Договор № ЕСПД/28680/26-01
об оказании услуг юридическому лицу, финансируемому из соответствующего бюджета

г. Нальчик «12» января 2026 г.

ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «РОСТЕЛЕКОМ» (ПАО «РОСТЕЛЕКОМ»), именуемое в дальнейшем **«Оператор»**, в лице Заместителя директора филиала – Директора по работе с корпоративным и государственным сегментами Кабардино-Балкарского филиала ПАО «Ростелеком» Бекишева Ахмеда Ратмировича, действующего на основании доверенности от 16.07.2025 № 0404/29/19/25, с одной стороны, и **Муниципальное казённое общеобразовательное учреждение «Средняя общеобразовательная школа № 21 с углубленным изучением отдельных предметов» городского округа Нальчик Кабардино-Балкарской республики**, именуемое в дальнейшем **«Абонент»**, в лице директора Казаковой Зухры Магаметовны, действующего на основании Устава, с другой стороны, заключили настоящий договор об оказании услуг юридическому лицу, финансируемому из соответствующего бюджета (далее – «Договор») о нижеследующем:

1. Предмет Договора

1.1. Настоящий Договор заключен на основании п. 4 ч. 1 ст. 93 Федерального закона от 05.04.2013 № 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

1.2. Идентификационный код закупки 263071103829807260100100020000000000.

1.3. В соответствии с условиями настоящего Договора Оператор обязуется оказывать Абоненту услуги, описанные в Приложениях к настоящему Договору (далее – Услуги), а Абонент обязуется принимать и оплачивать оказываемые ему Услуги. Состав, перечень и стоимость Услуг, а также дополнительные права и обязанности Сторон, определяются Приложениями к настоящему Договору.

1.4. Цена настоящего Договора составляет: **217680 руб. (двести семнадцать тысяч шестьсот восемьдесят рублей 00 копеек)**, в том числе НДС в соответствии с действующим законодательством Российской Федерации.

Цена Договора является твердой и определяется на весь срок исполнения Договора.

1.4.1. Источник финансирования: местный бюджет.

1.5. Изменение цены Договора возможно по соглашению сторон в случаях, предусмотренных ст. 95 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

2. Права и обязанности Сторон

2.1. Оператор обязан:

2.1.1. Оказывать Абоненту Услуги в соответствии с законодательством РФ, лицензиями, настоящим Договором.

2.1.2. Вести учет оказываемых Услуг.

2.1.3. Оформлять и направлять Акты начала оказания услуг и/или Акты выполненных работ (оказанных услуг) Абоненту (далее совместно именуемые – Акты).

2.1.4. Оповещать Абонента о проведении ремонтно-настроечных и профилактических работах на сетях любыми доступными способами, в т.ч. путем размещения информации на сайте https://espd.wifi.rt.ru.

2.2. Оператор имеет право:

2.2.1. В одностороннем порядке путем направления Абоненту письменного уведомления вносить изменения в п. 7.1 настоящего Договора.

2.2.2. Требовать от Абонента исполнения обязательств по настоящему Договору, в т.ч. не исполненных перед Оператором денежных обязательств.

2.2.3. Приостанавливать оказание Услуг при возникновении чрезвычайных ситуаций природного и техногенного характера, в соответствии со ст. 66 Федерального закона от 07.07.2003 № 126-ФЗ «О связи».
2.2.4. Приостанавливать оказание Услуг в случае нарушения Абонентом требований, связанных с оказанием этих Услуг и установленных Федеральным законом от 07.07.2003 № 126-ФЗ «О связи», иными нормативными правовыми актами и настоящим Контрактом, в том числе нарушения сроков оплаты оказанных Абоненту Услуг, до устранения нарушения или предоставления документов, подтверждающих оплату Оператору стоимости оказанных Услуг. Приостановление оказания услуг связи, услуг присоединения и услуг по пропуску трафика, производится Оператором с письменного согласия Абонента или по решению суда. При этом сохраняется доступ к сети связи.
2.2.5. Требовать возмещения Абонентом убытков (в виде упущенной выгоды) за период вынужденного приостановления оказания услуги, возникшего из-за повреждений оборудования Оператора по вине Абонента, из расчета тарифа за соответствующую услугу пропорционально времени приостановления ее оказания.
2.2.6. Предоставлять (направлять) Абоненту информацию об услугах Оператора, способах и условиях их предоставления и заказа в соответствии с требованиями действующего законодательства.
2.2.7. Оператор продолжает оказывать услуги связи в полном объеме после окончания срока действия Договора до момента, когда Абонент в письменной форме предоставит согласие на прекращение оказания услуг в порядке, указанном в п. 2.3.11 Договора.
2.3. Абонент обязан:
2.3.1. Пользоваться услугами исключительно в пределах установленных лимитов бюджетных обязательств. Оплачивать Услуги в полном объеме и в сроки в соответствии с настоящим Договором. Осуществлять контроль над расходованием денежных средств, выделенных на Услуги, в пределах лимитов бюджетных обязательств.
В случае возникновения риска увеличения цены Договора, указанной в п. 1.4 Договора, в связи с увеличением объема потребляемых услуг инициировать заключение дополнительного соглашения или расторжение Договора по соглашению Сторон. При несоблюдении условий настоящего пункта оплачивать фактически оказанные услуги, потребленные сверх лимитов бюджетных обязательств, на основании выставленных Оператором счетов.
2.3.2. Письменно уведомлять Оператора об изменении наименования юридического лица, юридического и почтового адреса Абонента в срок, не превышающий 30 (тридцати) календарных дней с даты введения в действие соответствующих изменений. Письменно уведомить Оператора об изменении адреса доставки счетов, счетов-фактур, Актов и банковских реквизитов Абонента в течение 5 (пяти) календарных дней с момента изменения. Уведомление производится по реквизитам, указанным в разделе 5 Договора. Уведомление должно быть подписано лицом, уполномоченным на внесение изменений в Договор.
2.3.3. Извещать Оператора обо всех случаях перерывов связи в предоставляемых Абоненту Услугах.
2.3.4. Принимать Услуги и возвращать Оператору подписанные со своей стороны уполномоченными лицами оригиналы Актов в течение 10 (десяти) календарных дней с момента получения. В том случае если в течение 10 (десяти) календарных дней со дня начала оказания Услуг и (или) окончания Отчетного периода (месяц оказания Услуг) Абонент не предоставляет Оператору письменного мотивированного отказа в признании надлежащего исполнения обязательств Оператором, Абонент считается согласившимся с датой, объемом и качеством Услуг, указанных в Актах. При этом, Оператор вправе требовать оплату счетов на суммы, указанные в Актах, а Абонент обязан оплачивать эти счета в соответствии с условиями Договора.
2.3.5. В рабочее время обеспечить беспрепятственный доступ работников Оператора, предъявивших соответствующее удостоверение, для выполнения работ, необходимых во исполнение настоящего Договора, а также для проведения осмотра, ремонта и технического обслуживания средств, сооружений, линий связи в помещениях, находящихся во владении и (или)

пользовании Абонента. В случае необходимости проведения работ по организации абонентской линии обеспечить получение необходимых разрешений и согласований от владельца территории (помещения), на которой расположено оборудование Оператора и (или) оборудование Абонента, на проведение работ по прокладке кабеля, строительству кабельной канализации и организации кабельного ввода, а также по размещению и электропитанию оборудования Оператора.
2.3.6. В случае одностороннего полного (частичного) отказа от Услуг по настоящему Договору письменно уведомить об этом Оператора, а также оплатить Оператору фактически понесенные расходы. Оплата должна быть произведена в течение 10 (десяти) рабочих дней с момента выставления счета Оператором.
2.3.7. Не допускать самовольного подключения к сети пользовательских (оконечных) устройств и иного оконечного оборудования, подключения к другим абонентским линиям.
2.3.8. Не допускать использования средств связи для преднамеренного создания другим абонентам условий, затрудняющих пользование услугами связи, а также создания помех для нормального функционирования сети связи.
2.3.9. Не использовать пользовательское (оконечное) устройство и (или) выделенный абонентский номер для оказания услуг связи третьим лицам, в том числе путем организации шлюзов для доступа к сети связи, IP-телефонии и т.п.
2.3.10. Содержать в исправном состоянии абонентскую линию и пользовательское (оконечное) оборудование, находящиеся в помещении Абонента, а также соблюдать правила эксплуатации этого оборудования.
2.3.11. В течение 5 (пяти) рабочих дней с даты получения запроса Оператора о подтверждении факта оказания услуг после истечения срока действия настоящего Договора, направленного в порядке исполнения абз. 3 п. 4 ст. 51.1 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», направляет Оператору подтверждение факта оказания услуг и/или согласие на приостановление/прекращение оказания Услуг по настоящему Договору.
2.3.12. Оплатить услуги связи, оказанные после истечения срока действия Договора в соответствии с п. 2.2.8 Договора, в сроки, указанные в Договоре, во внесудебном порядке с учетом положений п. 2.3.11 Договора в части подтверждения факта оказания Услуг.

2.4. Абонент имеет право:

2.4.1. Получать от Оператора информацию, необходимую для исполнения настоящего Договора, в том числе информацию о реквизитах Оператора, режиме работы, тарифах и оказываемых Услугах, о состоянии лицевого счета Абонента.
2.4.2. Требовать устранения неисправностей, препятствующих пользованию Услугами, в сроки, установленные действующими нормативными актами.
2.4.3. Запрашивать у Оператора направление в адрес Абонента Актов оказанных услуг.

3. Стоимость услуг, порядок расчетов

3.1. Стоимость Услуг, оказываемых Абоненту Оператором, определяется в соответствии с условиями Договора. Сумма к оплате за Услуги определяется с учетом стоимости и объема оказанных Услуг.
3.2. При изменении цены Договора по основаниям, указанным в п. 1.5 Договора, Абонент обязан подписать с Оператором Дополнительное соглашение о соответствующих изменениях.
3.3. Расчетный период устанавливается с первого до последнего числа (включительно) срока оказания Оператором Услуг, подлежащих оплате.
3.4. Оператор выставляет Абоненту счет, счет-фактуру, Акт выполненных работ (оказанных услуг), а также отчетные документы, предусмотренные приложениями к Договору, в течение 60 (шестидесяти) рабочих дней с даты окончания Расчетного периода. В Акте выполненных работ (оказанных услуг) и счет-фактуре Оператор заполняет графу единица измерения в соответствии с единицей, указанной в Приложениях к настоящему Договору. В случае невозможности указать в Акте выполненных работ (оказанных услуг) и счет-фактуре фактическую единицу измерения в связи с технологическими особенностями проставляется прочерк и данный вид работ (оказываемых услуг) заполняется в денежном измерении.
3.5. Оплата Услуг производится путем безналичных расчетов не позднее 10 (десяти) рабочих дней

с даты подписания Абонентом документа о приемке оказанных Услуг, указанного в п. 3.4 Договора.
3.6. Утеря, неполучение Абонентом выставленного Оператором счета, счетов-фактур и Актов, в т.ч. в связи с невыполнением условий, предусмотренных п. 2.3.2 настоящего Договора, не освобождает Абонента от обязанности своевременной оплаты Услуг.
3.7. Выставление счета-фактуры Оператором Абоненту производится в соответствии с налоговым законодательством РФ.
3.8. Стороны могут осуществлять сверку расчётов по Договору с оформлением двустороннего акта сверки расчётов по мере необходимости.
В случае направления акта сверки расчетов по электронной почте, такой акт будет признаваться Сторонами в качестве документа, составленного в письменной форме.
Акт сверки расчётов составляется заинтересованной Стороной подписывается уполномоченным представителем такой Стороны. Сторона-инициатор сверки направляет в адрес Стороны-получателя акт сверки расчётов.
Если Сторона-получатель не согласна с актом сверки расчетов, она направляет Стороне-инициатору свои письменные мотивированные возражения по поводу достоверности содержащейся в акте сверки расчётов информации. Если в течение 10 (десяти) рабочих дней со дня получения акта сверки расчётов Сторона-получатель не направит в адрес Стороны-инициатора письменные мотивированные возражения по поводу достоверности содержащейся в нем информации, акт сверки расчётов считается признанным Стороной-получателем в редакции Стороны-инициатора.
Стороны признают равную юридическую силу собственноручной подписи и факсимильной подписи, воспроизведенных с помощью средств механического или иного копирования на актах сверки расчётов к настоящему Договору.

4. Ответственность Сторон. Условия изменения и расторжения Договора. Прочие условия.

4.1. За неисполнение или ненадлежащее исполнение обязательств, установленных Договором, Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации (в том числе в соответствии с постановлением Правительства Российской Федерации от 30 августа 2017 г. № 1042) и условиями Договора.
4.2. В случае просрочки исполнения Абонентом обязательств, предусмотренных Договором, а также в иных случаях неисполнения или ненадлежащего исполнения Абонентом обязательств, предусмотренных Договором, Оператор вправе потребовать уплаты неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Договором, начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства. Такая пеня устанавливается Договором в размере 1/300 (одной трехсотой) действующей на дату уплаты пеней ключевой ставки Центрального банка Российской Федерации от неуплаченной в срок суммы. Штрафы начисляются за ненадлежащее исполнение Абонентом обязательств, предусмотренных Договором, за исключением просрочки исполнения обязательств, предусмотренных Договором. Размер штрафа устанавливается Договором в виде суммы, определенной в порядке, установленном Правительством Российской Федерации.
4.3. За каждый факт неисполнения Абонентом обязательств, предусмотренных Договором, за исключением просрочки исполнения обязательств, предусмотренных Договором, устанавливается штраф в размере 1 000 рублей.
4.4. Общая сумма начисленных штрафов за ненадлежащее исполнение Абонентом обязательств, предусмотренных Договором, не может превышать цену Договора.
4.5. Пеня начисляется за каждый день просрочки исполнения Оператором обязательства, предусмотренного Договором, начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства, и устанавливается Договором в размере 1/300 (одной трехсотой) действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены Договора, уменьшенной на сумму, пропорциональную объему обязательств,

предусмотренных Договором и фактически исполненных Оператором.
4.6. Штрафы начисляются за неисполнение или ненадлежащее исполнение Оператором обязательств, предусмотренных Договором, за исключением просрочки исполнения Оператором обязательств (в том числе гарантийного обязательства), предусмотренных Договором. Размер штрафа устанавливается Договором в порядке, установленном Правительством Российской Федерации. Размеры штрафов устанавливаются настоящим Договором в следующем порядке:
4.6.1. За каждый факт неисполнения или ненадлежащего исполнения Оператором обязательств, предусмотренных Договором, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Договором, устанавливается штраф в размере 10 процентов цены Договора (этапа).
4.6.2. За каждый факт неисполнения или ненадлежащего исполнения Оператором обязательства, предусмотренного Договором, которое не имеет стоимостного выражения, устанавливается штраф в размере 1 000 рублей.
4.7. Общая сумма начисленных штрафов за неисполнение или ненадлежащее исполнение Оператором обязательств, предусмотренных Договором, не может превышать цену Договора.
4.8. Сторона Договора освобождается от уплаты неустойки (штрафа, пени) если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного Договором, произошло вследствие непреодолимой силы или по вине другой Стороны.
4.9. Оператор не несет ответственности за содержание информации, передаваемой Абонентом по сетям электросвязи.
4.10. Все споры и разногласия, которые могут возникнуть из настоящего Договора или в связи с ним, Стороны рассматривают предварительно в претензионном порядке. Срок рассмотрения ответа на письменную претензию – 30 (тридцать) календарных дней с момента ее получения.
В случае если споры и разногласия не урегулированы в претензионном порядке в сроки, определенные в настоящем пункте, каждая из Сторон вправе обратиться в Арбитражный суд по месту нахождения ответчика с иском о разрешении спора.
4.11. Подписанием Договора Абонент подтверждает своё согласие со всеми его условиями, дает согласие на размещение оборудования связи Оператора в помещениях Абонента, а также то, что до него в понятной, доступной форме и в полном объеме доведены сведения об основных потребительских свойствах предоставляемых Оператором услуг, цены/тарифы на услуги, тарификация соединений, порядок и сроки расчетов, правила и условия оказания и использования услуг, информация об Операторе, территория обслуживания и иная необходимая информация, в т.ч. предусмотренная п. 17 Правил оказания телематических услуг связи (утв. постановлением Правительства РФ № 2607 от 31.12.2021) и п. 16 Правил оказания услуг связи по передаче данных (утв. постановлением Правительства РФ № 2606 от 31.12.2021).
4.12. Все изменения и дополнения к настоящему Договору действительны, если они оформлены в письменной форме и подписаны обеими Сторонами, за исключением изменений и дополнений, осуществляемых Сторонами в одностороннем порядке в соответствии с настоящим Договором или законодательством РФ. Изменения и дополнения к настоящему Договору вносятся путем подписания Дополнительных соглашений к настоящему Договору.
4.13. Внесение изменений в настоящий Договор в части изменения перечня Услуг производится Оператором по письменной заявке Абонента, с обязательным оформлением впоследствии соответствующих Приложений к настоящему Договору.
4.14. Настоящий Договор вступает в силу с даты его подписания Сторонами и действует до выполнения сторонами обязательств. Условия настоящего Договора распространяются на отношения Сторон, возникшие с 1.01.2026. **Срок оказания Услуг: с 1.01.2026 по 31.12.2026.**
4.15. Досрочное расторжение Договора допускается по соглашению сторон, по решению суда, а в случае одностороннего отказа Абонента от исполнения Договора в соответствии с гражданским законодательством.
4.16. Договор составлен в 2 экземплярах, подписанных уполномоченными лицами Сторон.

5. Адреса и способы доставки расчетно-платежных документов (РПД) и уведомлений.

Абонент соглашается получать от Оператора РПД (счет, счет-фактура, Акт выполненных работ (оказанных услуг) и письменные уведомления, подписанные усиленной квалифицированной электронной подписью по телекоммуникационным каналам связи через оператора электронного документооборота. При этом, электронный документ, подписанный электронной подписью, признается документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

5.1. Способ доставки оригиналов РПД

Электронный документооборот:

☐ АО «ПФ» СКБ Контур»

☒ ООО «Такском»

Абонент согласен на получение расчетных документов по выбранному им способу доставки.

5.2. Способ обмена письменными уведомлениями:

Надлежащим уведомлением Сторон считается доставка уведомлений одним из следующих способов: ЭДО, почтовой связью или курьером, направление на адрес электронной почты, указанный в Разделе 7 настоящего Договора.

6. Все Приложения, Дополнительные соглашения к настоящему Договору являются его неотъемлемой частью.

7. Адреса и реквизиты Сторон:

7.1. Оператор:

ПАО «Ростелеком»

Юридический адрес:
191167, Г.САНКТ-ПЕТЕРБУРГ, ВН. ТЕР. Г. МУНИЦИПАЛЬНЫЙ ОКРУГ СМОЛЬНИНСКОЕ, НАБ. СИНОПСКАЯ, Д. 14, ЛИТЕРА А

ИНН 7707049388 КПП 784201001

Телефон: 8-800-200-30-00

Сайт: www.rt.ru

Кабардино-Балкарский филиал ПАО "Ростелеком"

Почтовый адрес:
360001, Кабардино-Балкарская Республика, город Нальчик, проспект Кулиева, дом 14

ИНН 7707049388 КПП 616743001

Банковские реквизиты:

Наименование банка:
Краснодарское отделение № 8619 ПАО Сбербанк г. Краснодар

БИК 040349602

р/с 40702810430020102244

к/с 30101810100000000602

7.2. Абонент:

Муниципальное казённое общеобразовательное учреждение «Средняя общеобразовательная школа № 21 с углубленным изучением отдельных предметов» городского округа Нальчик Кабардино-Балкарской республики

Юридический адрес:360009, КБР, г.Нальчик, ул. Тимирязева,7

Почтовый адрес: 360009, КБР, г.Нальчик, ул. Тимирязева,7

ИНН 0711038298 КПП 072601001

Банковские реквизиты:

Наименование банка: УФК ПО КБР

БИК (БИК ТОФК) 018327106

Р/С (Казначейский счет) 03231643837010000400

К/С (ЕКС ТОФК) 40102810145370000070

ОКТМО 83701000

ОКПО 34629028

ОКВЭД 85.14

ОГРН 1020700750333

ОКПО	17514186
ОКВЭД	61.10
ОГРН	1027700198767

От Оператора:

Заместитель директора филиала – Директор по работе с корпоративным и государственным сегментами Кабардино-Балкарского филиала ПАО «Ростелеком»

_____ А.Р. Бекишев
(подпись) (расшифровка подписи)

От Абонента:

Директор муниципального казённого общеобразовательного учреждения «Средняя общеобразовательная школа № 21 с углубленным изучением отдельных предметов» городского округа Нальчик Кабардино-Балкарской республики

_____ З.М.Казакова
(подпись) (расшифровка подписи)

Приложение к Договору

Бланк заказа № 1
к договору № ЕСПД/28680/26-01 об оказании услуг юридическому лицу, финансируемому из соответствующего бюджета

Состав заказа

№	Тип продукта	ЛС
1	Услуга «Единая сеть передачи данных»	
2	Услуга «Предоставление частной виртуальной сети»	

[X] **Услуга «Единая сеть передачи данных»** Тип действия [X] подключение [ ] изменение (к бланку заказа № _____ от _____)

Лицевой счет

Система оплаты: кредитная

№	Адрес предоставления услуги	Технология доступа	Тарифный план	Скорость до, Мб/с	Ежемесячный тариф по услуге (без НДС)	Ежемесячный тариф по услуге (с НДС)	Старт тарификации	Планируемая дата обеспечения доступа к услуге не позднее:
28680	Кабардино-Балкарская Республика, г. Нальчик, ул. Тимирязево, 7	ВОЛС	Единая сеть передачи данных 100	100	7836,07	9560,00	01.01.2026	-

[X] **Услуга «Предоставление частной виртуальной сети»** Тип действия [X] подключение [ ] изменение (к бланку заказа № _____ от _____)

Лицевой счет

Система оплаты: кредитная

№	Адрес предоставления услуги	Технология доступа	Тарифный план	Скорость до, Мб/с	Ежемесячный тариф по услуге (без НДС)	Ежемесячный тариф по услуге (с НДС)	Старт тарификации	Планируемая дата обеспечения доступа к услуге не позднее:
28680	Кабардино-Балкарская Республика, г. Нальчик, ул. Тимирязево, 7	ВОЛС	Тарифный план 85.2.100	100	7032,79	8580,00	01.01.2026	-

От Оператора:

Заместитель директора филиала – Директор по работе с корпоративным и государственным сегментами Кабардино-Балкарского филиала ПАО «Ростелеком»

_____ А.Р. Бекишев
(подпись) (расшифровка подписи)

От Абонента:

Директор муниципального казённого общеобразовательного учреждения «Средняя общеобразовательная школа № 21 с углубленным изучением отдельных предметов» городского округа Нальчик Кабардино-Балкарской республики

_____ З.М.Казакова
(подпись) (расшифровка подписи)

Приложение
к договору об оказании услуг юридическому лицу,
финансируемому из соответствующего бюджета,

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на оказание услуг «Единая сеть передачи данных», услуг по предоставлению частной виртуальной сети

1. Термины, определения и сокращения

1.1. В настоящем техническом задании используются следующие термины, определения и сокращения:

Термин	Определение
CE	Customer Edge Router, граничное устройство в локальной вычислительной сети объектов образовательных организаций, используемое для маршрутизации трафика из сети объекта образовательных организаций в сеть Оператора и обратно. Находится под управлением выделенного подразделения Оператора.
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 Оператора	Сетевая инфраструктура Оператора и привлекаемых Оператором субподрядчиков (соисполнителей), состоящая из расположенных на узлах Оператора и привлекаемых Оператором 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

Термин	Определение
	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).
MPLS	Multi Protocol Label Switching, технология коммутации пакетов с использованием меток.
MPLS сеть Оператора	Построенная по технологии MPLS сетевая инфраструктура Оператора и привлекаемых Оператором субподрядчиков (соисполнителей), включающая опорные маршрутизаторы (P), граничные маршрутизаторы (PE), соединяющие их магистральные каналы и иные средства связи.
RIPE NCC	Региональный Европейский Регистратор Интернет адресов.
SNMP	Simple Network Management Protocol, протокол сетевого управления.
Авария	Недоступность услуг Оператора, вызванная неисправностью оборудования, сети, инженерных систем и инфраструктуры Оператора или привлекаемых Оператором 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 Оператора
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.
ВОЛС	Волоконно-оптическая линия связи.
ВЧС	Виртуальная частная сеть, построенная на базе MPLS сети Оператора и привлекаемых Оператором субподрядчиков (соисполнителей), путем организации виртуальных каналов между портами на узлах доступа сети Оператора, к которым подключен объект образовательной организации, и обеспечивающая передачу различных типов трафика с гарантией

Термин	Определение
	параметров качества.
Доступность услуги	Отношение времени нахождения оказываемых услуг в рабочем состоянии к общей продолжительности интервала наблюдения, выраженное в процентах (доступность за расчетный 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) Оператора, 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).
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.
Канал L2	Канал связи от объекта образовательной организации, до Точки присоединения ЕСПД.
Класс трафика	Набор требований к эксплуатационным параметрам, соблюдаемым Оператором при передаче по сети применительно ко всем IP-пакетам, принадлежащим данному типу.
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.

Термин	Определение
Личный кабинет	Персональная страница для Потребителя, организованная на ресурсе сайта Оператора, 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.
Объект	Совокупность технических средств, средств вычислительной техники и программного обеспечения, расположенных по одному адресу.
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 Оператора.
Постоянный белый список	Перечень ресурсов в сети «Интернет», доступ к которым разрешен по запросам Потребителей и уполномоченных государственных органов на постоянной основе.
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».
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 Оператора обстоятельствам.
ТЗ	Настоящее техническое задание.
Точка присоединения ЕСПД	Средства связи, входящие в состав сети электросвязи Оператора, с помощью которых осуществляется подключение и доступ образовательной организации к ЕСПД.
Трафик	Совокупность IP-пакетов, переданных по сети передачи данных.
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. Услуги связи оказываются непрерывно, круглосуточно и ежедневно в соответствии с условиями ТЗ.

2.2. Оказание Услуг связи осуществляется в соответствии с Бланком заказа, являющимся неотъемлемой частью Договора.

2.3. Перечень Услуг связи включает в себя:

2.3.1. **Услуга «Единая сеть передачи данных»** (передача данных при осуществлении доступа к государственным, муниципальным, иным информационным системам и к сети «Интернет») (**Компонент «Передача данных»**) в составе услуг:

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

— обеспечение 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»**);

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

2.3.2. **Предоставление доступа к услуге «Единая сеть передачи данных»** (предоставление с использованием ЕСПД доступа к государственным, муниципальным, иным информационным системам и к сети «Интернет» (**Компонент «Предоставление доступа»**).

2.3.3. **Услуга по организации канала** (организации подключения к ЕСПД) (**Компонент «Организация канала L2»**).

2.3.4. **Услуга по предоставлению частной виртуальной сети** (передаче данных при осуществлении доступа к ЕСПД) (**Компонент «Передача данных L2»**).

2.4. 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.

2.5. Для оказания Услуг связи в составе ЕСПД организуются каналы передачи данных и Точки присоединения ЕСПД.

2.6. Оператор обеспечивает присоединение канала связи между образовательной организацией и ЕСПД в Точках присоединения ЕСПД.

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

2.8. 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».

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

2.10. Оператор обязан оказывать Услуги связи для образовательной организации без ограничения объема передачи (безлимитно).

2.11. Подключение Канала L2 от образовательной организации к Точке присоединения ЕСПД проводится силами Оператора.

2.12. Оператор предоставляет и устанавливает для объектов Абонента, присоединяемых (подключаемых) к ЕСПД, криптомаршрутизаторы. Установка криптомаршрутизаторов осуществляется в телекоммуникационные шкафы. В случае отсутствия на объекте образовательной организации телекоммуникационного шкафа Оператор осуществляет его установку.

2.13. Оператор в течение всего срока оказания Услуг связи обеспечивает за свой счет настройку CE для оказания Услуг связи, предусмотренных Договором, техническое обслуживание и ремонт оборудования, в том числе криптомаршрутизаторов, установленных Оператором в образовательной организации. При этом сроки и порядок выполнения регламентных и ремонтных работ устанавливаются Регламентом технической поддержки при оказании Услуги связи.

2.14. Требования к средствам маршрутизации:

2.14.1. 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.

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

2.15. Требования к технической поддержке при оказании Услуг связи:

2.15.1. В период оказания Услуг связи Оператор обязан осуществлять техническую поддержку Потребителей (далее – Техническая поддержка) по вопросам оказания Услуг связи в соответствии с Единым регламентом технической поддержки при оказании услуг связи с использованием единой сети передачи данных в рамках исполнения контрактов, заключенных ПАО «Ростелеком» с образовательными организациями, размещенным на сайте https://espd.wifi.rt.ru/docs/regulation_single.pdf.

2.15.2. 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, Оператор использует ресурс в сети «Интернет» https://espd.wifi.rt.ru, размещает на нем инструкции и дополнительные материалы для Потребителей, а также Личный кабинет.

2.15.3. Техническая поддержка должна осуществляться круглосуточно и ежедневно в соответствии с Регламентом технической поддержки при оказании Услуги связи.

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

– по единому бесплатному контактному номеру телефона 8 800-301-34-14;

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

– посредством Личного кабинета https://espd.wifi.rt.ru/cabinet;

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

2.15.5. 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.

2.15.6. 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);

2-ой приоритет – Высокий:

– 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 Оператора и иных работ, требующих выезда в образовательную организацию, нормативные сроки решения инцидента увеличиваются на 48 часов. Указано время для восстановительных работ инфраструктуры Оператора, 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 Оператора, замены оборудования Оператора 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 Абонента в срок не менее трех рабочих дней до времени проведения работ;
- работа на оборудовании Оператора 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 Оператором обязательств в рамках ТЗ.

3. Состав Услуг связи

Оказание Оператором 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.

Оператор 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 Оператора;
– параметры качества передачи IP-пакетов и Ethernet-кадров для образовательной организации в зоне ответственности Оператора;
– параметры качества передачи IP-пакетов для образовательной организации в зоне ответственности Оператора;
– приостановление или возобновление оказания Услуг связи;
– прекращение оказания Услуг связи;
– иные согласованные Абонентом и Оператором 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*.

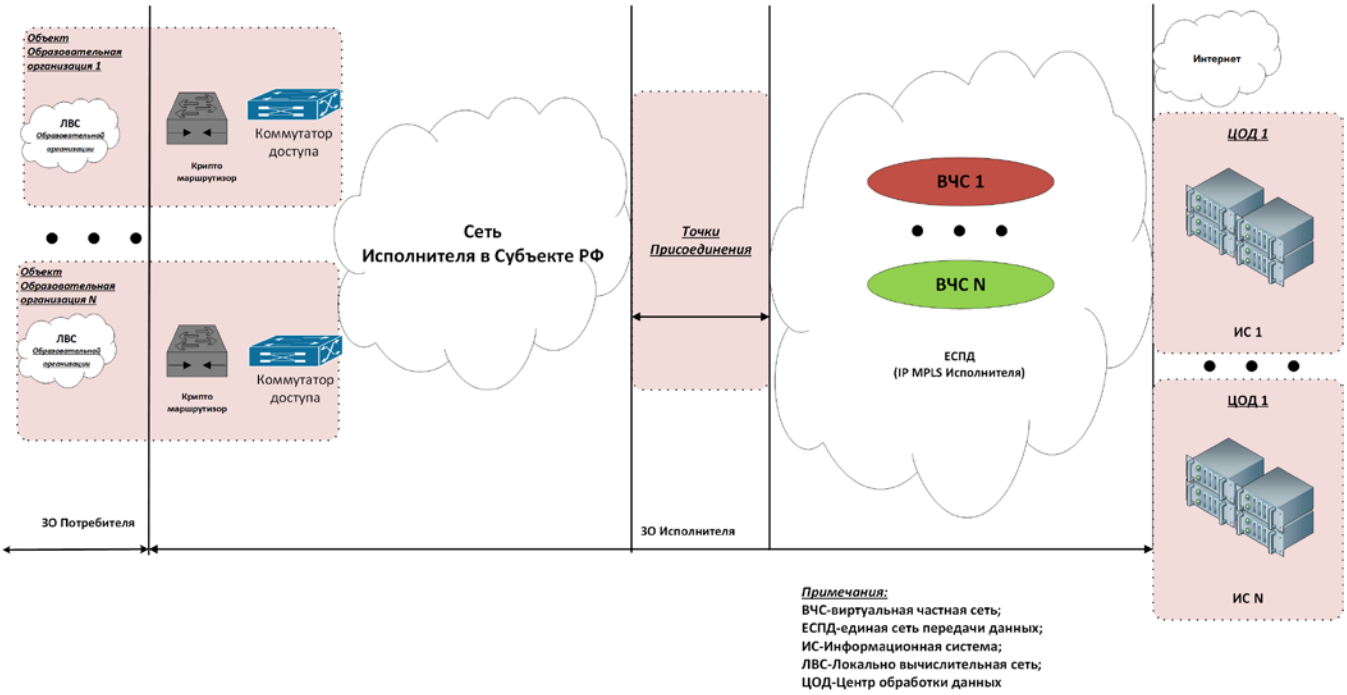


Рисунок 1 Архитектура Компонента "Предоставление доступа"

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».

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

– интерфейс на оборудовании Оператора, 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 Оператора;
– параметры качества передачи IP-пакетов и Ethernet кадров для образовательных организаций в зоне ответственности Оператора;
– приостановление или возобновление оказания Услуги 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 Оператора 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 Оператора и использующую собственные каналы связи Оператора, 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) Оператор 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) ЕСПД должна обладать возможностью организации следующих типов связей для ВЧС:

– «каждый с каждым» (Full mesh) – между любой парой CE пакет проходит по оптимальному с точки зрения сети Оператора 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 Абонент;

– «произвольная связность» – другие варианты топологии виртуальной частной сети, необходимые Абоненту; 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.

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. Пересечение адресных пространств исключается использованием легитимных (выданных централизованно Оператором) адресных пулов.

5.2.11. Требования к качеству обслуживания:

1) ЕСПД должна предоставлять как минимум 3 класса качества обслуживания трафика модели DiffServ.

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 Оператора, 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 Оператора 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*.

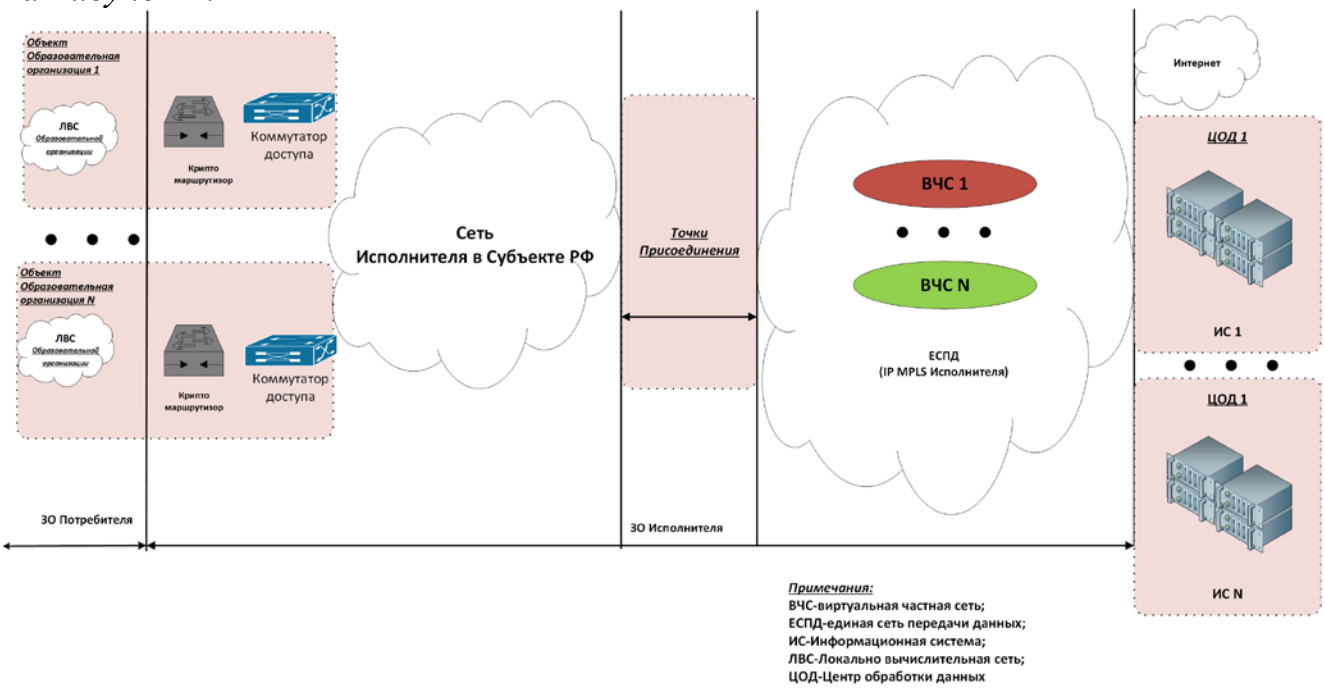


Рисунок 2 Архитектура Компонента «Передача данных».

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.

Пропускная способность канала от СЗО до Точки присоединения к ЕСПД определяется в соответствии с Бланком заказа.

5.3.2.3. Требования к качеству обслуживания.

1) Элемент ПД в ВЧС должен предоставлять как минимум 3 класса качества обслуживания трафика модели DiffServ.

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 Оператора, 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 Оператора заголовки IP-пакетов меняться не должны;
- При превышении трафиком Класса 1 пропускной способности, установленной на порту для Класса 1, должен производиться сброс IP-пакетов с качеством Класса 3; при превышении трафиком Класса 2, пропускной способности, установленной на порту для Класса 2, –

сброс IP-пакетов с качеством Класса 3; при превышении трафиком Класса 3 пропускной способности порта – сброс IP-пакетов.

5.3.2.4. Требования к качеству Элемента ПД в ВЧС.

1) При оказании Элемента ПД в ВЧС Оператор 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 IP-пакетов, не более	Задержка передачи IP-пакетов в одну сторону, не более	Вариация задержки, не более
Класс 1	0,2%	75 мс	50 мс
Класс 2	0,2%	100 мс	не нормируется
Класс 3	5%	125 мс	не нормируется

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

Тип трафика	Процент потерянных IP-пакетов, в не более	Задержка передачи IP-пакетов в одну сторону, не более	Вариация задержки, не более
Класс 1	0,2%	100 мс	50 мс
Класс 2	0,2%	150 мс	не нормируется
Класс 3	5%	200 мс	не нормируется

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

5.3.3.1. Требования к Элементу ПД в «Интернет»:

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

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

3) При оказании ПД в «Интернет» Оператором 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) Оператор для оказания ПД в «Интернет» должен зарезервировать достаточное количество внешних IPv4 адресов из зарегистрированного за Оператором в базе данных RIPE NCC пространства IPv4 адресов. Объем (количество) IPv4 адресов Оператора 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 Оператор 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 Оператором.
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».

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

- интерфейса на оборудовании Оператора, 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;
- прекращение оказания 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.

5.5. **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.

5.5.2. Требования к архитектуре Компонента:

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

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

5.5.3. Управление Компонентом.

Оператор 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.

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

5.5.4.1. Требования к архитектуре Элемента.

Архитектура решений по контентной фильтрации в рамках ЕСПД представлена на *Рисунок 4*.

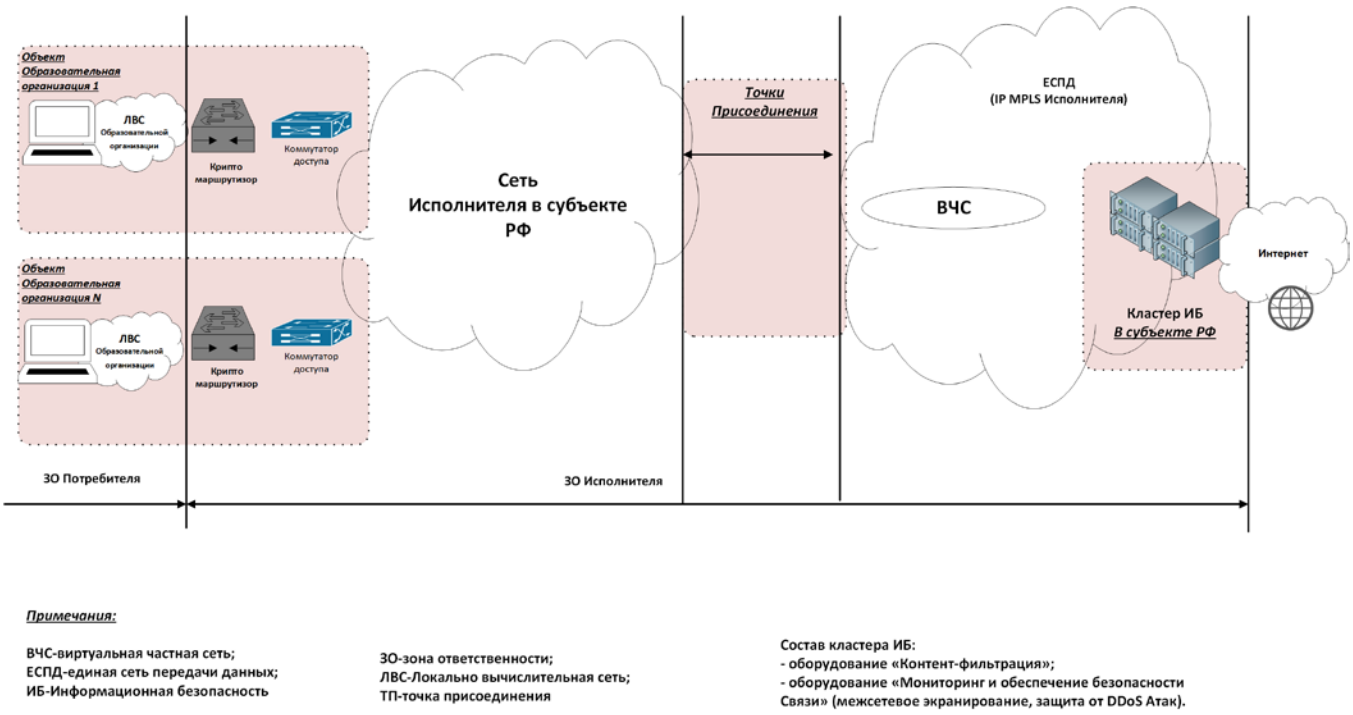


Рисунок 3 Общая архитектура решений по контентной фильтрации.

5.5.4.2. Требования к Элементу.

Контентная фильтрация должна поддерживать следующие функции:

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

– добавление сервисов в обход контентной фильтрации по запросу Абонента.

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 Оператора;

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

5.5.4.3. Требования к применяемым техническим решениям:

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

5.5.4.4. 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 Оператора;

– 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 ресурсу сети «Интернет» 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 Оператором 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;

1) 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 Оператора (ППР, проблемы с канальной, сетевой частью как на объекте, так и на магистральной части) с глубиной хранения данных 12 месяцев;

2) 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;

3) 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 Абонента (ремонт и другие работы на продолжительный период связанные с отключением услуги, но не приводящие к исключению объекта из заявки к Договору) 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.

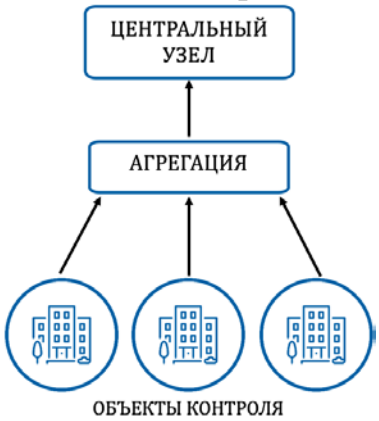


Рисунок 4 Общая архитектура Компонента «Мониторинг и обеспечение безопасности связи».

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 Оператора, 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.

Оператор 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;
– прекращение мониторинга и обеспечения безопасности связи/

5.6.1.6. Требования к наличию отчетов.

Компонент должен обеспечивать по каждому объекту образовательной организации формирование в электронном виде по запросу уполномоченного представителя Абонента 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 Абонента;

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

5.6.2.3. Оператор должен обеспечивать защиту от DoS/DDoS-атак на оборудовании Оператора.

1) Защита от DoS/DDoS-атак средствами Оператора 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 Оператора, 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 Оператора аномалии в трафике Потребителя;

– вручную, путем обращения Потребителем в Службу технической поддержки;

– вручную Оператором при обнаружении оборудованием Оператора 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 Оператора.

5.7.2. Требования к Компоненту:

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

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.

3) Организованные каналы связи начинаются на оборудовании Оператора 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 Оператора 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;

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

7) Организованные каналы должны предоставлять как минимум 3 класса качества обслуживания трафика;

8) 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 скорость передачи данных в соответствии с Бланком заказа.

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 скорость передачи данных в соответствии с Бланком заказа.

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.

5.8.3. Требования к качеству обслуживания.

В рамках модели с 3 классами обслуживания при передаче трафика между образовательными организациями и узлом Оператора 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 L2-пакетов, не более	Задержка передачи L2-пакетов в одну сторону, не более	Вариация задержки, не более
Класс 1	0,2%	15 мс	10 мс
Класс 2	0,2%	20 мс	не нормируется
Класс 3	5%	25 мс	не нормируется

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

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

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

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

6. Порядок контроля качества Услуг связи

6.1. Для объектов, которым оказываются Услуги связи, наличие доступа к информационным системам и сети «Интернет» на объекте определяется Абонентом посредством Компонента «Мониторинг и обеспечение безопасности связи». Ежемесячно в срок, установленный Договором, Оператор предоставляет сводный акт о прерывании в предоставлении Услуг связи и отчет о функционировании Элемента «Мониторинг параметров качества предоставляемых услуг», на основании которых Абонентом осуществляется контроль оказания Услуг связи.

6.2. Оплата Услуг связи осуществляется за фактически оказанные Услуги связи, предусмотренные Бланком заказа. При этом расчет стоимости фактически оказанных Услуги связи по компонентам Услуги связи «Передача данных» и «Передача данных L2» (далее – Услуги) осуществляется Абонентом на основании Отчетов о функционировании Элемента «Мониторинг параметров качества предоставляемых услуг» согласно условиям Договора, предусматривающим абонентскую систему оплаты из расчета за 1 календарный месяц. В случае, если Услуги связи фактически оказывались неполный календарный месяц, стоимость Услуг связи подлежит перерасчету Абонентом по следующей формуле:

$$C = T-((T/Д1) \times (Дн+Дпр)), \text{ где:}$$

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 Оператора, выполняемыми по запросу Абонента;
- неисправностей оборудования Потребителя;
-действий Потребителей, вызванных в том числе отключением электропитания оборудования Оператора;

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.

6.3. Исполнение Оператором обязательств по Договору считается ненадлежащим в случае, если коэффициент доступности Услуг **Кд общий** за расчетный период составляет менее 0,9.

6.3.1.1. 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;

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

- проведением плановых профилактических работ.

Оператор проводит технологические перерывы в порядке, предусмотренном Регламентом технической поддержки при оказании Услуг связи. 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 Оператора, выполняемыми по запросу Абонента;
- неисправностей оборудования Абонента;
- действий Потребителей, вызванных в том числе отключением электропитания оборудования Оператора.

Порядок открытия и закрытия инцидентов для расчета времени недоступности Услуг связи определяется в соответствии с Регламентом технической поддержки при оказании Услуг связи. 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.