Приложение № 1 к Контракту
от «2» ноября 2021 года
№ 0410119

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на оказание услуг государственным и муниципальным образовательным организациям, реализующим образовательные программы общего и среднего профессионального образования по предоставлению с использованием единой сети передачи данных доступа к государственным, муниципальным и иным информационным системам, а также к информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»); по передаче данных при осуществлении доступа к государственным, муниципальным и иным информационным системам, а также к сети «Интернет»; по защите данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным и иным информационным системам, а также к сети «Интернет»; по обеспечению ограничения доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, наносящей вред здоровью и развитию детей, содержащейся в сети «Интернет»; по мониторингу и обеспечению безопасности связи при предоставлении доступа к государственным, муниципальным и иным информационным системам, а также к сети «Интернет»

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 Потребителя услуг, установленное на объекте Потребителя услуг и используемое для маршрутизации трафика из сети Потребителя услуг 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 Потребителя услуг
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

Термин	Определение
MPLS сеть Исполнителя	Построенная по технологии MPLS сетевая инфраструктура Исполнителя и привлекаемых Исполнителем субподрядчиков (соисполнителей), включающая опорные маршрутизаторы (P), граничные маршрутизаторы (PE), соединяющие их магистральные каналы и иные средства связи
RIPE NCC	Региональный Европейский Регистратор Интернет адресов
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
Оператор связи/ОС	Оператор связи, оказывающий услуги по подключению к сети передачи данных, обеспечивающей доступ к единой сети передачи данных, и по передаче данных при осуществлении доступа к этой сети государственным и муниципальным образовательным организациям, реализующим образовательные программы общего и среднего профессионального образования, приведенным в Приложении №1.
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

Термин	Определение
Внешние IPv4 адреса	Внешние (публичные) IP адреса из зарегистрированного в базе данных RIPE NCC IP адресов 4 версии протокола IP
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 Потребителя услуг, построенная на базе MPLS сети Исполнителя и привлекаемых Исполнителем субподрядчиков (соисполнителей), путем организации виртуальных каналов между портами на узлах доступа сети Исполнителя, к которым подключены объекты Потребителя услуг, 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).
ЕСПД	Виртуальная частная сеть (сети) оператора единой сети передачи данных, обеспечивающая доступ социально-значимых объектов к информационным системам и к сети 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, развернутая в соответствии с проектом, согласованным в части Модели угроз и нарушителя с федеральными органами, уполномоченными в области безопасности и защиты информации
Задержка	one-way delay, время прохождения IP-пакетов по участку измерения в одну сторону (от передающей стороны к приемной). Определяется согласованными с Потребителем услуг методами и при необходимости рассчитывается как половина временного интервала

Термин	Определение
	между моментом отправления сообщения «запрос эхо» передающей стороной и моментом получения сообщения «отклик эхо» от приемной стороны (PING протокола ICMP).
ИС	Государственная, региональная, муниципальная и иная информационная система, к которой предоставляется доступ с использованием единой сети передачи данных Исполнителя.
Исполнитель/Оператор ЕСПД	Оператор связи, на которого возложена обязанность по оказанию услуг единой сети передачи данных и с которым заключен Государственный контракт
Класс трафика	Набор требований к эксплуатационным параметрам, соблюдаемым Исполнителем при передаче по сети применительно ко всем IP-пакетам, принадлежащим данному типу
Компоненты услуг	Составляющая Услуг, определяющая одну из основных потребностей, удовлетворяемых с помощью оказываемых Услуг
Контентная фильтрация	Действие Исполнителя по блокировке доступа Потребителей услуги к различным категориям Интернет-ресурсов, компонентов Услуг
КСА	Комплекс средств автоматизации
Коэффициент потери пакетов	Максимальная потеря пакетов – отношение общего количества недоставленных пакетов к общему количеству переданных пакетов, выражаемая в процентах потерянных пакетов
КФ	Контентная фильтрация
Локальная сеть передачи данных	Сеть передачи данных ОС, с использованием которой обеспечивается присоединение и доступ социально значимых объектов к единой сети передачи данных в Точке присоединения ЕСПД и передача данных при осуществлении доступа к этой сети
МСЭ	Межсетевое экранирование
Нежелательный Интернет-трафик	Интернет-трафик, поступающий на оборудование Потребителя услуг, наличие которого может быть обусловлено наличием DDoS-атаки, либо другими нежелательными для Потребителя услуг факторами

Термин	Определение
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
Объект Потребителя услуг	Объект, расположенный на обособленной площадке Потребителя услуг в соответствии с перечнем, приведенном в Приложение №1.
Оператор СКПУС	Организация, на которую возложена обязанность по контролю параметров качества предоставляемых Услуг. Определяется Заказчиком.
Отчетный период	Период времени оказания Услуг, по окончании которого производится сдача-приемка Услуг и их оплата
Оператор СКЗИ	Оператор связи, оказывающий услугу по компоненту «Защита данных» на участке от СЗО до точки присоединения к ЕСПД на момент исполнения Контракта
Пакет	Форматированный блок информации, передаваемый по сети связи, функционирующей посредством технологии коммутации пакетов
ПД	Передача данных
Потребитель	Получатель Услуг или ее компонентов, расположенный на объектах образовательных организаций, лицо со стороны образовательных организаций, осуществляющее доступ в сеть Интернет и/или к информационным системам
Порт	Логический интерфейс ВЧС Потребителя услуг на узлах доступа сети Исполнителя
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.
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,

Термин	Определение
	к количеству отправленных в конечную точку IP-пакетов
РОИВ	Региональный орган исполнительной власти
Сеть «Интернет»	Информационно-телекоммуникационная сеть «Интернет»
СЗО - Социально значимый объект	Образовательная организация.
СКЗИ	Средства криптографической защиты информации
СКПУС Система мониторинга	Программный или программно-аппаратный комплекс контроля качества Услуг предоставляется оператором СКПУС для установки Исполнителем. Оператор СКПУС определяется Заказчиком.
СМЭВ	Система межведомственного электронного взаимодействия
СОРМ	Системы технических средств для обеспечения функций оперативно-розыскных мероприятий
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 физическое подключение к средствам связи сетей электросвязи ОС и обеспечивается возможность пропуска трафика между этими сетями
Трафик	Совокупность IP-пакетов, переданных по сети передачи данных
Услуги ОС	Услуги, оказываемые оператором связи, по подключению к сети передачи данных, обеспечивающей доступ к единой сети передачи данных, и по передаче данных при осуществлении доступа к этой сети государственным и муниципальным образовательным организациям, реализующим образовательные программы общего и среднего профессионального образования, приведенным в Приложении №1
Услуги	Оказание оператором ЕСПД услуги по передаче данных при осуществлении доступа СЗО к ИС и сети Интернет с использованием ЕСПД (далее – Услуги по передаче

Термин	Определение
	данных) и обеспечивающей: 1. предоставление осуществляемого с использованием ЕСПД доступа СЗО к ИС и к сети «Интернет» (далее – Компонент Услуг «Предоставление доступа»); 2. передачу данных при осуществлении доступа СЗО к ИС и сети «Интернет» с использованием ЕСПД (далее – Компонент Услуг «Передача данных») 3. защиту данных, обрабатываемых и передаваемых при осуществлении доступа СЗО к ИС и сети «Интернет», (далее – Компонент Услуг «Защита данных»); 4. ограничение доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, наносящий вред здоровью и развитию детей, содержащейся в сети «Интернет» (далее – Компонент Услуг «Ограничение доступа к информации»); 5. мониторинг и безопасность связи при подключении и предоставлении доступа СЗО к ИС и к сети «Интернет» (далее – Компонент Услуг «Мониторинг и обеспечение безопасности связи»)
ФОИВ	Федеральный орган исполнительной власти
ФСБ	Федеральная служба безопасности Российской Федерации
ЦОД	Центр обработки и хранения данных

2. Общие сведения

2.1. Основания оказания Услуг:

2.1.1. Поручение Президента Российской Федерации от 01.06.2020 № Пр-900.

2.1.2. Перечень поручений Президента Российской Федерации от 27.02.2019 № Пр-300.

2.1.3. Распоряжение Правительства Российской Федерации от 01.09.2020 № 2219-р

2.1.4. 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 06.05.2019 № 8.

2.1.5. Положение о Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации, утвержденное постановлением Правительства Российской Федерации от 02.06.2008 № 418 «О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации».

2.1.6. Оказание Услуг должно соответствовать:

- Федеральному закону от 07.07.2003 № 126-ФЗ «О связи»;
- Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральному закону от 06 июля 2016 года № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму»;
- Федеральному закону от 26 июля 2017 года № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации";
- Федеральный закон от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в редакции Федерального закона от 01.05.2019 №93-ФЗ;
- Указу Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»;
- Правилам оказания услуг связи по передаче данных, утвержденных постановлением Правительства Российской Федерации от 23.01.2006 № 32;
- Правилам оказания телематических услуг связи, утвержденных постановлением Правительства Российской Федерации от 10.09.2007 № 575;
- Постановлению Правительства Российской Федерации от 30.12.2005

№ 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. N 538 "Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность";

- Приказу Министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 18 «Об утверждении требований к системному проекту сети связи»;

- Приказу Минкомсвязи России от 26.08.2014 № 258 (ред. от 06.02.2019) «Об утверждении Требований к порядку ввода сетей электросвязи 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. N 83 "Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий";

- Приказу Министерства связи и массовых коммуникаций РФ от 16 января 2008 г. N 6 «Об утверждении требований к сетям электросвязи для проведения оперативно-розыскных мероприятий Часть 1. Общие требования»;

- Техническим нормам в соответствии с «РД 45.129-2000. Руководящий документ отрасли. Телематические службы», утвержденным приказом Минсвязи России от 23.07.2001 № 175;

- ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и

определения»;

- ГОСТ 34.201-89 «Информационная технология. 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»;

- ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»;

- ГОСТ 34.603-92 «Информационная технология. 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»;

- ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

- ГОСТ Р 34.12-2015 " Информационная технология. Криптографическая

защита информации. Блочные шифры».

2.2. Срок оказания Услуг:

начало: с 01 декабря 2021 года;

окончание: 31 декабря 2021 года.

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

2.3. Оказание неразрывно связанных Услуг по передаче данных для СЗО, в соответствии с перечнем Приложения № 1.

Услуги включают в себя:

Компонент Услуг «Предоставление доступа»;

Компонент Услуг «Передача данных»;

Компонент Услуг «Защита данных»;

Компонент Услуг «Ограничение доступа к информации»;

Компонент Услуг «Мониторинг и обеспечение безопасности связи».

2.4. Место оказания Услуг:

Субъекты Российской Федерации, по месту нахождения Точек присоединения ЕСПД, по месту нахождения СЗО.

2.5. Исходные данные.

При оказании Услуг Исполнитель должен руководствоваться следующими исходными данными:

- настоящим ТЗ;
- перечнем Точек присоединения ЕСПД
- адресным переченем СЗО, которым оказываются Услуги (Приложение № 1)

2.6. Результаты оказания Услуг.

1) Подключение к ЕСПД СЗО в соответствии с требованиями настоящего ТЗ.

2) Оказание Услуг СЗО, указанным в Приложении № 1;

3) Осуществление передачи данных с использованием ЕСПД:

- с предоставлением осуществляемого с использованием ЕСПД доступа

СЗО к ИС и к сети Интернет;

– с осуществлением защиты данных, обрабатываемых и передаваемых при осуществлении доступа СЗО к ИС и сети Интернет;

– с обеспечением ограничения доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, наносящий вред здоровью и развитию детей, содержащейся в сети Интернет;

– с мониторингом и обеспечением безопасности связи при подключении и предоставлении доступа СЗО к ИС и сети Интернет.

2.7. 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 (пп. «б» п. 4);

– 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) (пп. «е» п. 4).

– 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 копии соответствующих лицензий в установленном законодательством Российской Федерации порядке.

2.8. Услуга должна оказываться 24 (двадцать четыре) часа в сутки 7 (семь) дней в неделю.

2.9. Услуги должны предоставляться посредством сети передачи данных Оператора ЕСПД.

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.

2.11. Для оказания Услуги СЗО в составе ЕСПД организуются каналы передачи данных и Точки присоединения ЕСПД.

2.12. Для оказания Услуг 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, а также в случае, если производитель такого телекоммуникационного оборудования не в состоянии обеспечить его наличие в достаточном количестве для начала оказания Услуг или в течении срока ее оказания, Исполнитель вправе использовать для оказания Услуг 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;

– 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, а также предоставления ответа производителя, подтверждающего невозможность такого обеспечения.

2.15. Оператор ЕСПД обеспечивает присоединение сети передачи данных ОС в Точках присоединения ЕСПД.

2.16. Требования к оборудованию Точек присоединения ЕСПД

1) Исполнитель должен обеспечить возможность установки каналообразующего оборудования ОС в Точках присоединения к ЕСПД на основании договора, заключенного между Исполнителем и ОС в соответствии с действующим законодательством Российской Федерации.
2) ОС согласовывает с Исполнителем установку необходимого оборудования на Точке присоединения. Установку необходимого оборудования ОС осуществляют своими силами и за свой счет.

3) Точкой присоединения ЕСПД является комплект оборудования Исполнителя, в состав которого входит оборудование, с сетевыми интерфейсами для подключения оборудования ОС. Количество интерфейсов для подключения оборудования ОС должно обеспечить выполнение Услуг.
4) Состав оборудования Точек присоединения ЕСПД должен быть определен Исполнителем с учетом требований ТЗ. При этом в обязательном порядке должна быть предусмотрена возможность размещения и подключения к оборудованию Точки присоединения ЕСПД оборудования СКПУС.
5) Исполнитель обеспечивает установку необходимого оборудования в Точке присоединения ЕСПД своими силами и за свой счет
6) Адреса размещения Точек присоединения ЕСПД, предоставляются Исполнителем Заказчику до 10.11.2021 на утверждение по форме в соответствии с Приложением № 4 к Техническому заданию.

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

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

2.19. Точки присоединения ЕСПД должны обеспечивать достаточное количество интерфейсов для подключения к ЕСПД сетей передачи данных ОС. Типы абонентских физических интерфейсов, которые могут использоваться при присоединении в том числе:

- 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).

2.20. Каналы связи ЕСПД между Точками присоединения ЕСПД, задействованные в предоставлении Услуг, должны использовать ВОЛС, за исключением Чукотского автономного округа.

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

2.22. Не допускается организация каналов связи, использующихся для оказания Услуг СЗО, через сеть Интернет.

2.23. 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.

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

2.25. ЕСПД должна соответствовать следующим параметрам:

– количество Точек присоединения ЕСПД не менее 85;
– в административном центре каждого субъекта Российской Федерации должно быть не менее одной Точки присоединения ЕСПД за исключением Республики Крым и г. Севастополя (для указанных субъектов Российской Федерации Точки присоединения ЕСПД организуется в г. Краснодар);
– полоса пропускания на одну точку присоединения должна обеспечивать гарантированное выполнение параметров качества передачи данных, соответствующих требованиям подключения для каждого СЗО, подключенного к ЕСПД ОС;
– коэффициент готовности сети Кг не менее 0,997 за расчетный период;
– коэффициент готовности Точки присоединения ЕСПД не менее 0,997 за расчетный период;

– процент потери IP-пакетов, задержка передачи IP-пакетов и вариация времени задержки IP-пакетов должны соответствовать п. 5.5.4. ТЗ;

– другим требованиям, изложенным в ТЗ.

2.26. Оператор ЕСПД обязан оказывать Услуги по передаче данных для СЗО без ограничения объема передачи (безлимитно).

2.27. Оператор ЕСПД самостоятельно присоединяет к ЕСПД ИС, на основании запросов от Заказчика.

2.28. Оператор ЕСПД обязан произвести присоединение ИС к ЕСПД в течении 30 (тридцати) дней с даты получения запроса от Заказчика или запросов от Владельцев ИС.

2.29. Оператор ЕСПД 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.

2.30. Оператор ЕСПД 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.

2.31. Оператор ЕСПД ведет реестр присоединенных к ЕСПД ИС в информационно-аналитическая система «Реестр услуг связи» (ИАС РУС), с указанием: названия ИС; даты присоединения ИС к ЕСПД и перечня СЗО, использующих ИС. Доступ к системе Исполнителю предоставляет Заказчик.

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

2.33. Оператор ЕСПД, для обеспечения Услуг, оказывает содействие СЗО по настройке локальных вычислительных сетей и всех АРМ, расположенных в СЗО по запросам от представителей СЗО.

2.34. Параметры ЕСПД контролируются Оператором СКПУС посредством

устанавливаемых программно-аппаратных измерительных комплексов различного типа, в соответствии с Приложением № 3 к ТЗ, в Точках присоединения ЕСПД.

2.35. Подключение сетей передачи данных ОС к Точке присоединения ЕСПД проводится в границах одного субъекта Российской Федерации за исключением Республики Крым и г. Севастополя (для указанных субъектов Российской Федерации Точки присоединения ЕСПД организуется в г. Краснодар). При отсутствии экономической и технической целесообразности подключения сети ОС к ЕСПД в границах одного субъекта Российской Федерации, подключение может быть выполнено к Точке присоединения ЕСПД соседнего субъекта Российской Федерации, при этом данное решение согласовывается Оператором ЕСПД с Заказчиком.

2.36. Подключение сетей передачи данных ОС к Точке присоединения ЕСПД проводится силами ОС.

2.37. Оператор ЕСПД доводит до ОС параметры маршрутизации трафика для организации доступа СЗО к сети ЕСПД и другие технические условия в течение 5 (пять) рабочих дней после получения запроса от ОС.

2.38. Оператор ЕСПД обеспечивается Оператором СКПУС программно-аппаратными комплексами различного типа в соответствии с запросом Оператора ЕСПД:

- для установки в Точках присоединения ЕСПД не позднее срока начала оказания Услуг.

2.39. Количество и типы программно-аппаратных комплексов определяется Оператором СКПУС в соответствии с требованиями к измерительному контуру СКПУС на основании параметров контролируемого канала связи, предоставляемых Оператором ЕСПД в запросе.

2.40. Установка измерительных зондов осуществляется силами Исполнителя в соответствии с техническими требованиями на подключение к СКПУС, представленными в Приложении № 3 к ТЗ.

2.41. Исполнитель не несет ответственности за не установку в Точках присоединения ЕСПД программно-аппаратных комплексов СКПУС в случае не

предоставления их Оператором СКПУС.

2.42. Требования к взаимодействию между Оператором ЕСПД и Оператором СКПУС, а также Оператором ЕСПД и ОС, а также Оператором ЕСПД и Представителем СЗО:

2.42.1. Оператор ЕСПД предоставляет и устанавливает для всех СЗО, присоединяемых (подключаемых) к ЕСПД, криптомаршрутизаторы страной происхождения которых является Российская Федерация и сведения о которых 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. Установка криптомаршрутизаторов осуществляется в телекоммуникационные шкафы. В случае отсутствия на объекте СЗО телекоммуникационного шкафа Исполнитель осуществляет его установку.

2.42.2. Установка криптомаршрутизатора Оператором ЕСПД 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.

2.42.3. Оператор ЕСПД в течение всего срока оказания Услуги обеспечивает за свой счет настройку, включая изменение настроек в соответствии с запросами Заказчика, техническое обслуживание и ремонт оборудования, в том числе криптомаршрутизаторов, установленных Оператором ЕСПД в СЗО, за исключением программно-аппаратных комплексов СКПУС. При этом сроки и порядок выполнения регламентных и ремонтных работ устанавливаются Регламентами взаимодействия и технической поддержки, подписываемыми между Оператором ЕСПД и Оператором СКПУС, между Оператором ЕСПД и ОС.

2.42.4. Проекты Регламентов взаимодействия и технической поддержки разрабатывает Оператор ЕСПД в срок не более 30 (тридцать) рабочих дней с даты подписания государственного контракта.

2.42.5. Регламент взаимодействия между Оператором ЕСПД и ОС

должен учитывать требования Постановления Правительства Российской Федерации от 23.01.2006 № 32 «Об утверждении правил оказания услуг связи по передачи данных» в части пп. И) п. 26 и п. 26(1).

2.42.6. Исполнитель должен обеспечить наличие электропитания для программно-аппаратных зондов, устанавливаемых в Точках присоединения ЕСПД.

2.43. Оператор ЕСПД принимает участие в работе испытательной комиссии по приемке услуги по подключению СЗО к ЕСПД.

2.44. Требования к модульности Услуги

1) Услуги доступа должны обладать модульностью.

2) Модульность должна обеспечивать возможность добавлять и комбинировать Компоненты услуг в рамках предоставления Услуг.

3) Каждый компонент должен обеспечивать выполнение своей функции.

2.45. Требования к масштабируемости Услуг

1) Исполнитель должен обеспечить техническую готовность сети передачи данных Исполнителя к оказанию Услуг СЗО в соответствии с Приложением №1.

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

3) Масштабируемость Услуг 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 и не должно оказывать влияние на Компоненты Услуг.

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

2.46. Требования к отказоустойчивости Услуг

1) Услуги должны обеспечивать отказоустойчивость в целом и отказоустойчивость Компонентов Услуг в частности. В случае возникновения

сбоев или аварий Услуг должна предоставлять возможность изменения алгоритмов работы, для обеспечения сохранения работоспособности Услуг в полном объеме.

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

- использование резервных каналов связи на магистральных линиях ЕСПД;
- использование отказоустойчивых конфигураций оборудования и программного обеспечения, по схемам N+1 или N+N;
- использование источников бесперебойного питания 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, Оператор ЕСПД обязан продолжить предоставление Услуг в течение 4 часов. Более длительные перерывы в электроснабжении, подтвержденные со стороны энергоснабжающих организаций, считаются форс-мажором.

2.46.1. Требования к отказоустойчивости компонента Услуг «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.

2.46.2. Требования к отказоустойчивости Компоненты Услуг

«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.

2.47. 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. N 6);

2) Правила оказания телематических услуг связи (утв. постановлением Правительства РФ от 10 сентября 2007 г. N 575);

3) Постановление Правительства РФ от 27 августа 2005 г. N 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. N 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. N 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. N 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 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 года № 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».

2.49. Требования к реализации взаимодействия с Центром Мониторинга и Управления сетью связи общего пользования Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее ЦМУ ССОП).

Обеспечить реализацию взаимодействия с ЦМУ ССОП в соответствии с приказами о порядке предоставления информации в ЦМУ ССОП.

2.50. Требования к системному проектированию.

Не позднее 15.11.2021, Исполнитель должен предоставить Заказчику,

актуализированный системный проект, разработанный в рамках исполнения государственного контракта 0410/75 от 29.11.2019 и в соответствии с Приказом Министерства информационных технологий и связи Российской Федерации от 13.02.2008 № 18, описывающий вопросы предоставления Услуг по предоставлению доступа и Услуг передачи данных в ЕСПД, включая:

2.50.1. 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, а также учитывается информация из Банка данных угроз безопасности ФСТЭК России (https://bdu.fstec.ru/):

- 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».

Требования к Компоненту Услуг «Защиты данных» определяются в зависимости от класса защищенности и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к Компоненту Услуг «Защиты данных» разрабатываются 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 Услуг «Защита данных»;

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

2.50.2. Реализацию СОРМ;

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

2.50.4. Обеспечение выполнения требований к ЕСПД и обеспечения присоединения к ЕСПД сетей передачи данных ОС с созданием Точек присоединения ЕСПД;

2.50.5. Обеспечение выполнения требований к оказанию Компонента услуги «Предоставление доступа»;

2.50.6. Обеспечение выполнения требований по оказанию Компонента услуги «Ограничение доступа к информации;

2.50.7. Обеспечение выполнения требований по оказанию Компонента услуги «Мониторинг параметров качества предоставляемых услуг»;

2.50.8. Общие принципы построения сетевой инфраструктуры для оказания Услуги;

2.50.9. Инженерно-технические решения по организации оказания Услуги для СЗО на базе ЕСПД;

2.50.10. Инженерно-технические решения по организации оказания Услуги для СЗО на базе спутниковой сети связи;

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

2.51. Требования к технической поддержке при оказании Услуги:

2.51.1. В период оказания Услуги Исполнитель обязан осуществлять техническую поддержку СЗО, ОС (далее - Техническая поддержка). Техническая поддержка должна основываться на обращениях представителей СЗО, ОС и на результатах работы СКПУС;

2.51.2. Техническая поддержка должна осуществляться круглосуточно и ежедневно в соответствии с Регламентом взаимодействия технических служб, разрабатываемым Исполнителем.

1) Обращения в техническую поддержку должны регистрироваться посредством следующих способов:

– по единому бесплатному контактному номеру телефона **8-800-301-32-31**;

– посредством отправки сообщений электронной почты на единый почтовый ящик **espd_ce@rt.ru**;

2.51.3. Профилактические (ремонтно-восстановительные) работы:

1) При проведении профилактических или ремонтно-восстановительных работ допускается перерыв в оказании Услуги.

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, о чем уведомляется Оператор СКПУС.

2.51.4. Приоритеты и время восстановления работоспособности Услуги 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, относящиеся к одному событию;

2-ой приоритет – Высокий:

– наблюдается массовая деградация производительности или периодическое прерывание услуги в не менее 5 процентов общего СЗО в регионе;
– фиксируются периодические прерывания в работе услуги в одном СЗО;
– нарушена СКПУС;

3-й приоритет – Средний:

– наблюдается деградация производительности услуги в одном СЗО;
– нарушение вспомогательной функциональности Услуг;
– запрос на обслуживание или изменение настроек;
– запрос на изменение конфигурации или функциональности Услуг;

4-й приоритет – Низкий:

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

Показатель	Норматив времени реакции	
	Для Точек присоединения ЕСПД, СЗО в населённых пунктах с населением более десяти тысяч человек	Для Точек присоединения ЕСПД, СЗО в административных центрах сельских поселений и прочих населенных пунктах
Режим регистрации обращений	24 часа 7 дней в неделю	24 часа 7 дней в неделю
Время решения инцидентов первого приоритета	12* часов рабочего времени (с 09:00 до 18:00 местного времени по рабочим дням) с момента регистрации обращения. В периоды проведения избирательных компаний различного уровня и периоды проведения единого	9* часов рабочего времени (с 09:00 до 18:00 местного времени по рабочим дням) с момента регистрации обращения для Точек присоединения. В период проведения избирательных компаний различного уровня и

Показатель	Норматив времени реакции	
	Для Точек присоединения ЕСПД, СЗО в населённых пунктах с населением более десяти тысяч человек	Для Точек присоединения ЕСПД, СЗО в административных центрах сельских поселений и прочих населенных пунктах
	государственного экзамена- круглосуточно	периоды проведения единого государственного экзамена - круглосуточно
		28 * часов рабочего времени (с 09:00 до 18:00 местного времени по рабочим дням) с момента регистрации обращения для СЗО. В период проведения избирательных компаний различного уровня и периоды проведения единого государственного экзамена - круглосуточно
Время решения инцидентов второго приоритета	16 * часов рабочего времени (с 09:00 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	32* часа рабочего времени (с 09:00 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	24* часа рабочего времени (с 09:00 до 18:00 местного времени по	36* часов рабочего времени (с 09:00 до 18:00 местного времени по

Показатель	Норматив времени реакции	
	Для Точек присоединения ЕСПД, СЗО в населённых пунктах с населением более десяти тысяч человек	Для Точек присоединения ЕСПД, СЗО в административных центрах сельских поселений и прочих населенных пунктах
	рабочим дням). В период проведения избирательных компаний различного уровня- круглосуточно	рабочим дням). В период проведения избирательных компаний различного уровня- круглосуточно
Время решения инцидентов четвертого приоритета	32* часа рабочего времени (с 09:00 до 18:00 местного времени по рабочим дням) В период проведения избирательных компаний различного уровня- круглосуточно	40* часов рабочего времени (с 09:00 до 18:00 местного времени по рабочим дням) В период проведения избирательных компаний различного уровня- круглосуточно

*) Указано время устранения неисправности без учета времени восстановления кабельной инфраструктуры и замены оборудования в СЗО. В случае восстановления кабельной инфраструктуры и замены оборудования на СЗО нормативные сроки решения инцидента увеличиваются на 72 часа. Указано время для восстановительных работ инфраструктуры Исполнителя, без учета времени восстановительных работ инфраструктуры ОС, 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 до 10 рабочих дней.

Примечания:

1) В случаях, если недоступность функционирования ЕСПД вызвана неквалифицированными действиями Потребителя услуги или внешними воздействиями (отсутствие электропитания), не зависящими от Исполнителя, связанное с ними время простоя не учитывается при определении доступности.
2) В случаях, если для решения заявки требуется дополнительная информация от Потребителя услуги или проверка работоспособности с его стороны, время простоя не учитывается, до получения запрошенной информации.
3) Отключения (перерывы), вызванные любой из перечисленных ниже причин, не классифицируются как недоступность или неисправность:

- проведение плановых профилактических или неотложных ремонтных работ с уведомлением представителей Заказчика и/или Потребителей в срок не менее трех рабочих дней до времени проведения работ;
- работа на оборудовании Исполнителя по запросу представителя Потребителя и/или по запросу ОС с уведомлением Потребителей;
- тестирование Услуги по запросу представителей Потребителя в случае, когда не было выявлено никакой неисправности или недоступности;
- неисправности или дефекты оборудования ОС и/или Потребителей;
- перерывы в предоставлении Услуг, вызванные умышленными или неумышленными действиями Потребителей и/или ОС;
- форс-мажор.

3. Состав Услуги ЕСПД

3.1 Оказание Услуги по передаче данных при осуществлении доступа для СЗО к государственным, муниципальным, иным информационным системам и к информационно-телекоммуникационной сети Интернет и к информационно-телекоммуникационной сети «Интернет» с использованием ЕСПД (далее – **Услуга**).

3.1.1. Компонент Услуги по предоставлению осуществляемого с использованием ЕСПД доступа для СЗО к государственным, муниципальным, иным информационным системам и к информационно-телекоммуникационной сети Интернет (далее – **Предоставление доступа**).

3.1.2. Компонент Услуги «Передача данных». Обеспечивает передачу данных для СЗО, при осуществлении доступа к государственным, муниципальным, иным информационным системам и к информационно-телекоммуникационной сети «Интернет» и к информационно-телекоммуникационной сети «Интернет» с использованием единой сети передачи данных (далее – **Передача данных**).

3.1.3. Компонент Услуги «Защита данных». Обеспечивает защиту данных, обрабатываемых и передаваемых при осуществлении доступа для СЗО к государственным, муниципальным, иным информационным системам и к сети «Интернет» и к информационно-телекоммуникационной сети «Интернет» (далее – **Защита данных**).

3.1.4. Компонент Услуги «Ограничение доступа к информации». Обеспечивает ограничение для СЗО доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, наносящей вред здоровью и развитию детей, содержащейся в сети «Интернет» (далее – **Ограничение доступа к информации**).

3.1.5. Компонент Услуги «Мониторинг и обеспечение безопасности связи». Обеспечивает мониторинг и безопасность связи при подключении и предоставлении доступа СЗО к ИС и к сети «Интернет» (далее – **Мониторинг и обеспечение безопасности связи**).

4. Требования к Услуге

4.1. Услуга должна представлять собой совокупность компонентов с возможностью их комбинации и изменений. Основными принципами обеспечения Услуги должны являться универсальность, управляемость и масштабируемость.

4.2. Управление Услугой.

1) Исполнитель должен осуществлять управление изменениями, которые могут включать изменения параметров Услуги:

- интерфейсы оборудования Точек присоединения ЕСПД, к которому подключается оборудование ОС;
- топология ЕСПД;
- IP адреса и подсети;
- протоколы маршрутизации;
- профили портов доступа;
- пропускная способность передачи трафика разных типов по предоставляемым каналам связи между СЗО в зоне ответственности Оператора ЕСПД;
- параметры качества передачи IP-пакетов и Ethernet кадров СЗО между СЗО в зоне ответственности Оператора ЕСПД;
- подключение СЗО к сети Исполнителя при изменении количества СЗО, адреса месторасположения СЗО в зоне ответственности Оператора ЕСПД;
- параметры качества передачи IP-пакетов между СЗО в зоне ответственности Исполнителя;
- приостановление или возобновление оказания Услуги по передаче данных;
- оказание Услуги для новых СЗО по согласованию между Заказчиком и Исполнителем;
- прекращение оказания Услуги;
- иные согласованные Исполнителем и Заказчиком параметры Услуги.

4.3. Требования к производительности Услуги.

1) Производительность Услуги 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 Услуги должно достигаться следующими способами:

– замена или модернизация аппаратного обеспечения;
– замена или модернизация программного обеспечения;
– увеличение пропускной способности каналов связи.

5. Требования к компонентам Услуги

5.1. Услуга должна представлять собой набор следующих компонентов и элементов:

1) Компонент услуги «Предоставление доступа».
2) Компонент услуги «Передача данных»:
- Элемент «Передача данных в ВЧС с заданными параметрами качества»;
- Элемент «Передача данных в сеть «Интернет».
3) Компонент услуги «Защита данных»:
- Элемент «Криптографическая защита каналов связи».
4) Компонент услуги «Ограничение доступа к информации»:
- Элемент «Контентная фильтрация».
5) Компонент услуги «Мониторинг и обеспечение безопасности связи»:
- Элемент «Мониторинг параметров качества предоставляемых услуг»;
- Элемент «Защита от DDoS атак»;
- Элемент «Межсетевое экранирование».

5.2. Компонент Услуги «Предоставление доступа»

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

5.2.1. Требования к архитектуре Компонента услуги «Предоставление доступа»

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

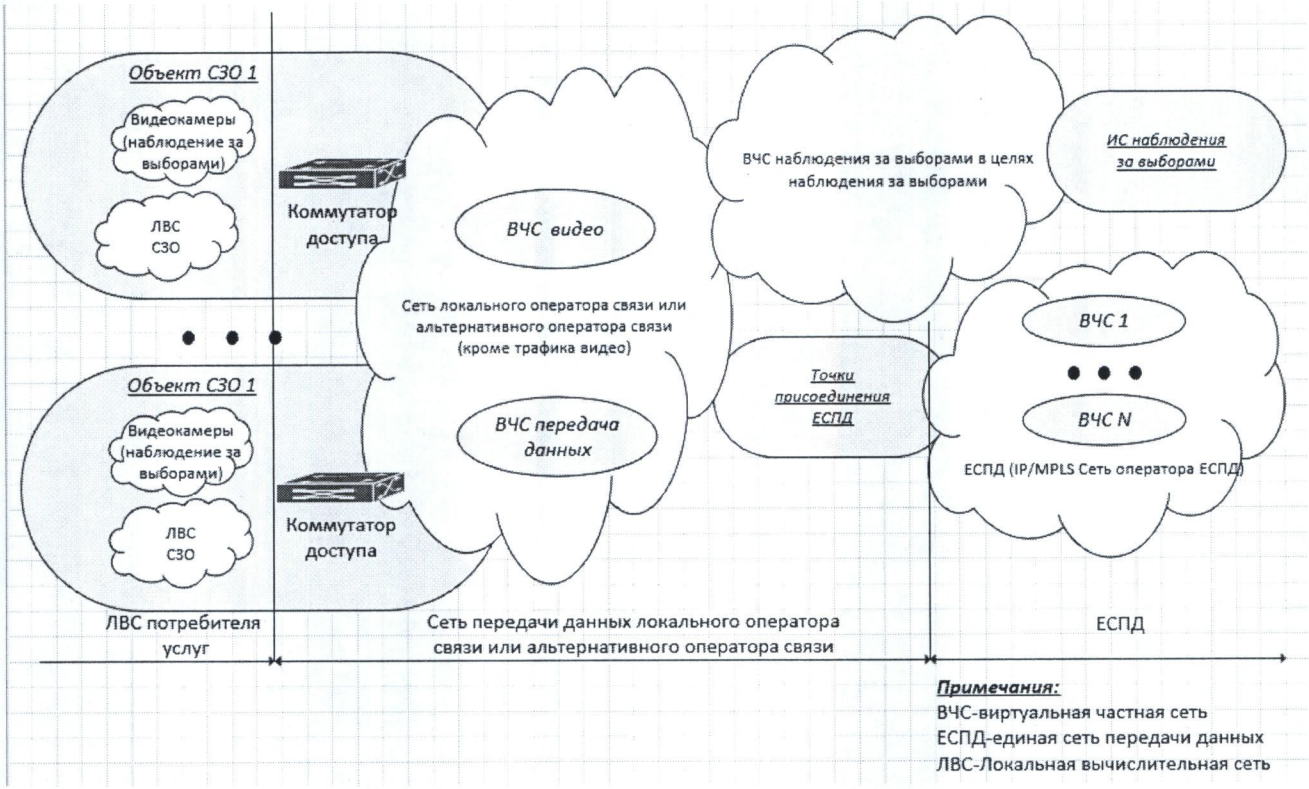


Рис.1.Архитектура Компонента услуги «Предоставление доступа» для СЗО

5.2.2. Технические средства реализации Компонента услуги «Предоставление доступа»

1) Подключение сетей передачи данных ОС к Точке присоединения ЕСПД осуществляется в соответствии с п. 2.12. ТЗ.

2) Границы технической ответственности Оператора ЕСПД определяются в договоре присоединения, заключаемом Оператором ЕСПД и ОС в соответствии с законодательством Российской Федерации.

5.2.3. Управление Компонентом услуги «Предоставление доступа»

Для указанных Заказчиком СЗО Оператор ЕСПД должен осуществлять управление изменениями, которые могут включать изменения параметров оказания Услуги:

– интерфейс на оборудовании Оператора ЕСПД, к которому подключается

оборудование ОС;

- топология ЕСПД;
- IP адреса и подсети;
- протоколы маршрутизации;
- профили портов доступа;
- пропускная способность передачи трафика разных типов по предоставляемым каналам связи между СЗО в зоне ответственности Оператора ЕСПД;
- параметры качества передачи IP-пакетов и Ethernet кадров СЗО между СЗО в зоне ответственности Оператора ЕСПД;
- подключение СЗО к сети Оператора ЕСПД при изменении адреса месторасположения СЗО в зоне ответственности Оператора ЕСПД;
- приостановление или возобновление оказания Услуги;
- оказание Услуги для новых СЗО в зоне ответственности Оператора ЕСПД по согласованию между Заказчиком и Исполнителем;
- прекращение оказания Услуги по предоставлению доступа;
- иные согласованные Оператором ЕСПД и Заказчиком параметры Услуги.

5.2.4. Требования к дополнительному функционалу и сопряжению со смежными системами

1) Услуга должна иметь возможность расширять функционал посредством подключения к информационных ресурсам и системам, без снижения уровня информационной безопасности, емкости Услуги и производительности.

2) К смежным системам относятся:

- сеть Интернет;
- внешние центры обработки данных Оператора ЕСПД и/или Владельцев ИС.

5.2.5. Требования к производительности

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

производительности Исполнитель должен предусмотреть такую возможность.

5.2.6. Компонент услуги «Предоставление доступа» должен обеспечить совокупную пропускную способность из расчета необходимости обеспечения каждому подключенному СЗО 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;

5.2.7. Увеличение производительности Компонента услуги «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.

5.3. Компонент услуги «Предоставление доступа» должен обеспечивать доступ к сети Интернет и возможность доступа СЗО к ИС в соответствии с требованиями ТЗ.

5.3.1. Назначение Компонента услуги «Предоставление доступа».

Компонент услуги «Предоставление доступа» предназначен для организации подключения СЗО через сети передачи данных ОС к Точкам присоединения ЕСПД, указанных в Плане организации Точек присоединения к ЕСПД.

5.3.2. Требование к Компоненту услуги «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 услуги 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.

5.3.3. 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 (за исключением удаленных и труднодоступных муниципальных образований). 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 CE 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.

5.3.4. 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 при взаимодействии между Потребителями услуги должна отсутствовать. Пересечение адресных пространств исключается использованием легитимных (выданных централизованно) адресных пулов.

5.3.5. Требования к пропускной способности

При оказании Услуги должен обеспечиваться доступ СЗО к ЕСПД со следующими скоростными параметрами:

	Скорость доступа к ЕСПД Интернет
Образовательные организации, расположенные в городских населенных пунктах	100 Мбит/с
Образовательные организации, расположенные вне городских населенных пунктах	50 Мбит/с
Образовательные организации, подключаемых с использованием спутниковых линий связи	В соответствии с Приложением №1к ТЗ (Не менее 1 Мбит/с)

5.3.6. 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 услуги 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.

5.3.7. Дополнительные требования по обеспечению Компонент услуги «Предоставление доступа» могут быть установлены приказом Минцифры России.

5.4. Компонент услуги «Передача данных»

5.4.1. Требования к архитектуре Компонента услуги «Передача данных».

Архитектура Компонента услуги «Передача данных» приведена на рисунках 3 и 4.

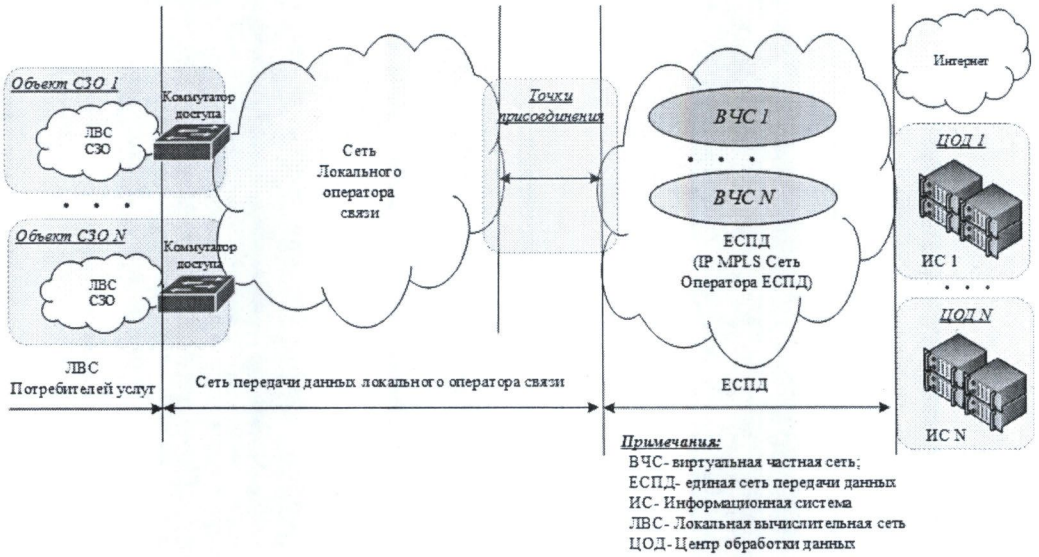


Рис.3.Архитектура Компонента услуги «Передача данных».

5.4.2. Дополнительные требования по обеспечению Компонент услуги «Передача данных» могут быть установлены приказом Минцифры России.

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

5.5.1. 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.

5.5.2. Требования к пропускной способности

ПД в ВЧС должна осуществляться с учетом следующих скоростных параметров подключения СЗО к ЕСПД:

	Скорость доступа к сети Интернет
Образовательные организации, расположенные в городских населенных пунктах	100 Мбит/с
Образовательные организации, расположенные вне городских населенных пунктах	50 Мбит/с
Образовательные организации, подключаемых с использованием спутниковых линий связи	В соответствии с Приложением №1к ТЗ (Не менее 1 Мбит/с)

5.5.3. 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.

5.5.4. 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) Пропускная способность передачи данных между любыми двумя СЗО по каналам через ЕСПД в зоне ответственности Оператора ЕСПД, должна определяться как наименьшее значение из пропускных способностей подключений данных объектов к ЕСПД.

3) Гарантии качества передачи IP-пакетов с данными Потребителя услуги 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

Значения параметров качества передачи данных на составных каналах с учетом наличия беспроводного участка между Точками присоединения, расположенными на территории Чукотского автономного округа:

Тип трафика	Процент потерянных IP-пакетов, не более	Задержка передачи IP-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

5.6. Элемент «Передача данных в сеть Интернет (далее –Элемент ПД в Интернет)

5.6.1. 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. Севастополь, в соответствии с п. 2.18. Элемент ПД в Интернет должен предоставляться в географических точках субъектов Российской Федерации (за исключением Республики Крым и г. Севастополь), наиболее близко расположенных к Точкам присоединения ЕСПД, из которых инициируется такой доступ.

3) Перед началом оказания ПД в Интернет для СЗО, указанных в Приложении №1, Исполнителем должны предоставляться выделенный симметричный дуплексный доступ к сети Интернет с пропускной способностью, соответствующей требованиям ТЗ.

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-адерса.

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, 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.

5.7. Компонент услуги «Защита данных»

5.7.1. Назначение Компонента услуги «Защита данных»

Компонент услуги «Защита данных» предназначена 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.

1) 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.

5.7.2. Требования к архитектуре Компонента услуги

Архитектура Компонента услуги «Защита данных» определяется Исполнителем.

Компонент услуги «Защита данных» должен использовать ЕСПД в качестве транспорта для защищаемых криптографическими средствами данных. Компонент услуги должен обеспечивать защищенный доступ из СЗО до ИС, расположенных в федеральном, региональном или муниципальном ЦОД Владельцев ИС, в соответствии с п.2.27. - 2.31.

5.7.3. Управление Компонентом услуги «Защита данных»

Для указанных Заказчиком СЗО Исполнитель должен осуществлять управление изменениями, которые могут включать изменения следующих

параметров:

- интерфейса на оборудовании Исполнителя, к которому подключается оборудование СЗО;
- 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;
- 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.

5.7.4. Требования к производительности Компонента услуги «Защита данных»

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

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

5.7.5. Дополнительные требования по обеспечению Компонент услуги «Защита данных» могут быть установлены приказом Минцифры России.

5.8. Элемент «Криптографическая защита каналов связи» (далее – Элемент

«Криптозащита»)

5.8.1. 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.

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.

5.8.2. 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 Потребителей услуг.

3) Шифрование реализуется на основе криптомаршрутизаторов, соответствующих требованиям п.2.45.1. п. 2.45.2. 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.

5.8.3. 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 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования» или 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.

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

- возможность «горячего» резервирования (в режиме отказоустойчивого активно-пассивного кластера);

- 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.

5.8.5. 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 500 Мбит/с.

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

- возможность «холодного» резервирования;
- возможность обеспечивать производительность шифрования не менее 50 Мбит/с;
- скорость передачи данных при работе в сетях L3 VPN - до 100 Мбит/с.

5.9. Требования к Компоненту услуги «Ограничение доступа к информации» (далее – Компонент услуги)

Компонент услуги «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 года «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

утверждённые Минобрнауки России 28 апреля 2014г.

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

5.9.1. Требования к архитектуре Компонента услуги

- 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.

5.10. Управление Компонентом услуги

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

- 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;
- прекращение оказания услуги;
- и иные согласованные Исполнителем и Заказчиком параметры Компонента услуги.

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

1) Компонент услуги 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 услуги должны быть использованы для размещения ресурсов, необходимых для обеспечения Компонентов услуги, а также для получения дополнительной информации по фильтрации.

5.12. Требования к производительности Компонента услуги:

1) Производительность Компонента услуги 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 услуги должно достигаться следующими способами:

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

5.12.1. Дополнительные требования по обеспечению Компонент услуги

«Ограничение доступа к информации» могут быть установлены приказом Минцифры России.

5.13. Элемент «Контентная фильтрация» (далее - Элемент)

5.13.1. Требования к архитектуре Элемента

Архитектура решений по контентной фильтрации в рамках ЕСПД представлена на рисунках 5 и 6.

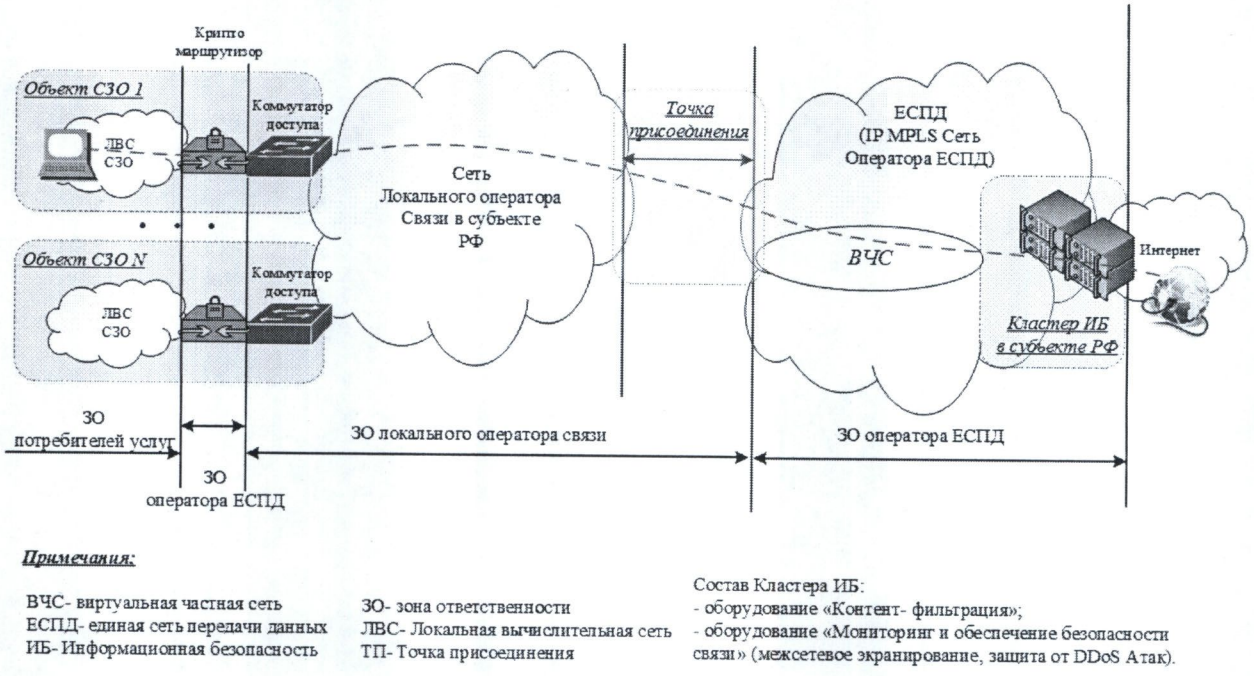


Рис. 5. Общая архитектура решений по контентной фильтрации.

Оборудование КФ должно располагаться в административных центрах субъектов РФ в соответствии с п. 2.16. (за исключением Республики Крым и г. Севастополь).

5.13.2. 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;
- блокировка приложений популярных социальных сетей, с возможностью открытия доступа, по запросу Потребителя услуг 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.
- 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.

5.13.3. Требования к применяемым техническим решениям

- КФ должна быть реализована с использованием программно-аппаратных комплексов;
- поставляемое решение должно быть внесено в Единый реестр российских программ для электронных вычислительных машин и баз данных;
- возможность, по запросу от Потребителя услуги, автоматизации процессов, связанных с предоставлением услуги «Ограничение доступа к информации» посредством элемента «Контентная фильтрация».

5.13.3.1. 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 пользователей/IP-адресов.
- 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.

5.14. Компонент Услуги «Мониторинг и обеспечение безопасности связи»

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 соблюдения требуемого качества услуг связи, целостности и устойчивости функционирования сетей передачи данных посредством использования метрологического программно-аппаратного комплекса, а также безопасность связи при подключении

и предоставлении доступа для СЗО к государственным, муниципальным, иным информационным системам и к сети «Интернет»;

2) Протоколирование действий пользователей и администраторов системы.

3) Формирование отчетности с предоставлением функционала:

– задания фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности;
– формирования запросов к базе данных;
– задания формата отчетов.

4) Отправку отчетов по расписанию и по запросу администраторов системы.

5.14.1. Требования к наличию отчетов

Компонент Услуги должен обеспечивать формирование отчетности в табличном и графическом виде о совершаемых пользователями действиях в сети Интернет за различные периоды времени.

5.14.2. Требования к Компоненту услуги «Мониторинг и обеспечение безопасности связи» (далее – Компонент услуги):

1) Компонент услуги должен представлять собой совокупность Элементов с возможностью их комбинации и изменений.

2) Основными принципами мониторинга и обеспечения безопасности связи должны являться универсальность, управляемость и масштабируемость.

3) Компонент услуги должен позволять запуск дополнительных Элементов по требованию Потребителя услуги без дополнительных затрат (за исключением необходимости расширения каналов ПД при расширении каналов сетей доступа).

4) Технические программно-аппаратные средства, используемые при оказании Компонента услуги, 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.
- сертификация оборудования в соответствии с постановлением Правительства Российской Федерации от 25 июня 2009 г. № 532 «Об утверждении перечня средств связи, подлежащих обязательной сертификации»;
- использования отечественного радиоэлектронного оборудования в порядке, предусмотренном постановлением Правительства Российской Федерации от 10 июля 2019 г. № 878 «О мерах стимулирования производства радиоэлектронной продукции на территории Российской Федерации при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, о внесении изменений в постановление Правительства Российской Федерации от 16 сентября 2016 г. № 925 и признании утратившими силу некоторых актов Правительства Российской Федерации».

5.14.3. Требования к архитектуре Компонента услуги

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

Технические решения, применяемые в рамках оказания Компонента услуги,

должны представлять собой иерархическую систему с возможностью горизонтального и вертикального масштабирования.

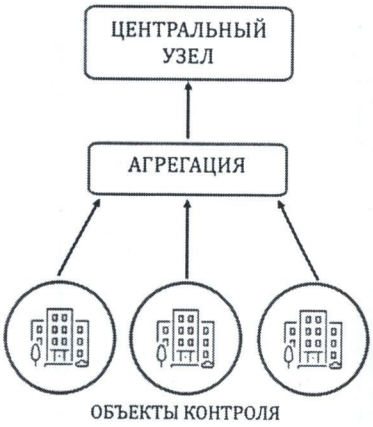


Рис. 6. Общая архитектура Компонента услуги.

Центральным узлом технических решений, применяемых в рамках оказания Компонента услуги, должен являться отказоустойчивый кластер серверов. Уровнем агрегации должны являться зонды уровня агрегации, размещаемые в зоне ответственности Оператора ЕСПД и/или ОС, объектами контроля должны являться оказываемые СЗО, приведенным в Приложении № 1, услуги связи с использованием зондов, размещаемых на указанных СЗО.

Технические решения, применяемые для оказания Компонента услуги, 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.

Измерения качества услуг для каждого СЗО должны производиться для двух участков отдельно:

- от СЗО до Точки присоединения к ЕСПД;
- от СЗО до Интернет-ресурсов.

5.14.4. Управление Компонентом услуги

Для указанных Заказчиком объектов Потребителей услуги 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 объектами Потребителя услуг;
- IP адрес для защиты от DDoS атак;
- подключение объектов Потребителя услуги к сети Исполнителя при изменении адреса месторасположения объектов Потребителя услуги;
- приостановление или возобновление оказания мониторинга и обеспечения безопасности связи;
- Мониторинг и обеспечение безопасности связи для новых объектов Потребителей услуги по согласованию между Заказчиком и Исполнителем;
- прекращение мониторинга и обеспечения безопасности связи;
- иные согласованные Исполнителем и Заказчиком параметры мониторинга и обеспечения безопасности связи.

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

1) Компонент услуги 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 услуги должны быть использованы для мониторинга параметров качества предоставляемых услуг

5.14.6. Требования к производительности Компонента услуги

1) Производительность Компонента услуги должна быть достаточной,

для выполнения возложенных на нее задач. В случае необходимости увеличения производительности Исполнитель должен предусмотреть такую возможность.

2) Увеличение производительности Компонента услуги должно достигаться следующими способами:

– замена или модернизация аппаратного обеспечения;

– замена или модернизация программного обеспечения;

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

5.14.7. Дополнительные требования по обеспечению Компонент услуги «Мониторинг и обеспечение безопасности связи» могут быть установлены приказом Минцифры России.

5.14.8. . Требования к наличию отчетов

— Система мониторинга должна обеспечивать по каждому СЗО, представленному в Приложении №1, формирование в электронном виде по запросу уполномоченного оператора 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 уполномоченным лицам Заказчика;

— формирование в электронном виде оперативных отчетов за произвольный период времени о качестве конкретной услуги связи для конкретного СЗО при самостоятельном обращении Заказчика к Системе;

— накопление сформированных отчетов в базе данных регламентной отчетности.

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

5.15.1. 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.

5.15.2. Требования к Элементу:

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

2) должен проводиться анализ Интернет-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) круглосуточно должны предоставляться Потребителю в личном кабинете Потребителя результаты анализа Интернет-трафика в графическом виде посредством демонстрации графиков или таблиц и в виде стандартизованных отчетов;

6) необходимо оповещать Потребителя о наличии нежелательного Интернет-трафика при его появлении;

7) 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.

5.15.3. 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;
- 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.

5.16. Элемент «Межсетевое экранирование» (далее – Элемент)

5.16.1. Назначение Элемента

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

5.16.2. Требования к Элементу:

1) Элемент должен решать следующие задачи:

- разграничение сетевого взаимодействия между сегментами;
- блокировка запрещенных типов взаимодействий;
- журналирование или подсчет числа попыток осуществления запрещенных взаимодействий;
- блокировка обращений к известным серверам злоумышленников;

– поддержка блокировки трафика на основании сигнатур.

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.

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.

5.16.3. Требования к применяемым техническим решениям Элемента

5.16.4. Требования к поставке:

- оборудование Элемента системы должно быть реализовано в виде программно-аппаратного комплекса для организации кластера отказоустойчивости active-passive или active-active;
- поставляемое решение должно быть внесено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

5.16.5. Требования к функционалу средств мониторинга и отчетности:

- должно обеспечиваться протоколирование действий пользователей и администраторов Системы;
- должно обеспечиваться формирование отчетности с предоставлением функционала:
- должно обеспечиваться задание фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности;
- должно обеспечиваться формирование запросов к базе данных;
- должно обеспечиваться задание формата отчетов;
- должна обеспечиваться отправка отчетов по расписанию и по запросу администраторов системы;
- должно обеспечиваться отключение мониторинга функционирования и формирования отчетности для конкретных пользователей/IP-адресов;
- должно обеспечиваться управление доступом к средствам мониторинга и отчетности с использованием ролевой модели.

5.16.6. Требования к пользовательскому интерфейсу:

- программный интерфейс компонентов системы, включая средства управления, а также формы оповещений и уведомлений администраторов системы и пользователей сети Интернет должен полностью поддерживать русский язык, используя кодировку текста UTF-8;
- наличие Web-интерфейса для доступа к компонентам узла фильтрации Интернет-трафика, включая средства управления, полностью поддерживающего русский язык, используя кодировку текста UTF-8.

5.16.7. Требования к наличию отчетов

Элемент должен обеспечивать формирование отчетности в табличном и графическом виде о совершаемых пользователями действиях в сети Интернет за различные периоды времени.

6. Порядок контроля, приемки и измерения качества предоставления Услуги

6.1. Исполнитель не позднее **10.11.2021** предоставляет на утверждение Заказчику:

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

— Форму отчета об использовании оборудования российского происхождения;

— Форму отчета о присоединенных ИС;

— Методику проведения приемо-сдаточных испытаний.

6.2. В срок до **10 декабря 2021** года Исполнитель направляет Заказчику документы в соответствии с п. 6.10.1. ТЗ по итогам оказания Услуг СЗО, указанным в Приложении № 1 к ТЗ.

6.3. В срок, указанный в п. 6.2., Исполнитель предоставляет отчет об использовании телекоммуникационного оборудования, страной происхождения которого является Российская Федерация в соответствии с п. 2.12. ТЗ.

6.4. В срок, указанный в п. 6.2., Исполнитель предоставляет отчет о присоединённых к ЕСПД ИС и региональных сетей передачи данных субъектов Российской Федерации, в соответствии с п. 2.27. и п. 2.28. ТЗ.

6.5. В срок, указанный в п. 6.2., Исполнитель предоставляет копии соглашений с оператором СКЗИ, заверенных Исполнителем, для СЗО, присоединенных к ЕСПД в соответствии с п. 2.42.2 ТЗ.

6.6. В срок, указанный в п. 6.2., Исполнитель направляет Заказчику сведения об использовании оборудования российского происхождения по форме, разработанной в соответствии с п.6.1 и утвержденной Заказчиком.

6.7. В срок, указанный в п. 6.2., в рамках Компонента услуги «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).

6.8. Для СЗО, которым оказываются Услуги, Заказчик посредством СКПУС определяет наличие доступа к информационным системам и сети Интернет на СЗО.

6.9. При отсутствии СКПУС, Заказчик имеет право проводить выборочную проверку оказываемых Услуг. Выборочная проверка проводится в Точках присоединения ЕСПД в соответствии с Программой и методикой испытаний (Приложение № 2).

6.9.1. По итогам проведения испытаний составляется Протокол проведения тестирования Услуги (далее – Протокол) (Приложение № 6) с указанием результатов испытаний по каждому параметру компонентов Услуги. Протокол заверяется Исполнителем, уполномоченным представителем Заказчика, ответственным представителем Министерства просвещения Российской Федерации, 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.

6.9.2. На основании Протокола составляется Акт проверки оказания Услуг (Приложение № 8), подписываемый Исполнителем, уполномоченным представителем Заказчика, ответственным представителем Министерства просвещения Российской Федерации, 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.

6.10. Заказчик производит приемку оказанных Услуг в следующей последовательности:

6.10.1. Исполнитель предоставляет Заказчику Акты об оказании Услуг по передаче данных (Приложение № 5), подписанные Исполнителем и уполномоченным представителем каждого СЗО. Скан-копии Актов об оказании Услуги загружаются Исполнителем в СКПУС.

6.10.1.1. Услуги считаются оказанными в случае если по результатам тестирования в соответствии с утвержденной Заказчиком Методикой проведения приемо-сдаточных испытаний Получатель подписал Акт об оказании Услуг.

6.10.2. Контроль качества предоставления Услуг по передаче данных осуществляется Заказчиком посредством СКПУС.

6.10.3. Акт сдачи-приемки оказанных услуг по этапу (Приложение № 2 к государственному контракту), подписывается Исполнителем и Заказчиком на основании предоставленных Исполнителем Актов об оказании Услуг по передаче данных и отчета Оператора СКПУС.

6.11. Исполнитель в срок до 10 декабря 2021 годов, соответственно, направляет Заказчику сведения о подключении СЗО к ЕСПД по форме, указанной в Приложении № 7.

6.12. Исполнитель в срок до 31 января года, следующего за годом подключения, размещает в информационной системе Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации в электронном виде информацию о технологических возможностях сетей связи, реализованных в ходе исполнения государственного контракта, перспективах их развития, средствах и линиях связи, в соответствии с требованиями Приложения № 1 к Требованиям к порядку ввода сетей электросвязи в эксплуатацию, утвержденным Приказом Минцифры России от 26.08.2014 № 258 (ред. от 06.02.2019).

Приложения:

1. Перечень СЗО;
2. Программа и методика испытаний;
3. Технические требования по взаимодействию ЕСПД со СКУПС СЗО;
4. План организации Точек присоединения (Форма);
5. Акт об оказании Услуг по передаче данных(Форма);
6. Протокол проведения тестирования Услуг (Форма);
7. Сведения о подключении СЗО к ЕСПД (Форма);
8. Акт проверки оказания Услуг (Форма);
9. Технический акт по присоединению (Форма);
10. Сведения о СЗО, по которым отсутствует готовность Оператора связи к присоединению к ЕСПД и (или) параметры сети Оператора связи не соответствуют Требованиям, в рамках исполнения государственного контракта (Форма).

от Заказчика:
Заместитель Министра цифрового развития, связи и массовых коммуникаций Российской Федерации

_____ / Д.М. Ким /

М.П.

от Исполнителя:
Старший Вице-Президент по работе с корпоративным и государственным сегментами ПАО «Ростелеком»

_____ /В.В. Ермаков/

М.П. (при наличии)