ограниченного доступа («Для служебного пользования»), которые направляются согласно установленного порядка для таких документов) и направлена в адрес Исполнителя официальным письмом.

6.5. Исполнитель в срок не позднее 5 рабочих дней с даты получения Заявки официальным письмом за подписью уполномоченного лица информирует Заказчика о принятии Заявки в работу и начале ее исполнения.

6.6. Исполнитель по итогам проработки возможности оказания услуги по Компоненту «Организация канала L2» в соответствии с Заявкой в срок не позднее 15 рабочих дней с даты получения Заявки вправе направить Заказчику уведомление о невозможности подключения объекта с требуемыми параметрами и необходимости внесения изменений в Заявку в случае, если оказание данной Услуги связи возможно по иной технологии, отличной от указанной в Заявке.

6.7. Заказчик имеет право до формирования Заявки направить в адрес Исполнителя запрос на определение технической возможности и технологии подключения объектов. Исполнитель обязан предоставить ответ Заказчику на запрос в течение 30 календарных дней.

6.8. Исполнитель обязан уведомить Заказчика о необходимости внесения изменений в Заявку в следующих случаях:

– если наименования и (или) адреса СЗО и Объектов ЦИК, указанные в адресном перечне к Заявке не соответствуют фактическим;

– если СЗО и (или) Объект ЦИК прекратили/приостановили свою деятельность;

– при перемещении СЗО и (или) Объекта ЦИК на новый адрес размещения организации в пределах населенного пункта.

6.9. При необходимости внесения изменений в Заявку Исполнитель направляет в адрес Заказчика соответствующее уведомление, подписанное уполномоченных лицом.

6.10. При переезде СЗО на новый адрес размещения, *в пределах одного населенного пункта*, оказание Услуг связи Исполнителем по Компонентам «Передача данных» и «Передача данных L2» по новому адресу осуществляется без Компонента «Организация канала L2» на основании письменного обращения Заказчика и Заявки.

6.11. При переезде СЗО на новый адрес размещения в *иной населенный пункт* оказание Услуг связи Исполнителем по Компонентам «Передача данных» и «Передача данных L2» СЗО по новому адресу осуществляется на основании письменного обращения Заказчика и Заявки без Компонента «Организация канала L2» при условии наличия ВОЛС по новому адресу размещения СЗО. При отсутствии ВОЛС по новому адресу размещения СЗО, Исполнителем подтверждается отсутствие ВОЛС в письменной форме в адрес Заказчика и оказание Услуг связи по Компонентам «Передача данных» и «Передача данных L2» осуществляется Исполнителем с Компонентом «Организация канала L2» на основании Заявки.

7. Порядок контроля, приемки и измерения качества предоставления Услуг связи.

7.1. Исполнитель предоставляет Заказчику:

7.1.1 На утверждение, не позднее **30 рабочих дней со дня подписания Контракта**:

1) План организации Точек присоединения ЕСПД по форме в соответствии с Приложением № 4 к Техническому заданию;

2) Форму отчета об использовании оборудования российского происхождения;

3) Форму отчета о присоединенных ИС;

4) Методику проведения приемо-сдаточных испытаний;

5) Регламент технической поддержки при оказании Услуги связи;

6) Форму Сводного акта о прерывании в предоставлении Услуг связи (содержащего в том числе перечень объектов, длительность перерывов в предоставлении Услуг связи);

7) Форму отчета о функционировании элемента «Защита от DDoS атак»;

8) Форму отчета о функционировании элемента «Межсетевое экранирование»;

9) Форму отчета по функционированию Компонента «Мониторинг и обеспечение безопасности связи» Элемент «Мониторинг параметров качества предоставляемых услуг»;

10) Форму отчета по исполнению Компонента «Защита данных».

7.1.2. На утверждение не позднее 30 календарных дней с даты заключения Контракта Инструкцию по работе Пользователя в Личном кабинете.

7.2. В срок до:

- **31 января 2024 года включительно** Исполнитель направляет Заказчику документы в соответствии с п. 7.11.1. ТЗ по итогам оказания в соответствии с Заявками в рамках Контракта Услуг связи СЗО, Объектам ЦИК указанным в Заявках Заказчика;

7.3. В срок, указанный в п. 7.2. ТЗ, Исполнитель предоставляет отчет об использовании телекоммуникационного оборудования при исполнении Контракта для Компонентов «Организация канала L2» и «Предоставление доступа», страной происхождения которого является Российская Федерация по форме, разработанной в соответствии с п. 7.1 и утвержденной Заказчиком.

7.4. В срок, указанный в п. 7.2. ТЗ, Исполнитель предоставляет отчет о присоединённых к ЕСПД ИС и региональных сетей передачи данных субъектов Российской Федерации, в соответствии с п. 2.32. и п. 2.33. ТЗ.

7.5. В срок, указанный в п. 7.2. ТЗ, Исполнитель предоставляет копии соглашений с оператором СКЗИ, заверенных Исполнителем, для СЗО, присоединенных к ЕСПД в соответствии с п. 2.42.2 ТЗ.

7.6. В срок, указанный в п. 7.2. ТЗ, в рамках Компонента «Мониторинг и обеспечение безопасности связи» Исполнитель предоставляет:

— Копию Свидетельства об утверждении типа средств измерений или регистрационный номер средства измерений в Федеральном информационном фонде по обеспечению единства измерений. Предоставляется для каждого типа средств измерений, для:

- системы в целом (технического решения);
- аппаратных средств контроля уровня агрегации;
- аппаратных средства контроля уровня СЗО;
- рабочего эталона – сервера точного времени.

— Копию действующего Свидетельства о поверке средств измерений (предоставляется для каждого средства измерений).

7.7 Для СЗО, Объектов ЦИК, которым оказываются Услуги связи, наличие доступа к информационным системам и сети Интернет на СЗО, Объектах ЦИК определяется Заказчиком посредством Компонента «Мониторинг и обеспечение безопасности связи». В срок, указанный в п. 7.2. ТЗ, Исполнитель предоставляет ежемесячные отчеты по функционированию:

1) Элемента «Мониторинг параметров качества предоставляемых услуг»;

2) Элемент «Защита от DDoS атак»;

3) Элемент «Межсетевое экранирование».

7.8. В срок, указанный в п. 7.2. ТЗ, Исполнитель предоставляет отчет по функционированию Компонента «Защита данных».

7.9. Заказчик имеет право проводить выборочную проверку оказываемых Услуг связи. Выборочная проверка проводится на СЗО, Объектах ЦИК в соответствии с Программой и методикой испытаний (Приложение № 2).

7.10. По итогам проведения испытаний в рамках выборочной проверки составляются Протокол проведения тестирования Услуги связи (далее – Протокол) (Приложение № 6) с указанием результатов испытаний по каждому параметру заказанных Компонентов. Протокол заверяется Исполнителем, уполномоченным представителем Заказчика, ответственным представителем Министерства просвещения Российской Федерации (для СЗО), представителем ЦИК (для объектов ЦИК), представителем органа государственной власти субъекта Российской Федерации и (или) представителем органа местного самоуправления, по согласованию - представителем территориального органа федерального органа исполнительной власти, осуществляющего функции по контролю в сфере связи.

7.11. На основании Протокола проведения тестирования составляется Акт проверки оказания Услуг связи (Приложение № 3), подписываемый Исполнителем, уполномоченным представителем Заказчика, ответственным представителем Министерства просвещения Российской Федерации (для СЗО), ответственным представителем ЦИК (для объектов ЦИК), представителем органа государственной власти субъекта Российской Федерации и (или) представителем органа местного самоуправления, по согласованию – представителем территориального органа федерального органа исполнительной власти, осуществляющего функции по контролю в сфере связи.

7.12. Заказчик производит приемку оказанных Услуг связи в следующей последовательности:

7.12.1. Исполнитель предоставляет Заказчику:

– Акты об оказании Услуг связи (по форме Приложения № 5 к ТЗ),

подписанные Исполнителем и уполномоченным представителем каждого СЗО, Объекта ЦИК. По письменному согласованию с Заказчиком Акты об оказании Услуг связи (по форме Приложения №5 к ТЗ) могут быть подписаны Исполнителем и третьим лицом, не являющимся руководителем СЗО или руководителем объекта ЦИК, а именно: руководителем (уполномоченным представителем) государственного органа субъекта Российской Федерации, органа местного самоуправления;

– Сводные акты о прерывании в предоставлении Услуг связи;

– Отчеты по исполнению Компонента «Мониторинг и обеспечение безопасности связи» Элемент «Мониторинг параметров качества предоставляемых услуг».

7.12.1.1. В случае если ограничивается доступ к Актам об оказании Услуг связи, они направляются Исполнителем Заказчику в соответствии с требованиями к документам, составляющим государственную тайну, или сведениям ограниченного доступа («Для служебного пользования»).

При направлении Акта об оказании услуг связи в форме электронного документа в случае, если Заявка согласно п. 6.4 ТЗ направлена в соответствии с требованиями к документам, составляющим государственную тайну, или сведениям ограниченного доступа («Для служебного пользования») в Акте об оказании Услуг связи Адрес Объекта, Широта, Долгота, Полное наименование учреждения и Точка присоединения к ЕСПД порт № не указываются. Информация о соответствии Адреса Объекта по которому фактически были оказаны Услуги связи Адресу Объекта, указанному в Заявке, отражается в Графе № 5 Акта об оказании Услуг связи. В случае несоответствия Адреса Объекта, по которому фактически были оказаны Услуги связи, Адресу Объекта, указанному в Заявке, Исполнитель в дополнение к Акту об оказании Услуг связи в срок не позднее 3 рабочих дней после подписания Акта об оказании Услуг связи обязан направить Заказчику информацию о фактическом Адресе Объекта, по которому были оказаны Услуги связи, оформленную в соответствии с требованиями к документам, составляющим государственную тайну, или сведениям

ограниченного доступа («Для служебного пользования»).

7.12.2. Контроль оказания Услуг связи осуществляется Заказчиком на основании отчетов Службы технической поддержки Заказчика и отчетов Компонента «Мониторинг и обеспечение безопасности связи» Элемент «Мониторинг параметров качества предоставляемых услуг».

7.12.3. Документ о приемке подписывается Исполнителем и Заказчиком на основании предоставленных Исполнителем Актов об оказании Услуг связи, отчетов Службы технической поддержки Заказчика и Сводных Актов о прерываниях в предоставлении Услуг связи и Отчетов по исполнению Компонента «Мониторинг и обеспечение безопасности связи» Элемент «Мониторинг параметров качества предоставляемых услуг».

7.12.4. Оплата Услуг связи осуществляется за фактически оказанные Услуги связи в соответствии с Заявками и Ценами единиц Услуги (Приложение № 2 к государственному контракту). При этом расчет стоимости фактически оказанных Услуги связи по компонентам «Передача данных» и Услуги связи «Передача данных L2» (далее – Услуги) осуществляется согласно Ценам единиц Услуги (Приложение № 2 к государственному контракту), предусматривающим абонентскую систему оплаты из расчета за 1 календарный месяц. В случае, если Услуги связи фактически оказывались не полный календарный месяц, стоимость Услуг связи подлежит перерасчету по следующей формуле:

С = Т-((Т/Дм) х Дн), где:

С – стоимость Услуги связи в рассчитываемом месяце;

Т – Цена единицы Услуги связи;

Дм – количество дней в месяце, за который производится расчет;

Дн – количество дней, когда Услуги связи не оказывались.

В случае, если коэффициент доступности Услуг связи в отношении конкретного СЗО или объекта ЦИК (**Кд сзо** за календарный месяц составил менее 0,98, Услуги связи для такого СЗО или объекта ЦИК за данный календарный месяц не подлежат оплате.

7.13. Исполнение обязательств по оказанию Услуг связи считается ненадлежащим в следующих случаях:

7.13.1. Исполнитель должен обеспечивать Коэффициент доступности Услуг **Кд общий** не менее 0,98 от общего количества предоставляемых по Контракту, в каждый календарный месяц.

7.13.1.1. Коэффициент доступности Услуг **Кд общий** менее 0,98 считается ненадлежащим оказанием Услуг связи и с Исполнителя в соответствии с условиями Контракта взимается штраф в размере, предусмотренном п. 6.3 ГК.

7.13.1.2. Для расчета коэффициента доступности Услуг связи **Кд общий** используется следующая формула:

$$\text{Кд общий} = (\sum_{n=1}^{M}(\text{Кд}_n))/M$$

где:

Кд – коэффициент доступности Услуги связи по каждому СЗО или объекту ЦИК за календарный месяц, рассчитываемый по формуле:

$$\text{Кд} = \frac{(24\ \text{часа x Д1}) - \text{В1} - \text{В2}}{24\text{xД1} - \text{В1}}$$

Д1 – количество календарных дней оказания Услуг связи в месяце;

М – Количество объектов, которым оказываются Услуги связи в расчетном календарном месяце в соответствие с ГК

В1 – общее фактическое время технологических перерывов за календарный месяц в часах, вызванных:

- проведением плановых профилактических работ.

Исполнитель проводит технологические перерывы в порядке, предусмотренном Регламентом технической поддержки при оказании Услуг связи, разработанным в соответствии с пунктом 7.1 ТЗ и утвержденным Заказчиком. Суммарное время технологических перерывов в СЗО, Объекте ЦИК не должно превышать для любой Услуги связи 6 (шесть) часов в течение

календарного месяца.

B2 – общее фактическое время перерыва в предоставлении Услуг связи в календарном месяце в рабочих часах, которое равняется времени недоступности Услуг связи без учета:

- технологических перерывов;
- работ на оборудовании Исполнителя, выполняемыми по запросу Заказчика;
- неисправностей оборудования Потребителя;
-действий Потребителей, вызванных в том числе отключением электропитания оборудования Исполнителя.

Порядок открытия и закрытия инцидентов для подсчета времени недоступности Услуг связи определяется в соответствии с Регламентом технической поддержки при оказании Услуг связи, разработанным в соответствии с пунктом 7.1. ТЗ и утвержденным Заказчиком. В случае, если в течение одного календарного месяца открыто инцидентов в зоне ответственности Исполнителя с превышением времени решения инцидентов в количестве 3 (трех) и более процентов общего количества предоставляемых по Контракту Услуг связи, обязательства Исполнителя считаются ненадлежаще исполненными и с Исполнителя в соответствии с условиями Контракта взимается штраф в размере, предусмотренном п. 6.3 ГК.

7.13.2. В случае единовременного (в течение одних календарных суток) отказа 8 (восьми) и более процентов Услуг связи обязательства Исполнителя считаются ненадлежащее исполненными и с Исполнителя в соответствии с условиями Контракта взимается штраф в размере, предусмотренном п. 6.3 ГК. Процент Услуг связи рассчитывается как величина отношения стоимости Услуг связи, оказываемых с отклонением от заданных параметров Услуг связи, к стоимости Услуг связи, заказанных по состоянию на дату, в которую был зафиксирован соответствующий отказ Услуг связи.

7.13.3. В случае, если в течение одного месяца более 20% от общего количества предоставляемых по Контракту Услуг связи имеют Коэффициент

доступности менее 0,98, то Услуги связи для общего количества предоставляемых по Контракту Услуг связи в данном календарном месяце считаются не оказанными и не подлежат оплате, при этом в соответствии с условиями Контракта взимается штраф в размере, предусмотренном п. 6.3 ГК.

Приложения:

1. Заявка на оказание Услуг связи (Форма);
2. Программа и методика испытаний;
3. Акт проверки оказания Услуг связи (Форма)
4. План организации Точек присоединения (Форма);
5. Акт об оказании Услуг связи за период с «___» ____202_ г. по «___» _____202_ г. (Форма);
6. Протокол проведения тестирования Услуг связи (Форма);
7. Технические требования на оказание Услуг территориальным избирательным комиссиям и избирательным комиссиям субъектов Российской Федерации для обеспечения функционирования ГАС «Выборы».

от Заказчика:	**от Исполнителя:**
Заместитель Министра цифрового развития, связи и массовых коммуникаций Российской Федерации	**Старший Вице-Президент по работе с корпоративным и государственным сегментами ПАО «Ростелеком»**
_____ / Д.М.Ким /	_____/ В.В.Ермаков /