Приложение № 1 к государственному контракту

от «__» _____ 202_ года № _____

# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

***на оказание обеспечения услугами по предоставлению с использованием единой сети передачи данных доступа к государственным, муниципальным, иным информационным системам и к информационно-телекоммуникационной сети «Интернет» образовательных организаций, реализующих образовательные программы общего образования и среднего профессионального образования***

## 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 объектов образовательных организаций, используемое для маршрутизации трафика из сети объекта образовательных организаций в сеть Исполнителя и обратно. Находится под управлением выделенного подразделения Исполнителя. |
| CIR | Committed Information Rate — гарантированная полоса пропускания: технология предоставления каналов связи, при которой осуществляется приоритизация клиентской полосы пропускания, и объекту предоставляется гарантированная скорость передачи данных при любых условиях (только для спутниковой технологии). |
| 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 образовательных организаций. |
| ICMP | Internet Control Message Protocol - протокол межсетевых управляющих сообщений. |
| IETF RFC | Документ (Request 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. |
| MIR | Maximum Information Rate — максимальная полоса пропускания: технология предоставления каналов связи, при которой определенная соглашением сторон скорость передачи данных является максимально возможной, и фактическая скорость передачи данных в каждый конкретный момент времени может зависеть от нагрузки на сеть (только для спутниковой технологии). |

| **Термин** | **Определение** |
|---|---|
| MPLS | Multi Protocol Label Switching, технология коммутации пакетов с использованием меток. |
| MPLS сеть Исполнителя | Построенная по технологии MPLS сетевая инфраструктура Исполнителя и привлекаемых Исполнителем субподрядчиков (соисполнителей), включающая опорные маршрутизаторы (P), граничные маршрутизаторы (PE), 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. |
| Альтернативный оператор | Оператор связи, обладающий необходимыми лицензиями в соответствии с законодательством Российской Федерации и предоставляющий каналы L2 и (или) услуги передачи данных по каналам L2 в соответствии с заказом Исполнителя или Потребителя. |
| АРМ | Автоматизированное рабочее место. |
| Вариация задержки | Jitter, отклонение от среднего значения времени прохождения IP-пакетов по участку измерения от передающей стороны к приемной стороне |
| Владелец ИС | Федеральный орган государственной власти, орган государственной власти субъекта Российской Федерации, орган местного самоуправления, образовательная организация, иное учреждение, владеющее ИС. |
| Внешние IPv4 адреса | Внешние (публичные) IP адреса из зарегистрированного в базе данных RIPE NCC IP адресов 4 версии протокола IP. |
| Временный белый список | Перечень ресурсов в сети «Интернет», доступ к которым разрешен по запросам Потребителей и уполномоченных государственных органов в течение определенного промежутка времени. |
| Время реакции | Срок, в течение которого Исполнитель обязуется приступить к работе над проблемой, обозначенной в запросе Получателя об инциденте, определенный SLA. |
| ВОЛС | Волоконно-оптическая линия связи. |

| **Термин** | **Определение** |
|---|---|
| ВЧС | Виртуальная частная сеть, построенная на базе MPLS сети Исполнителя и привлекаемых Исполнителем субподрядчиков (соисполнителей), путем организации виртуальных каналов между портами на узлах доступа сети Исполнителя, к которым подключен объект образовательной организации, и обеспечивающая передачу различных типов трафика с гарантией параметров качества. |
| Заказчик | Министерство цифрового развития, информационных технологий и связи Ростовской области. |
| Доступность услуги | Отношение времени нахождения оказываемых услуг в рабочем состоянии к общей продолжительности интервала наблюдения, выраженное в процентах (доступность за отчетный период). |
| ЕСИА | Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» (ЕСИА) |
| ЕСПД | Виртуальная частная сеть (сети) Исполнителя, 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». |
| Задержка | One-way delay, время прохождения IP-пакетов по участку измерения в одну сторону (от передающей стороны к приемной). Определяется согласованными с Потребителем методами и при необходимости рассчитывается как половина временного интервала между моментом отправления сообщения «запрос эхо» передающей стороной и моментом получения сообщения «отклик эхо» от приемной стороны (PING протокола ICMP). |
| Заявка | Надлежащим образом оформленное по форме (Приложение № 1 к ТЗ) обращение Заказчика к Исполнителю с указанием дат и перечня объектов, для которых необходимо оказывать Услуги связи. |
| Иная технология | Технологии линий связи, отличные от технологий волоконно-оптической связи и спутниковой технологии. Используется в случае невозможности использования ВОЛС с обеспечением наибольшей скорости подключения. |
| ИС | Государственная, муниципальная или иная информационная система, класс криптозащиты которой соответствует классу защиты ЕСПД и к которой предоставляется доступ с использованием ЕСПД. |
| Исполнитель | Оператор связи, с которым заключен Контракт. |
| Канал L2 | Канал связи от объекта образовательной организации, до |

| **Термин** | **Определение** |
|---|---|
| | Точки присоединения ЕСПД. |
| Класс трафика | Набор требований к эксплуатационным параметрам, соблюдаемым Исполнителем при передаче по сети применительно ко всем IP-пакетам, принадлежащим данному типу. |
| Контракт | Государственный контракт на оказание обеспечения услугами по предоставлению с использованием единой сети передачи данных доступа к государственным, муниципальным, иным информационным системам и к информационно-телекоммуникационной сети «Интернет» образовательных организаций, реализующих образовательные программы общего образования и среднего профессионального образования. |
| Компонент | Составляющая Услуг связи, определяющая одну из основных потребностей, удовлетворяемых с помощью оказываемых Услуг. |
| Коэффициент потери пакетов | Максимальная потеря пакетов – отношение общего количества недоставленных пакетов к общему количеству переданных пакетов, выражаемая в процентах потерянных пакетов. |
| КФ | Контентная фильтрация. |
| Личный кабинет | Персональная страница для Потребителя, организованная на ресурсе сайта Исполнителя, доступ на которую осуществляется путем аутентификации с использованием ЕСИА с любого устройства, подключенного к сети «Интернет». |
| МСЭ | Межсетевое экранирование. |
| Нежелательный Интернет-трафик | Интернет-трафик, поступающий на оборудование объекта образовательной организации, наличие которого может быть обусловлено наличием DDoS-атаки, либо другими нежелательными для Потребителя факторами. |
| Образовательная организация | Государственная или муниципальная образовательная организация, реализующая программы общего образования и (или) среднего профессионального образования. |
| Объект | Совокупность технических средств, средств вычислительной техники и программного обеспечения, расположенных по одному адресу. |
| Отчетный период | Период времени оказания Услуг связи, по окончании которого производится сдача-приемка Услуг связи и их оплата. |
| Пакет | Форматированный блок информации, передаваемый по сети связи, функционирующей посредством технологии коммутации пакетов. |
| ПД | Передача данных. |
| Потребитель | Пользователь Услугами связи на Объекте. |
| Порт | Логический интерфейс ВЧС Потребителя на узлах доступа сети Исполнителя. |
| Постоянный белый список | Перечень ресурсов в сети «Интернет», доступ к которым разрешен по запросам Потребителей и уполномоченных государственных органов на постоянной основе. |

| **Термин** | **Определение** |
|---|---|
| Представитель образовательной организации | Руководитель образовательной организации, в интересах которого Исполнитель оказывает услуги в соответствии с Государственным контрактом, или иное 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, к количеству отправленных в конечную точку IP-пакетов. |
| Сеть «Интернет» | Информационно-телекоммуникационная сеть «Интернет». |
| Служба технической поддержки | Организуемая Исполнителем служба технической поддержки Потребителя, которая осуществляет контроль оказания Услуг связи в соответствии с Регламентом технической поддержки при оказании Услуг. |
| СОРМ | Система технических средств для обеспечения функций оперативно-розыскных мероприятий. |
| Спутниковая технология | Один из видов космической радиосвязи, основанный на использовании в качестве ретрансляторов искусственных спутников Земли – специализированных спутников связи. |
| Стоп-фактор | Признак состояния Объекта, при котором оказание предусмотренных Заявкой Услуг связи не требуется по не зависящим от Исполнителя обстоятельствам. |
| ТЗ | Настоящее техническое задание. |
| Точка присоединения ЕСПД | Средства связи, входящие в состав сети электросвязи Исполнителя, с помощью которых осуществляется подключение и доступ образовательной организации к ЕСПД. |
| Трафик | Совокупность IP-пакетов, переданных по сети передачи данных. |
| Услуги связи | Оказание Исполнителем Услуг связи для образовательных организаций по:<br><br>по предоставлению с использованием ЕСПД доступа к государственным, муниципальным, иным информационным системам и к информационно-телекоммуникационной сети «Интернет» (Компонент «Предоставление доступа»);<br><br>по передаче данных при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети «Интернет» (Компонент Услуги связи «Передача данных»);<br><br>по защите данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети «Интернет» (Компонент «Защита данных»);<br><br>по обеспечению ограничения доступа к информации, распространение которой в Российской Федерации запрещено, и к информации, причиняющей вред здоровью и (или) развитию детей, содержащейся в сети «Интернет» (Компонент «Ограничение доступа к информации»);<br><br>по мониторингу и обеспечению безопасности связи при предоставлении доступа к государственным, муниципальным, иным информационным системам и к |

| Термин | Определение |
|---|---|
| | сети «Интернет» (Компонент «Мониторинг и обеспечение безопасности связи»);<br>по организации подключения к ЕСПД (Компонент «Организация канала L2»);<br>по передаче данных при осуществлении доступа к ЕСПД (Компонент «Передача данных L2») |
| ЦОД | Центр обработки и хранения данных. |
| Черный список | Перечень ресурсов в сети «Интернет», доступ к которым заблокирован на уровне КФ по запросам Потребителей и уполномоченных государственных органов. |

## 2. Общие сведения

2.1. Основания оказания Услуг связи:

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

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

2.1.3. Указание Президента Российской Федерации от 13 сентября 2025 г. № Пр-2181;

2.1.4. Пункт 1 Перечня поручений Заместителя Председателя Правительства Российской Федерации – Руководителя Аппарата Правительства Российской Федерации от 7 октября 2025 г. № ДГ-П10-37307;

2.1.5. Оказание Услуг связи должно соответствовать:

— Федеральному закону от 7 июля 2003 г. № 126-ФЗ «О связи»;

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

— Федеральному закону от 27 июля 2006 г. № 152-ФЗ «О персональных

данных»;

— Федеральному закону от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»;

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

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

— Перечень выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, утвержденным постановлением Правительства РФ от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

— Правилам оказания услуг связи по передаче данных, утвержденным постановлением Правительства Российской Федерации от 31 декабря 2021 г. № 2606;

— Правилам оказания телематических услуг связи, утвержденным постановленем Правительства Российской Федерации от 31 декабря 2021 № 2607;

— постановлению Правительства Российской Федерации от 30 декабря 2020

г. № 2385 «О лицензировании деятельности в области оказания услуг связи и признании утратившими силу некоторых актов Правительства Российской Федерации»;

— Правилам взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, утвержденным постановлением Правительства Российской Федерации от 27 августа 2005 г. № 538;

— Составу и содержанию 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, утвержденным приказом ФСБ России от 10 июля 2014 г. № 378;

— Правилам 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, утвержденным приказом Министерства связи и массовых коммуникаций Российской Федерации от 16 апреля 2014 г. № 83;

— Требованиям к сетям электросвязи для проведения оперативно-розыскных мероприятий Часть 1. Общие требования, утвержденным приказом Министерства связи и массовых коммуникаций Российской Федерации от 16 января 2008 г. № 6;

— Требованиям к подключению и доступу, включая требования к передаче данных, государственных и муниципальных образовательных организаций, реализующих программы общего и среднего профессионального образования,

к единой сети передачи данных, утвержденным 30 апреля 2021 г. приказом Минцифры России № 417 Минпросвещения России от № 221;

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

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

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

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

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

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

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

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

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

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

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

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

2.2. **Срок оказания Услуг связи: со дня заключения контракта по 31 декабря 2026 года включительно.**

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

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

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

2.3.1.1. Оказание Исполнителем услуг связи по:

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

— по защите данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети «Интернет» (**Компонент «Защита данных»**) (в определенных случаях возможно оказание услуг без Компонента «Защита данных»);

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

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

2) по предоставлению с использованием ЕСПД доступа к государственным, муниципальным, иным информационным системам и к сети

«Интернет» (**Компонент «Предоставление доступа»**).

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

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

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

2.4. Место оказания Услуг связи:

по месту нахождения Точек присоединения ЕСПД, по месту нахождения образовательных организаций, по месту нахождения Исполнителя.

2.5. Исходные данные.

При оказании Услуг связи Исполнитель должен руководствоваться следующими исходными данными:

– настоящим ТЗ;

– Заявками на оказание Услуг связи.

2.6. Результаты оказания Услуг связи.

2.6.1. Исполнителем оказаны услуги связи для образовательных организаций по:

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

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

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

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

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

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

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

2.7. Требования к Исполнителю.

Исполнитель должен соответствовать требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим оказание услуг связи, позволяющим на протяжении действия 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 должен иметь

лицензии на следующие виды деятельности:

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

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

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

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

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

– на оказание телематических услуг связи;

– лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических)

средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» в части следующих работ и услуг:

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

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

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

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

– предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей (п. 25 Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств);

– предоставление юридическим и физическим лицам защищенных с использованием шифровальных (криптографических) средств каналов связи для передачи информации (п. 27 Перечня выполняемых работ и оказываемых услуг,

составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств).

2.8. Время оказания Услуг связи.

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

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

2.10. ЕСПД должна быть организована по принципу полносвязной, защищенной сети связи, изолированной от сети «Интернет» и сетей других пользователей на логическом уровне и поддерживающей обмен данными (трафиком) через Точки присоединения ЕСПД.

2.11. Для оказания Услуг связи образовательным организациям в составе ЕСПД организуются каналы передачи данных и Точки присоединения ЕСПД.

2.12. Исполнитель обеспечивает присоединение канала связи между образовательной организацией и ЕСПД в Точках присоединения ЕСПД.

2.13. Требования к оборудованию Точек присоединения ЕСПД для образовательной организации:

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

2) Состав оборудования Точек присоединения ЕСПД определяется Исполнителем с учетом требований ТЗ;

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

4) Адрес (адреса) размещения Точек присоединения ЕСПД определяются Исполнителем.

2.14. Точки присоединения ЕСПД должны обеспечивать достаточное количество интерфейсов для подключения к ЕСПД Каналов L2.

2.15. Каналы связи ЕСПД между Точками присоединения ЕСПД для образовательных организаций, задействованные в оказании Услуг связи, должны использовать ВОЛС, за исключением каналов до образовательных организаций, находящихся в труднодоступных населенных пунктах и (или) подключенных по спутниковым каналам связи.

2.16. Не допускается организация каналов связи, использующихся для оказания Услуг связи образовательным организациям, через сеть «Интернет».

2.17. Для образовательных организаций 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».

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

2.19. Точки присоединения ЕСПД для образовательных организаций должны соответствовать следующим параметрам:

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

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

– другим требованиям, изложенным в ТЗ.

2.20. Исполнитель обязан оказывать Услуги связи для образовательной организации без ограничения объема передачи (безлимитно).

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

2.22. Исполнитель обязан произвести присоединение ИС к ЕСПД в течение 30 (тридцати) рабочих дней с даты получения запроса от Заказчика при условии готовности Владельцев ИС согласовать и реализовать предлагаемое

Исполнителем техническое решение по подключению в указанный срок, а также при назначении со стороны ИС лиц, ответственных за диагностику и устранение проблем, возникающих между ЕСПД и ИС (контакты ответственных передаются Исполнителю письмом). В случае неготовности Владельцев ИС исполнять указанные требования Исполнитель проводит эскалацию Заказчику для согласования новых сроков подключения.

2.23. Исполнитель за свой счет проводит все необходимые работы по присоединению ИС к ЕСПД в том числе в части обеспечения ИС оборудованием для обеспечения криптографической защиты передаваемых данных между ЕСПД и ИС, при наличии данной необходимости.

2.24. Исполнитель, для обеспечения Услуг связи, при подключении объекта к ЕСПД, в том числе после проведения капитального ремонта объекта единоразово оказывает содействие образовательной организации по настройке всех АРМ, имеющих техническую возможность подключения к ЕСПД. Последующее содействие по подключению новых АРМ после первичной организации услуги в образовательной организации или проведенного на объекте капитального ремонта оказываются путем предоставления необходимых инструкций и консультационной поддержки.

2.25. Подключение Канала L2 от образовательной организации к Точке присоединения ЕСПД проводится силами Исполнителя.

2.26. Требования к взаимодействию между Исполнителем и Представителем образовательной организации при предоставлении Услуг связи:

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

2.26.2. Исполнитель в течение всего срока оказания Услуг связи обеспечивает за свой счет настройку СЕ для оказания Услуг связи,

предусмотренных Контрактом, техническое обслуживание и ремонт оборудования, в том числе криптомаршрутизаторов, установленных Исполнителем в образовательной организации. При этом сроки и порядок выполнения регламентных и ремонтных работ устанавливаются Регламентом технической поддержки при оказании Услуги связи, утвержденным Заказчиком.

2.26.3. Требования к средствам маршрутизации:

2.26.3.1. Средства маршрутизации должны выполнять функции Firewall и QoS, а также должны:

- обеспечивать возможность мониторинга состояния по протоколу SNMP;
- поддерживать статическую и динамическую маршрутизацию IPv4 по протоколу BGPv4 (спецификация IETF RFC 1771);
- обладать механизмами фильтрации трафика по TCP/UDP портам;
- обеспечивать поддержку не менее 3 (трех) классов обслуживания трафика модели DiffServ.

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

2.27. Требования к модульности Услуг связи:

1) Услуги связи должны обладать модульностью;

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

3) Каждый Компонент должен обеспечивать выполнение своей функции.

2.28. Требования к отказоустойчивости Услуг:

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

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

– использование на сегментах MPLS-сети Исполнителя отказоустойчивых конфигураций оборудования и программного обеспечения;

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

–

– маршрутизацию трафика с применением протоколов статической или динамической маршрутизации;

3) В случае прекращения энергоснабжающей организацией подачи электропитания на Точку присоединения ЕСПД Исполнитель обязан обеспечить работоспособность Точки присоединения ЕСПД в течение 4 часов с момента прекращения подачи электропитания в Точку присоединения ЕСПД.

2.28.1. Требования к отказоустойчивости Компонента «Мониторинг и обеспечение безопасности связи» в части Элемента «Межсетевое экранирование:

1) Отказоустойчивость МСЭ должна обеспечиваться следующими решениями:

– использование отказоустойчивых конфигураций аппаратного и программного обеспечения;

– резервирование настроек средств защиты.

2.28.2. Требования к отказоустойчивости Компонента «Мониторинг и обеспечение безопасности связи» в части Элемента «Защита от DDoS-атак»:

1) Отказоустойчивость средств защиты от DDoS-атак 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.

2.29. Требования к реализации СОРМ.

Обеспечить реализацию функций СОРМ (СОРМ 2 и СОРМ 3), в соответствии с требованиями действующего законодательства Российской

Федерации.

2.30. Требования к технической поддержке при оказании Услуг связи:

2.30.1. В период оказания Услуг связи Исполнитель обязан осуществлять техническую поддержку Потребителей (далее - Техническая поддержка) по вопросам оказания Услуг связи в соответствии с Регламентом технической поддержки при оказании Услуги связи (утвержденным Заказчиком в соответствии с п. 7.1ТЗ).

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

2.30.3. Техническая поддержка должна осуществляться круглосуточно и ежедневно в соответствии с Регламентом технической поддержки при оказании Услуги связи, утвержденным Заказчиком. После утверждения Заказчиком Регламента технической поддержки при оказании Услуги связи он должен быть размещен Исполнителем на ресурсе, созданном в соответствии с п. 2.26.1 ТЗ.

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

– по единому бесплатному контактному номеру телефона;

– посредством отправки сообщений электронной почты на единый почтовый ящик;

– посредством личного кабинета;

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

2.30.5. Профилактические работы:

1) При проведении профилактических работ допускается перерыв в оказании Услуг связи.

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

2.30.6. Приоритеты и время восстановления работоспособности Услуг связи:

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 образовательных организаций) обращения в Службу технической поддержки, связанные с нарушением работоспособности Услуг связи, относящиеся к одному событию;

*2-ой приоритет – Высокий*:

– наблюдается массовая деградация производительности или периодическое прерывание услуги не менее, чем в 5 процентоах общего количества образовательных организаций, которым оказываются Услуги связи;
– фиксируются периодические прерывания или деградация (снижение скорости относительно заявленной) в работе Услуги связи в одной образовательной организации;

*3-й приоритет – Средний*:

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

*4-й приоритет – Низкий*:

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

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

*) Указано время устранения неисправности, не требующее выезда. Для восстановления магистральной кабельной инфраструктуры, работ на узловом и магистральном оборудовании, замены оборудования/восстановления кабельной инфраструктуры Исполнителя и иных работ, требующих выезда в образовательную организацию, нормативные сроки решения инцидента увеличиваются на 48 часов. Указано время для восстановительных работ инфраструктуры Исполнителя, без учета времени восстановительных работ оборудования образовательной организации, инфраструктуры информационных

систем, а также наличия образовательной организации в труднодоступном населенном пункте.

Для объектов, расположенных в труднодоступных населенных пунктах (труднодоступный населенный пункт - это населенный пункт, который в силу погодных, природных, техногенных и иных обстоятельств и (или) отсутствия элементов инфраструктуры становится недоступным или труднодостижимым для транспортных средств) срок решения инцидента для восстановления кабельной инфраструктуры Исполнителя, замены оборудования Исполнителя и иных работ, требующих выезда на объект, а также для восстановления магистральной кабельной инфраструктуры, работ на узловом и магистральном оборудовании, увеличивается на 9 рабочих дней.

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

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

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

2.30.7. **Регламент технической поддержки** при оказании Услуги связи

должен предусматривать порядок взаимодействия между Потребителем, Исполнителем и Заказчиком, в том числе:

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

## 3. Состав Услуг связи

Оказание Исполнителем Услуг связи состоит из следующих Компонентов:

3.1. Компонент «Предоставление доступа» обеспечивает предоставление доступа образовательным организациям к ЕСПД в случае его отсутствия (далее – **Предоставление доступа**).

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

— Компонент «Защита данных» обеспечивает защиту данных, обрабатываемых и передаваемых при осуществлении доступа к государственным, муниципальным и иным информационным системам, а также к сети «Интернет» (Далее - **Защита данных**) (в определенных случаях возможно оказание услуг без Компонента «Защита данных»);

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

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

3.3. Компонент «Организация канала L2» обеспечивает организацию канала связи, включая его создание или модернизацию в случае возможности улучшения параметров канала связи в соответствии с ТЗ с целью подключения к ЕСПД (Далее – **Организация канала L2**).

3.4. Компонент «Передача данных L2» обеспечивает передачу данных между объектами образовательных организаций и ЕСПД (Далее – **Передача данных L2**).

## 4. Требования к Услугам связи

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

4.2. Управление Услугами связи.

Исполнитель должен осуществлять управление изменениями, которые

могут включать изменения параметров Услуг связи:

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

– топология ЕСПД;

– IP-адреса и подсети;

– протоколы маршрутизации;

– профили портов доступа;

– пропускная способность передачи трафика разных типов по предоставляемым каналам связи для образовательной организацией в зоне ответственности Исполнителя;

– параметры качества передачи IP-пакетов и Ethernet-кадров для образовательной организации в зоне ответственности Исполнителя;

– подключение образовательных организаций к сети Исполнителя при изменении количества образовательных организаций;

– параметры качества передачи IP-пакетов для образовательной организации в зоне ответственности Исполнителя;

– приостановление или возобновление оказания Услуг связи;

– оказание Услуг связи для образовательных организаций по согласованию между Заказчиком и Исполнителем;

– прекращение оказания Услуг связи;

– иные согласованные Исполнителем и Заказчиком параметры Услуг связи.

## 5. Требования к Компонентам

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

1) Компонент «Предоставление доступа».

2) Компонент «Передача данных»:

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

3) Компонент «Защита данных»:
   - Элемент «Криптографическая защита каналов связи».
4) Компонент «Ограничение доступа к информации»:
   - Элемент «Контентная фильтрация».
5) Компонент «Мониторинг и обеспечение безопасности связи»:
   - Элемент «Мониторинг параметров качества предоставляемых услуг»;
   - Элемент «Защита от DDoS-атак»;
   - Элемент «Межсетевое экранирование».
6) Компонент «Организация канала L2».
7) Компонент «Передача данных L2».

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

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

#### 5.2.1. Требования к архитектуре Компонента «Предоставление доступа».

Архитектура Компонента «Предоставление доступа» приведена на Рисунок 1.

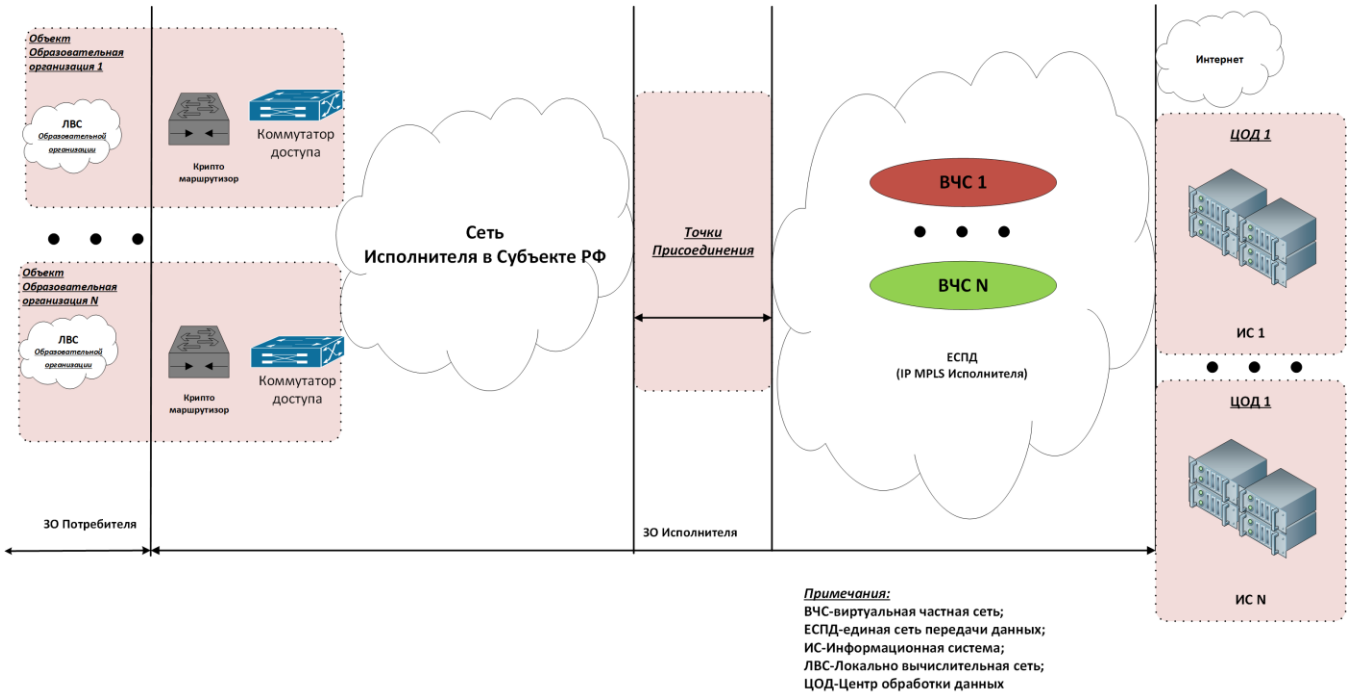



Рисунок 1 Архитектура Компонента "Предоставление доступа"

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

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

5.2.3. Управление Компонентом «Предоставление доступа».

Для указанных Заказчиком образовательных организаций Исполнитель должен осуществлять управление изменениями, которые могут включать изменения параметров оказания Услуг связи:

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

– топология ЕСПД;

– IP-адреса и подсети;

– протоколы маршрутизации;

– профили портов доступа;

– пропускная способность передачи трафика разных типов по предоставляемым каналам связи для образовательных организаций в зоне ответственности Исполнителя;

– параметры качества передачи IP-пакетов и Ethernet кадров для образовательных организаций в зоне ответственности Исполнителя;

– приостановление или возобновление оказания Услуги связи;

– оказание Услуг связи для новых образовательных организаций в зоне ответственности Исполнителя по согласованию между Заказчиком и Исполнителем;

– прекращение оказания Услуг связи по предоставлению доступа;

– иные согласованные Исполнителем и Заказчиком параметры Услуг связи.

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

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

2) К смежным системам относятся:

– сеть «Интернет»;

– ЦОД Исполнителя и/или Владельцев ИС.

5.2.5. Компонент «Предоставление доступа» должен обеспечить совокупную пропускную способность из расчета необходимости обеспечения для каждого подключаемого объекта образовательной организации, в соответствии с Заявками следующих параметров:

– находящиеся в городских поселениях – не менее 100 (ста) Мбит/с по направлению «от»/«к» образовательной организации;

– находящиеся в сельских поселениях – не менее 50 (пятидесяти) Мбит/с по направлению «от»/«к» образовательной организации;

– находящиеся в труднодоступных населенных пунктах, подключенные по спутниковым каналам связи – не менее 1 (одного) Мбит/с по направлению «от»/«к» образовательной организации.

Для объектов образовательных организаций, подключенных по спутниковой или иной технологии, отличной от волоконно-оптической линии

связи, допускается асимметричность канала связи.

5.2.6. Компонент «Предоставление доступа» должен обеспечивать доступ к сети «Интернет» и возможность доступа образовательной организации к ИС в соответствии с требованиями ТЗ.

5.2.7. Назначение Компонента «Предоставление доступа».

Компонент Услуг связи «Предоставление доступа» предназначен для организации подключения образовательной организации через Канал L2 к Точкам присоединения ЕСПД.

5.2.8. Требование к Компоненту «Предоставление доступа»:

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

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

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

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

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

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

– ВЧС для взаимодействия между образовательными организациями и централизованного доступа в сеть «Интернет», а также с возможностью доступа к ИС.

5.2.9. Требования к топологии сети:

1) должен организовать Точку (Точки) присоединения ЕСПД.

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

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

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

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

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

5.2.10. 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».

2) В ВЧС ЕСПД должны использоваться сети класса А из диапазона, разрешенного к применению в частных IP-сетях 10.0.0.0/8. Возможность использования иных сетей определяется Исполнителем по согласованию с Заказчиком.

3) Кроме основного адресного пространства, в виде исключения, могут

использоваться дополнительно диапазоны IP-сетей и отдельных адресов.

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

5.2.11. Требования к качеству обслуживания:

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

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

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

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

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

Примечания:

- При передаче данных через IP/MPLS сеть Исполнителя заголовки IP-пакетов меняться не должны.
- При превышении трафиком Класса 1 пропускной способности,

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

## 5.3. Компонент «Передача данных»

5.3.1. Требования к архитектуре Компонента «Передача данных».

Архитектура Компонента «Передача данных» приведена на Рисунок 2.

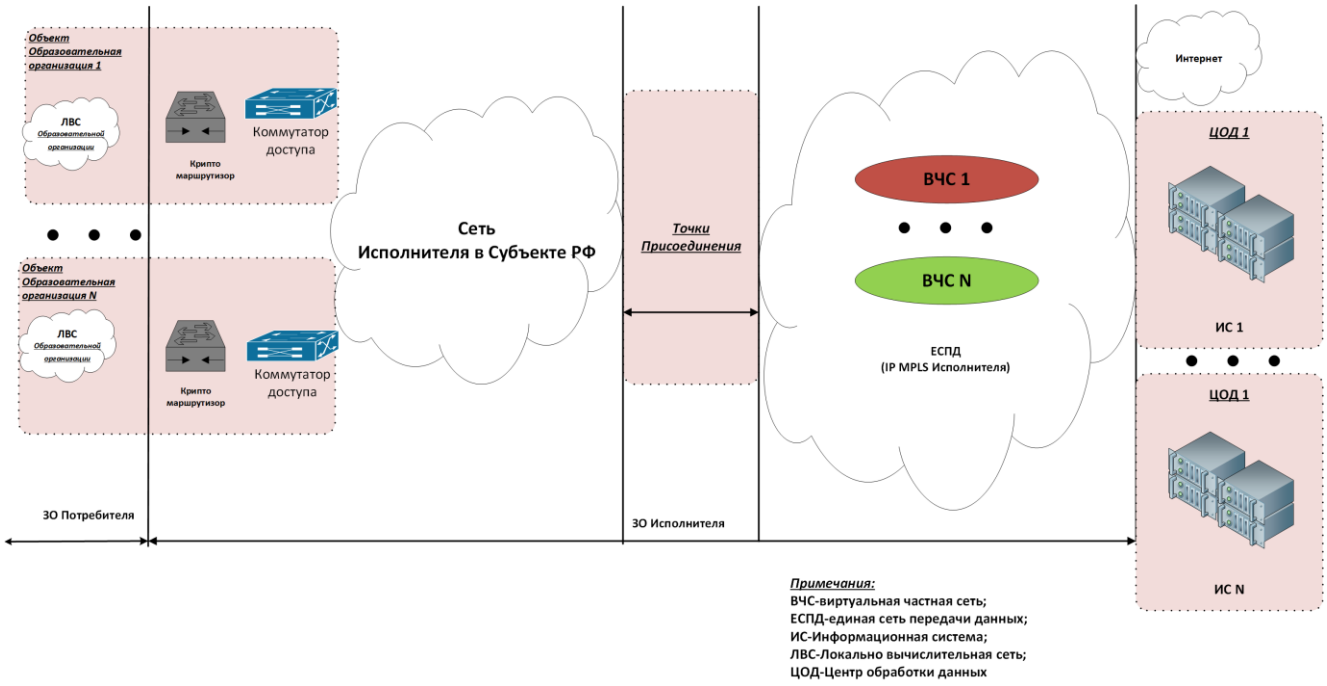



Рисунок 2 Архитектура Компонента «Передача данных».

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

5.3.2.1. Назначение Элемента ПД в ВЧС.

Элемент ПД в ВЧС предназначен для передачи данных посредством ЕСПД при осуществлении доступа образовательных организаций к ИС.

5.3.2.2. Требования к пропускной способности.

ПД в ВЧС должна осуществляться с учетом следующих скоростных

параметров подключения объектов образовательных организаций к ЕСПД, в соответствии с Заявками:

| | Пропускная способность канала от СЗО до Точки присоединения к ЕСПД |
|---|---|
| Для образовательных организаций, находящихся в городских поселениях | Не менее 100 Мбит/с |
| Для образовательных организаций, находящихся в сельских поселениях | Не менее 50 Мбит/с |
| Для образовательных организаций, подключаемых с использованием иных линий связи (в том числе спутниковых) в случае невозможности использования ВОЛС | Не менее 1 Мбит/с |

Для спутниковых каналов связи, организованных для объектов образовательных организаций с использованием максимальной (негарантированной) полосы пропускания (MIR), должна обеспечиваться минимальная гарантированная скорость доступа – 1 Мбит/с по направлению «от»/«к» образовательной организации.

5.3.2.3. Требования к качеству обслуживания.

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

2) В рамках модели с 3 классами обслуживания при передаче трафика для образовательной организации 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 IPпакетов меняться не должны;
- При превышении трафиком Класса 1 пропускной способности, установленной на порту для Класса 1, должен производиться сброс IPпакетов с качеством Класса 3; при превышении трафиком Класса 2, пропускной способности, установленной на порту для Класса 2, – сброс IP-пакетов с качеством Класса 3; при превышении трафиком Класса 3 пропускной способности порта – сброс IP-пакетов.

5.3.2.4. Требования к качеству Элемента ПД в ВЧС.

1) При оказании Элемента ПД в ВЧС Исполнитель должен осуществлять маршрутизацию IP-пакетов с данными Образовательной организации и обеспечивать передачу IP-пакетов с данными Образовательной организации к сетям и объектам, подключенным к ЕСПД;

2) Гарантии качества передачи IP-пакетов с данными Потребителя между 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 IPпакетов, не более | Задержка передачи IPпакетов 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 IPпакетов, в не более | Задержка передачи IPпакетов в одну сторону, не более | Вариация задержки, не более |
|---|---|---|---|
| Класс 1 | 0,2% | 100 мс | 50 мс |
| Класс 2 | 0,2% | 150 мс | не нормируется |
| Класс 3 | 5% | 200 мс | не нормируется |

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

5.3.3.1. Требования к Элементу ПД в «Интернет»:

1) Передача данных в сеть «Интернет» объекта Образовательной организации из ЕСПД должна осуществляться на ресурсах Исполнителя, с использованием частной адресации оборудования объекта Образовательной организации с использованием функции сетевой трансляции адресов (NAT) на сети Исполнителя;

2) Элемент ПД в «Интернет» должен быть централизован на уровне инфраструктуры Исполнителя в соответствии с требованиями ТЗ;

3) При оказании ПД в «Интернет» для образовательных организаций, указанных в Заявках, Исполнителем должен предоставляться выделенный симметричный дуплексный доступ к сети «Интернет» с пропускной способностью, соответствующей требованиям ТЗ. При этом для образовательных организаций, подключенных с использованием иных технологий, допускается предоставление асимметричного доступа;

4) Исполнитель для оказания ПД в «Интернет» должен зарезервировать достаточное количество внешних IPv4 адресов из зарегистрированного

за Исполнителем в базе данных RIPE NCC пространства IPv4 адресов. Объем (количество) IPv4 адресов Исполнителя должно быть достаточным для взаимодействия пользователей ЕСПД с информационными системами, размещенными в сети «Интернет», в т.ч. с системами, имеющими жесткие ограничения по количеству сессий, устанавливаемых с одного IPv4-адреса;

## 5.4. Компонент «Защита данных».

5.4.1. Назначение Компонента «Защита данных».

Компонент «Защита данных» предназначен для защиты данных, обрабатываемых и передаваемых при осуществлении доступа образовательных организаций к ИС, требующим защиты передачи данных и размещаемых в ЦОД Владельцев ИС.

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

– разместить оборудование криптографической защиты информации ЕСПД в ЦОД Владельцев ИС и обеспечить его подключение к ЕСПД самостоятельно и за свой счет.

– организовать криптографическую защиту передаваемых данных от пользователей образовательных организаций до ИС;

– организовать связность криптографических средств между собой в заданной конфигурации.

5.4.2. Требования к архитектуре Компонента.

Архитектура Компонента «Защита данных» определяется Исполнителем.

Для образовательных организаций Компонент должен обеспечивать защищенный доступ от образовательной организации до ИС в соответствии с требованиями ТЗ.

Компонент «Защита данных» должен использовать ЕСПД в качестве транспорта для защищаемых криптографическими средствами данных.

5.4.3. Управление Компонентом «Защита данных».

Для указанных Заказчиком образовательных организаций Исполнитель

должен осуществлять управление изменениями, которые могут включать изменения следующих параметров:

- интерфейса на оборудовании Исполнителя, к которому подключается оборудование образовательной организации;
- 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 для образовательной организации;
- приостановление или возобновление оказания услуги;
- оказание услуги для новых образовательных организаций по согласованию между Заказчиком и Исполнителем;
- прекращение оказания услуги;
- иные согласованные Исполнителем и Заказчиком параметры услуги.

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

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

5.4.5.1. Назначение Элемента «Криптозащита».

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

5.4.5.2. Требования к Элементу «Криптозащита»:

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

2) Шифрование должно обеспечивать возможность подключения образовательной организации к ИС, требующим защиты данных, размещаемых ЦОД;

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

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

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

6) Шифрование должно обеспечивать функцию защиты трафика при передаче персональных данных.

5.4.6. Средства криптозащиты информации должны выполнять:

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

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

5.4.7. Дополнительные требования к функциональности средств криптозащиты информации, установленных в образовательных организациях:

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

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

5.5.1. Компонент «Ограничение доступа к информации» должен обеспечивать блокирование доступа к ресурсам сети «Интернет» в соответствии с п. 2 ст. 5 Федерального закона от 29 декабря 2010 г. № 436-ФЗ «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.

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

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

Компонент не должен распространяться на АРМ административно-хозяйственного и педагогического состава образовательной организации, если иное не предусмотрено отдельными требованиями.

5.5.2. Требования к архитектуре Компонента:

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

- Предусмотреть возможность отключения Компонента на АРМ административно-хозяйственного и педагогического состава образовательной организации.

5.5.3. Управление Компонентом.

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

– IP адреса и подсети;
– правила фильтрации;
– ключевые слова и словосочетания для организации правил контент фильтрации;

– списки ресурсов ограниченного доступа;
– приостановление или возобновление оказания услуги;
– оказание услуги для новых объектов образовательных организаций по согласованию между Заказчиком и Исполнителем;
– прекращение оказания услуги и иные согласованные Исполнителем и Заказчиком параметры Компонента.

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

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

2) К смежным подсистемам относятся следующие:

– дополнительные источники списков фильтрации;
– ЦОД Исполнителя;

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

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

5.5.5.1. Требования к архитектуре Элемента.

Архитектура решений по контентной фильтрации в рамках ЕСПД представлена на Рисунок 3.

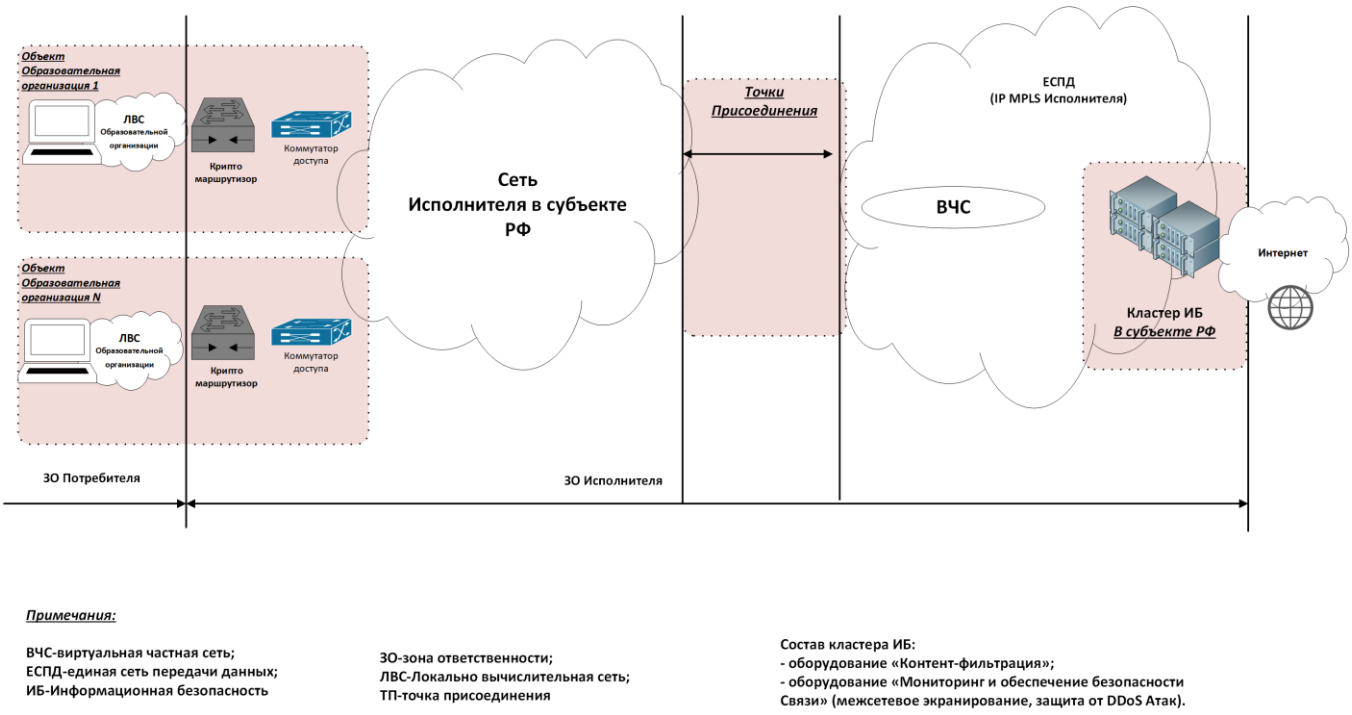



Рисунок 3 Общая архитектура решений по контентной фильтрации.

5.5.5.2. Требования к Элементу.

Контентная фильтрация должна поддерживать следующие функции:

– контроль веб-трафика по протоколам HTTP, HTTPS (в случае установки на клиентские устройства сертификата Исполнителя);

– блокировка злонамеренных интернет-ресурсов;

– поддержка черных и белых списков интернет-ресурсов;

– блокировка вредоносного ПО и нежелательной рекламы;

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

– принудительное включение безопасного поиска для поисковых систем в целях блокировки нежелательного контента;

– журналирование поисковых запросов пользователей на срок до 6 месяцев;

– блокировка приложений популярных социальных сетей, с возможностью открытия доступа, по запросу Потребителя в соответствии

с запрашиваемыми действиями для страниц каждой отдельно взятой социальной сети, при условии поддержки социальной сетью разграничения действий внутри сервиса;

– ограничение по объему использования веб-трафика;

– централизованное распространение политик безопасности на все узлы КФ;

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

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

– добавление сервисов в обход контентной фильтрации по запросу Заказчика.

Контентная фильтрация должна обеспечивать:

– гибкую фильтрацию HTTP трафика;

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

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

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

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

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

5.5.5.3. Требования к применяемым техническим решениям:

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

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

5.5.5.4. Требования к автоматизации.

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

– обеспечение и контроль доступа пользователей в сеть «Интернет» с фильтрацией входящего и исходящего Интернет-трафика по протоколам HTTP/HTTPS в случае установки на клиентские устройства сертификата Исполнителя;

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

– отключение функционала контроля доступа в сеть «Интернет» и фильтрации трафика сети «Интернет» для конкретных IP-адресов и с использованием аутентификации пользователей посредством ЕСИА;

– управление доступом пользователей к различным типам информации в сети «Интернет» (видео, аудио, изображения и т.д.);

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

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

–

– 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.

В Личном кабинете Исполнителем обеспечивается выполнение следующих функций:

– возможность доступа к Личному кабинету путем аутентификации с использованием ЕСИА работников образовательной организации, а также органов государственной власти, осуществляющих функции в сфере общего образования и среднего профессионального образования;

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

– возможность отслеживания статусов выполнения поданных заявок;

– возможность оценки качества исполнения поданных заявок;

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

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

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

5.6.1. Элемент «Мониторинг параметров качества предоставляемых услуг».

5.6.1.1. Требования к функционалу средств мониторинга и отчетности.

Средства мониторинга функционирования и формирования отчетности

должны обеспечивать возможность выполнения следующих функций:

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

2) Протоколирование действий пользователей и администраторов системы;

3) Формирование отчетности с предоставлением функциональности:

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

4) Сбор, формирование и отображение данных о статусе оказания Услуг связи, в том числе недоступности Услуг связи по причинам, находящимся в зоне ответственности Потребителя (электропитание в момент возникновения события, функция Dying gasp), а также по причинам в зоне ответственности Исполнителя (ППР, проблемы с канальной, сетевой частью как на объекте, так и на магистральной части) с глубиной хранения данных 12 месяцев;

5) Сбор, формирование и отображение данных по утилизации трафика на постоянной основе с интервалом снятия данных не реже одного раза в 10 минут. Данные снимаются по входящему и исходящему трафику (в Мбит/с), а также по объему входящего/исходящего потребления данных (в Мбайт) по

каждому объекту (протокол snmp) с глубиной хранения данных 12 месяцев с возможностью выгрузки данных за произвольно выбранный период;

6) Поддержка функционала по присвоению объекту признака, обозначающего необходимость увеличения пропускной способности канала связи;

7) Сбор, формирование и отображение данных по объему потребления трафика, в том числе суммарный объем потребления трафика за месяц и составление рейтинга потребления трафика за месяц;

8) Возможность присвоения объекту признака «стоп-фактор», находящегося в зоне ответственности пользователя (ремонт и другие работы на продолжительный период связанные с отключением услуги, но не приводящие к исключению объекта из заявки к Контракту) с глубиной хранения данных 12 месяцев;

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

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

и устойчивости функционирования сети связи общего пользования, а именно, в соответствии с постановлением Правительства Российской Федерации от 16 ноября 2020 г. № 1847 «Об утверждении перечня измерений, относящихся к сфере государственного регулирования обеспечения единства измерений»;

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

5.6.1.2. Требования к архитектуре Компонента.

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

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

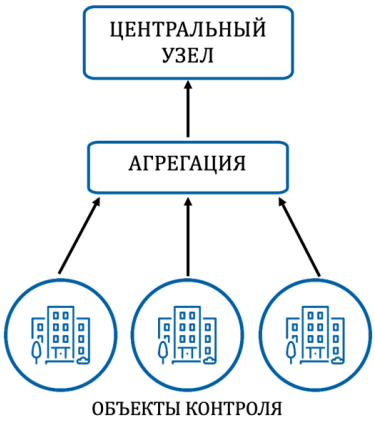



Рисунок 4 Общая архитектура Компонента «Мониторинг и обеспечение безопасности связи».

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

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

данных о работоспособности средств связи и соблюдению требуемого качества предоставления услуг связи не предусматривается.

5.6.1.3. Управление Компонентом.

Для указанных Заказчиком образовательных организаций 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 для образовательных организаций;
- приостановление или возобновление оказания мониторинга и обеспечения безопасности связи;
- Мониторинг и обеспечение безопасности связи для новых объектов образовательных организаций по согласованию между Заказчиком и Исполнителем;
- прекращение мониторинга и обеспечения безопасности связи;
- иные согласованные Исполнителем и Заказчиком параметры мониторинга и обеспечения безопасности связи.

5.6.1.4. Требования к дополнительному функционалу:

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

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

5.6.1.6. Требования к наличию отчетов.

Компонент должен обеспечивать по каждому объекту образовательной организации, в соответствии с Заявками, формирование в электронном виде по запросу уполномоченного представителя Заказчика и (или) в автоматическом режиме предопределенной (регламентированной) статистической и аналитической отчетности о качестве услуг связи:

— формирование периодических статистических и аналитических отчетов о качестве услуг связи, в том числе о периодах недоступности услуг связи по любым причинам за произвольный период времени, по предопределенным формам и их автоматизированную рассылку средствами электронной почты уполномоченным представителям Заказчика;

— формирование в электронном виде оперативных отчетов о качестве конкретной услуги связи для конкретного объекта, в том числе о периодах недоступности услуг связи по любым причинам за произвольный период времени, при самостоятельном обращении Заказчика к Компоненту;

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

5.6.2.1. Назначение Элемента.

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

5.6.2.2. Требования к Элементу:

1) элемент должен предоставляться для всех публичных IP сетей образовательных организаций;

2) должен проводиться анализ трафика следующих видов:

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

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

значений;

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

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

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

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

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

– характеристики Интернет-трафика (распределение по протоколам);

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

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

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

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

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

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

– атаки на переполнение каналов связи (Volumetric Attacks);

– атаки на сетевую инфраструктуру (State Exhaustion Attacks);

– атаки уровня приложений (Application Attacks).

2) Фильтрация трафика должна осуществляться по следующим критериям:

– по географическому признаку;

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

– протоколам;

– портам;

– с помощью регулярных выражений основных характеристик протоколов;

– с помощью регулярных выражений различных характеристик приложений;

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

– с отслеживанием соединений на наличие медленных атак.

3) Оборудование Исполнителя, обеспечивающее защиту от DoS/DDoS-атак, 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;

– 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-атак.

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

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

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

– вручную, путем обращения Потребителем в Службу технической поддержки;

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

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

5.6.3.1. Назначение Элемента.

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

5.6.3.2. Требования к Элементу:

1) Элемент должен обеспечивать:

– разграничение информационных потоков, сетевого взаимодействия между сегментами;

– блокировку запрещенных типов взаимодействий;

– журналирование или подсчет числа попыток осуществления запрещенных взаимодействий;

– блокировку обращений к известным серверам злоумышленников;

– поддержку функции выявления вредоносного трафика на основании сигнатур;

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

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

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

4) Выбор сертифицированных на соответствие требованиям по безопасности информации МСЭ, должен производиться с учетом совместимости с информационными технологиями и техническими средствами,

функций безопасности этих средств и особенностей их реализации, а также класса защищенности информационной системы и ЕСПД;

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) Защита на основе МСЭ должна реализовывать следующие возможности:

– фильтрация на основе сетевых адресов отправителя получателя;

– локальная сигнализация попыток нарушения правил фильтрации;

8) МСЭ должен быть использован для:

– ограничения или запрещения доступа хостов внутренней сети к сервисам внешней сети «Интернет»;

– ограничения доступа внешних пользователей к внутренним ресурсам сети Потребителя;

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

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

5.7.1. Назначение Компонента.

Компонент Услуг связи должен обеспечивать организацию канала связи от объектов образовательных организаций к Точкам присоединения ЕСПД по сети Исполнителя.

5.7.2. Требования к Компоненту:

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

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

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

Приоритетной технологией подключения объектов является ВОЛС.

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

3) Организованные каналы связи начинаются на оборудовании Исполнителя на объекте образовательной организации и заканчиваются в Точке присоединения ЕСПД;

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

5) Организованные каналы связи могут быть предоставлены в виде:

a. выделенных каналов для одного объекта образовательной организации;

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

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

прочих требований настоящего ТЗ;

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

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

9) Спутниковые каналы связи для объектов образовательных организаций могут быть организованы с использованием гарантированной полосы пропускания (CIR) или с максимальной (негарантированной) полосой пропускания (MIR) (в соответствии с технической возможностью оборудования спутниковой связи на Объекте), при этом должна обеспечиваться минимально допустимая пропускная способность, указанная в пункте 5.7.3 ТЗ.

5.7.3. Требования к пропускной способности.

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

Для образовательных организаций:

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

Для спутниковых каналов связи, организованных на объектах образовательных организаций с использованием максимальной (негарантированной) полосы пропускания (MIR), должна обеспечиваться минимальная гарантированная скорость доступа – 1 Мбит/с по направлению «от»/«к» образовательной организации.

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

5.8.1. Назначение Компонента.

Компонент должен обеспечивать передачу данных от образовательной организации к Точке (Точкам) присоединения ЕСПД.

5.8.2. Требования к пропускной способности.

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

Для образовательной организации

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

Для спутниковых каналов связи, организованных на объектах образовательных организаций с использованием максимальной (негарантированной) полосы пропускания (MIR), должна обеспечиваться минимальная гарантированная скорость доступа – 1 Мбит/с по направлению «от»/«к» образовательной организации.

5.8.2.1. Услуга по компоненту "Передача данных L2" может быть предоставлена Исполнителем с использованием каналов связи альтернативного оператора путем аренды соответствующих каналов связи или альтернативным оператором при наличии соответствующего соглашения между альтернативным оператором и Потребителем, а также при условии обеспечения Исполнителем доступа к ЕСПД из сети связи альтернативного оператора в интересах Потребителя.

5.8.3. Требования к качеству обслуживания.

В рамках модели с 3 классами обслуживания при передаче трафика между

образовательными организациями и узлом Исполнителя должна поддерживать:

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

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

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

Примечания:

- При передаче данных через канал связи заголовок 802.1p не должен изменяться.
- При превышении трафиком Класса 1 пропускной способности, установленной на порту для Класса 1, должен производиться сброс пакетов с качеством Класса 3; при превышении трафиком Класса 2, пропускной способности, установленной на порту для Класса 2, – сброс пакетов с качеством Класса 3; при превышении трафиком Класса 3 пропускной способности порта – сброс пакетов.
- Параметры качества передачи L2-пакетов через канал связи должны удовлетворять следующим требованиям:

*Гарантированные значения параметров качества передачи данных по каналам связи от образовательных организаций к Точкам присоединения ЕСПД, организованным по ВОЛС:*

| Тип трафика | Процент потерянных L2пакетов, не более | Задержка передачи L2пакетов в одну сторону, не более | Вариация задержки, не более |
|---|---|---|---|
| Класс 1 | 0,2% | 15 мс | 10 мс |
| Класс 2 | 0,2% | 20 мс | не нормируется |
| Класс 3 | 5% | 25 мс | не нормируется |

*Среднестатистические целевые значения параметров качества передачи данных по каналам связи от образовательных организаций к Точкам присоединения ЕСПД, организованным с использованием спутниковых линий связи:*

| Тип трафика | Процент потерянных L2пакетов, не более | Задержка передачи L2пакетов в одну сторону, не более | Вариация задержки, не более |
|---|---|---|---|
| Класс 1 | 0,5% | 500 мс | 50 мс |
| Класс 2 | 1% | 550 мс | не нормируется |
| Класс 3 | 5% | 600 мс | не нормируется |

*Среднестатистические целевые значения параметров качества передачи данных по каналам связи от образовательных организаций к Точкам присоединения ЕСПД, организованным по Иным технологиям*

| Тип трафика | Процент потерянных L2пакетов, не более | Задержка передачи L2пакетов в одну сторону, не более | Вариация задержки, не более |
|---|---|---|---|
| Класс 1 | 0,5% | 100 мс | 50 мс |
| Класс 2 | 1% | 200 мс | не нормируется |
| Класс 3 | 5% | 300 мс | не нормируется |

## 6. Порядок взаимодействия Сторон в рамках оказания Услуг связи

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

6.2. Состав заявки должен включать следующую информацию:

— Номер;

— Содержание;

— Состав компонентов;

— Параметры Услуг связи;

— Срок оказания Услуг связи;

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

— Адресный перечень объектов образовательных организаций.

Заявки (изменения к ранее направленным Заявкам) формируются Заказчиком в электронной форме и направляются в адрес Исполнителя в срок не менее чем за 30 рабочих дней до даты начала оказания Услуг связи, установленной Заявкой. Иные сроки, отличные от указанных выше в настоящем пункте ТЗ, могут применяться по согласованию между Заказчиком и Исполнителем.

6.3. Заявка должна быть подписана уполномоченным лицом Заказчика в электронной форме и направлена в адрес Исполнителя официальным письмом.

6.4. Исполнитель по итогам проработки возможности оказания услуги по Компоненту «Организация канала L2» в соответствии с Заявкой в срок не позднее 30 рабочих дней с даты получения Заявки вправе направить Заказчику уведомление о невозможности подключения объекта с требуемыми параметрами и необходимости внесения изменений в Заявку с указанием иной технологии и (или) параметров Услуги связи, в соответствии с которой (которыми) существует техническая возможность оказания Услуги связи для данного объекта (при наличии такой технической возможности).

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

6.6. При выявлении необходимости внесения изменений в Заявку Исполнитель в течение 30 календарных дней со дня получения соответствующей информации направляет в адрес Заказчика соответствующее уведомление, подписанное уполномоченных лицом.

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

6.8. При переезде образовательной организации на новый адрес размещения в *иной населенный пункт,* оказание Услуг связи Исполнителем по Компонентам «Передача данных» и «Передача данных L2» образовательной организации по новому адресу осуществляется на основании письменного обращения Заказчика и Заявки без Компонента «Организация канала L2» при условии наличия ВОЛС по новому адресу размещения образовательной организации.

При отсутствии ВОЛС по новому адресу размещения образовательной организации, Исполнителем подтверждается отсутствие ВОЛС в письменной форме в адрес Заказчика, и оказание Услуг связи по Компонентам «Передача данных» и «Передача данных L2» осуществляется Исполнителем с Компонентом «Организация канала L2» на основании Заявки.

## 7. Порядок контроля качества и приемки Услуг связи

7.1. Исполнитель предоставляет Заказчику:

7.1.1 На утверждение, не позднее **20 рабочих дней со дня подписания Контракта**:

1) Регламент технической поддержки при оказании Услуги связи;

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

7.2. В срок: - **не позднее 15 февраля 2027 года** Исполнитель направляет Заказчику документы в соответствии с п. 7.9 ТЗ по итогам оказания в соответствии с Заявками в рамках Контракта Услуг связи образовательным организациям, указанным в Заявках Заказчика;

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

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

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

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

7.4. Для объектов образовательных организаций, которым оказываются Услуги связи, наличие доступа к информационным системам и сети «Интернет» на объекте определяется Заказчиком посредством Компонента «Мониторинг и обеспечение безопасности связи». В срок, указанный в п. 7.2 ТЗ, Исполнитель предоставляет ежемесячные отчеты о функционировании:

1) Элемента «Мониторинг параметров качества предоставляемых услуг»;
2) Элемента «Защита от DDoS-атак»;
3) Элемента «Межсетевое экранирование».

7.5. В срок, указанный в п. 7.2 ТЗ, Исполнитель предоставляет отчет о функционировании Компонента «Защита данных».

7.6. Заказчик имеет право проводить выборочную проверку оказываемых Услуг связи. Выборочная проверка проводится на объектах в соответствии с Программой и методикой испытаний (Приложение № 2 к ТЗ).

7.7. По итогам проведения испытаний в рамках выборочной проверки составляются Протокол проведения тестирования Услуги связи (далее – Протокол) (по форме Приложения № 5 к ТЗ).

7.8. На основании Протокола проведения тестирования составляется Акт проверки оказания Услуг связи (по форме Приложения № 3 к ТЗ).

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

7.9.1. Исполнитель предоставляет Заказчику:

– Акты об оказании Услуг связи (по форме Приложения № 4 к ТЗ), подписанные Исполнителем и уполномоченным представителем образовательной организации. По письменному согласованию с Заказчиком Акты об оказании Услуг связи (по форме Приложения № 4 к ТЗ) могут быть подписаны Исполнителем и иным лицом, не являющимся руководителем образовательной организации, а именно: руководителем (уполномоченным представителем) государственного органа субъекта Российской Федерации, органа местного самоуправления;

– Сводные акты о прерывании в предоставлении Услуг связи;

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

7.9.2. Контроль оказания Услуг связи осуществляется Заказчиком на основании Сводных актов о прерывании в предоставлении Услуг связи и отчетов о функционировании Элемента «Мониторинг параметров качества предоставляемых услуг».

7.9.3. Документ о приемке подписывается Исполнителем и Заказчиком на основании предоставленных Исполнителем Актов об оказании Услуг связи, Сводных актов о прерываниях в предоставлении Услуг связи и Отчетов о функционировании Элемента «Мониторинг параметров качества предоставляемых услуг».

7.9.4. Оплата Услуг связи осуществляется за фактически оказанные

Услуги связи в соответствии с Заявками и Ценами единиц Услуги (Приложение № 2 к Контракту). При этом расчет стоимости фактически оказанных Услуги связи по компонентам Услуги связи «Передача данных» и «Передача данных L2» (далее – Услуги) осуществляется на основании Отчетов о функционировании Элемента «Мониторинг параметров качества предоставляемых услуг» согласно Ценам единиц Услуги (Приложение № 2 к Контракту), предусматривающим абонентскую систему оплаты из расчета за 1 календарный месяц. В случае, если Услуги связи фактически оказывались не полный календарный месяц, стоимость Услуг связи подлежит перерасчету по следующей формуле:

С = Т-((Т/Д1) х (Дн+Дпр)), где:

С – стоимость Услуги связи в рассчитываемом месяце;

Т – Цена единицы Услуги связи;

Д1 – количество календарных дней оказания Услуг связи в месяце;

Дн – количество дней, когда Услуги связи не оказывались (за исключением дней превышения времени недоступности Услуги при ее восстановлении (Дпр);

Дпр - количество дней превышения времени недоступности Услуги при ее восстановлении;

Дпр=В4/24 (округленное в большую сторону до целого натурального числа);

**В4** – время превышения допустимого времени простоя Услуги в месяц;

В4 = В2-В3;

**В2** – общее фактическое время перерыва в предоставлении Услуг связи в календарном месяце в рабочих часах, которое равняется времени недоступности Услуг связи без учета:

- работ на оборудовании Исполнителя, выполняемыми по запросу Заказчика;

- неисправностей оборудования Потребителя;

-действий Потребителей, вызванных в том числе отключением электропитания оборудования Исполнителя;

**В3** – допустимое время простоя услуги в месяц;

В3=(24*Д1)-0,98*(24*Д1);

В случае если В2 меньше или равно В3, Дпр приравняется к нулю.

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

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

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

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

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

где:

**Кд** – коэффициент доступности Услуги связи по объекту за календарный месяц, рассчитываемый по формуле:

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

**Д1** – количество календарных дней оказания Услуг связи в месяце;

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

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

- проведением плановых профилактических работ.

Исполнитель проводит технологические перерывы в порядке,

предусмотренном Регламентом технической поддержки при оказании Услуг связи, разработанным в соответствии с пунктом 7.1 ТЗ и утвержденным Заказчиком. Суммарное время технологических перерывов на объекте не должно превышать для любой Услуги связи 6 (шесть) часов в течение календарного месяца.

**В2** – общее фактическое время перерыва в предоставлении Услуг связи в календарном месяце в рабочих часах, которое равняется времени недоступности Услуг связи без учета:

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

Порядок открытия и закрытия инцидентов для расчета времени недоступности Услуг связи определяется в соответствии с Регламентом технической поддержки при оказании Услуг связи, разработанным в соответствии с пунктом 7.1 ТЗ и утвержденным Заказчиком. Время недоступности Услуг связи, рассчитанное в соответствии с Регламентом технической поддержки при оказании Услуг связи, и коэффициент доступности Услуг **Кд общий** определяются на основании Сводных актов о прерывании в предоставлении Услуг связи.

**Приложения**

1. Заявка на оказание Услуг связи (Форма);
2. Программа и методика испытаний;
3. Акт проверки оказания Услуг связи (Форма)
4. Акт об оказании Услуг связи за период с «___» ____202_ г. по «___»_____202_ г. (Форма);
5. Протокол проведения тестирования Услуг связи (Форма).

**от Заказчика:** **от Исполнителя:**

_____/Кривошеенко А.А./ _____/Котляров К.В./