ГРУППА КОМПАНИЙ «РОССЕТИ»



СТАНДАРТ ОРГАНИЗАЦИИ

СТО 34.01-9-005-2020

КОНЦЕПЦИЯ ПОСТРОЕНИЯ СЕТИ СВЯЗИ ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА

Стандарт организации

Дата введения: 02.09.2020

ПАО «Россети»

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации»; объекты стандартизации и общие положения при разработке и применении стандартов организаций Российской Федерации - ГОСТ Р 1.4-2004 «Стандартизация в Российской Федерации. Стандарты организаций. Общие положения»; общие требования к построению, изложению, оформлению, содержанию и обозначению межгосударственных стандартов, правил и рекомендаций по межгосударственной стандартизации и изменений к ним - ГОСТ 1.5-2001; правила построения, изложения, оформления и обозначения национальных стандартов Российской Федерации, общие требования к их содержанию, а также правила оформления и изложения изменений к национальным стандартам Российской Федерации - ГОСТ Р 1.5-2012.

Сведения о стандарте организации

1. РАЗРАБОТАН
   АО «Управление ВОЛС-ВЛ»
2. ВНЕСЕН
   ОАО «МРСК Урала»
3. УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ
   Распоряжением ПАО «Россети» от 02.09.2020 № 252р.
4. ВВЕДЕН ВПЕРВЫЕ

Замечания и предложения по НТД следует направлять в ПАО «Россети» согласно контактам, указанным на официальном информационном ресурсе, или электронной почтой по адресу gost.e-ecolog.ru

Настоящий документ не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения ПАО «Россети». Данное ограничение не предусматривает запрета на присоединение сторонних организаций к настоящему стандарту и его использование в их производственно-хозяйственной деятельности. В случае присоединения к стандарту сторонней организации необходимо уведомить ПАО «Россети».

Содержание

Введение ... 4
1. Область применения ... 4
2. Нормативные ссылки ... 4
3. Термины и определения ... 7
4. Обозначения и сокращения ... 8
5. Порядок разработки и внесения изменений в стандарт ... 11
6. Типовые сегменты ССЭСК ... 12
7. Требования и особенности предоставления услуг ССЭСК ... 14
8. Качества обслуживания трафика ССЭСК ... 15
9. Архитектура ССЭСК ... 19
9.1. Основные положения построения и развития ССЭСК ... 20
9.2. Функциональный состав ССЭСК ... 21
9.3. Требования к разрабатываемой системе управления ССЭСК ... 28
9.4. Функциональный состав единого центра управления ССЭСК ... 30
9.5. Требования к элементам архитектуры ССЭСК ... 33
9.6. Обеспечение устойчивости ССЭСК ... 36
10. Принципы межсетевого взаимодействия ССЭСК ... 37
10.1. Принципы и условия взаимодействия сегментов ССЭСК ... 37
10.2. Принципы и условия взаимодействия сетей связи ДЗО ПАО «Россети», входящих в состав ССЭСК ... 38
10.3. Принципы и условия взаимодействия ССЭСК с сетями связи сторонних организаций ... 41
10.4. Принципы и условия взаимодействия ССЭСК с сетью связи общего пользования ... 43
10.5. Основные положения предоставления сторонним организациям сетевых ресурсов ССЭСК и доступа к инфраструктурным объектам ДЗО ... 43
11. Информационная безопасность ССЭСК ... 44
12. Техническое обслуживание и эксплуатация ССЭСК ... 48
13. Нормативно-правовое обеспечение деятельности ССЭСК ... 51
14. Реализация концепции развития ССЭСК ... 59
14.1. Процесс оценки и надзора за реализацией Стандарта ... 59
14.2. Индикативные показатели успешной реализации Стандарта ... 59
Библиография ... 60
Приложение А Типовые сегменты, сервисы и микросегменты ССЭСК ... 64
Приложение Б Требования к каналам связи ... 68
Приложение В Альбом типовых решений по построению усилительных трактов в ВОЛС ... 72
Приложение Г Альбом типовых решений по построению узлов транспортной сети связи ... 75
Приложение Д Типовая архитектура РУОТ ... 79

Введение

Настоящий стандарт «Концепция построения сети связи электросетевого комплекса» (далее - Стандарт) является внутренним документом ПАО «Россети».

Стандарт уточняет требования Положения ПАО «Россети» о единой технической политике в электросетевом комплексе и Политики ПАО «Россети» в области информационных технологий, автоматизации и телекоммуникаций, а также учитывает и дополняет положения Концепции Цифровая трансформация 2030 и Концепции развития системы оперативно-технологического управления и ситуационного управления в электросетевом комплексе в части требований к архитектуре и функционального состава сети связи электросетевого комплекса.

Цель данного Стандарта является формирование единого подхода к построению и организации эксплуатации сети связи электросетевого комплекса.

Актуальность данного Стандарта определяется необходимостью решения задачи цифровой трансформации электросетевого комплекса, повышения его надежности и эффективности, т.е. обеспечение снижения удельных инвестиций и операционных расходов, прежде всего расходов на содержание информационно-телекоммуникационной инфраструктуры и обеспечение технологических процессов, при одновременном повышении надежности и качества услуг для потребителей.

1. Область применения

Настоящий Стандарт:

- содержит положения общего (методического) характера с описанием процесса реализации единой технической политики в области связи при создании (модернизации, реконструкции) и эксплуатации сетей связи ДЗО;
- распространяется на вновь сооружаемые, а также подлежащие техническому перевооружению и реконструкции объекты электросетевого хозяйства;
- предназначен для применения в ДЗО и подразделениях ПАО «Россети», осуществляющих развитие и эксплуатацию сетей связи электросетевого комплекса.

2. Нормативные ссылки

ГОСТ Р 1.4-2004 Стандартизация в Российской Федерации. Стандарты организаций. Общие положения.

ГОСТ Р 52266-2004 Кабельные изделия. Кабели оптические. Общие технические условия.

ГОСТ Р 57139-2016 Кабели оптические. Термины и определения.

ГОСТ 28470-90 Система технического обслуживания и ремонта технических средств вычислительной техники и информатики. Виды и методы технического обслуживания и ремонта.

ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем.

ГОСТ 15543.1-89 Изделия электротехнические и другие технические изделия. Общие требования в части стойкости к климатическим внешним воздействующим факторам.

ГОСТ 30429-96 Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования и аппаратуры, устанавливаемых совместно со служебными радиоприемными устройствами гражданского назначения. Нормы и методы испытаний.

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

ГОСТ Р 54429-2011 Кабели связи симметричные для цифровых систем передачи. Общие технические условия.

ГОСТ Р 53363-2009 Цифровые радиорелейные линии. Показатели качества. Методы расчета.

ГОСТ Р 54485-2011 Совместимость технических средств электромагнитная. Сигнализация в низковольтных электрических установках в полосе частот от 3 до 148,5 кГц. Часть 2-1. Оборудование и системы связи по электрическим сетям в полосе частот от 95 до 148,5 кГц, предназначенные для применения в жилых, коммерческих зонах и производственных зонах с малым энергопотреблением. Требования устойчивости к электромагнитным помехам и методы испытаний.

ГОСТ Р МЭК 60870-5-104-2004 Устройства и системы телемеханики. Часть 5. Протоколы передачи. Раздел 104. Доступ к сети для ГОСТ Р МЭК 870-5-101 с использованием стандартных транспортных профилей.

ГОСТ Р МЭК 60870-5-101-2006 Устройства и системы телемеханики. Часть 5. Протоколы передачи. Раздел 101. Обобщающий стандарт по основным функциям телемеханики.

ГОСТ Р МЭК 60870-5-103-2005 Устройства и системы телемеханики. Часть 5. Протоколы передачи. Раздел 103. Обобщающий стандарт по информационному интерфейсу для аппаратуры релейной защиты.

ГОСТ Р МЭК 61850-3-2005 Сети и системы связи на подстанциях. Часть 3. Основные требования.

ГОСТ Р МЭК 61850-5-2011 Сети и системы связи на подстанциях. Часть 5. Требования к связи для функций и моделей устройств.

ГОСТ Р МЭК 61850-6-2009 Сети и системы связи на подстанциях. Часть 6. Язык описания конфигурации для связи между интеллектуальными электронными устройствами на электрических подстанциях.

ГОСТ Р МЭК 61850-7-1-2009 Сети и системы связи на подстанциях. Часть 7. Базовая структура связи для подстанций и линейного оборудования. Раздел 1. Принципы и модели.

ГОСТ Р МЭК 61850-7-2-2009 Сети и системы связи на подстанциях. Часть 7. Базовая структура связи для подстанций и линейного оборудования. Раздел 2. Абстрактный интерфейс услуг связи (ACSI).

ГОСТ Р МЭК 61850-7-3-2009 Сети и системы связи на подстанциях. Часть 7. Базовая структура связи для подстанций и линейного оборудования. Раздел 3. Классы общих данных.

ГОСТ Р МЭК 61850-7-4-2011 Сети и системы связи на подстанциях. Часть 7. Базовая структура связи для подстанций и линейного оборудования. Раздел 4. Совместимые классы логических узлов и классы данных.

ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности.

ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности.

ГОСТ Р МЭК 60073-2000 Интерфейс человеко-машинный. Маркировка и обозначения органов управления и контрольных устройств. Правила кодирования информации.

ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения.

ГОСТ Р 50948-2001 Средства отображения информации индивидуального пользования. Общие эргономические требования и требования безопасности.

ГОСТ Р 50949-2001 Средства отображения информации индивидуального пользования. Методы измерений и оценки эргономических параметров и параметров безопасности.

ГОСТ Р 56938-2016 Защита информации. Защита информации при использовании технологий виртуализации. Общие положения.

ГОСТ Р МЭК 60950-2002 Безопасность оборудования информационных технологий.

ГОСТ Р 56087.5-2014 Система национальных стандартов в области качества услуг связи. Качество услуг сотовой подвижной связи. Нормативные значения показателей качества.

ГОСТ Р 56003-2014 Телекоммуникации. Нормы на параметры интерфейсов систем электропитания. Интерфейс переменного и постоянного тока напряжением до 400 В.

ГОСТ Р 55950-2014 Телекоммуникации. Нормы на параметры интерфейсов систем электропитания. Интерфейс постоянного тока.

ГОСТ Р 55949-2014 Телекоммуникации. Нормы на параметры интерфейсов систем электропитания. Интерфейс переменного тока.

ГОСТ Р 55711-2013 Комплекс технических средств автоматизированной адаптивной ВЧ (КВ) дуплексной радиосвязи. Алгоритмы работы.

ГОСТ Р 54417-2011 Компоненты волоконно-оптических систем передачи. Термины и определения.

ГОСТ Р 56172-2014 Национальный стандарт Российской Федерации. Радиостанции и ретрансляторы стандарта DMR.

ГОСТ 1.5-2001 Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Общие требования к построению, изложению, оформлению, содержанию и обозначению.

Примечание: при пользовании настоящим стандартом целесообразно проверить действие ссылочных документов в информационной системе общего пользования - на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3. Термины и определения

В настоящем Стандарте применены следующие термины с соответствующими определениями:

3.1. Вариация задержки - это различие во времени прохождения в сети последовательных пакетов одного соединения.

3.2. Время задержки - значение суммы параметров: времени подготовки информации для передачи по каналу связи, времени распространения в среде, времени ожидания обработки телекоммуникационным оборудованием и времени интерпретации информации приемником.

3.3. Коэффициент готовности - вероятность того, что объект, канал связи или система из двух взаимно резервируемых каналов связи окажется в работоспособном состоянии за период эксплуатации равный одному календарному году.

3.4. Коэффициент потери пакетов - отношение правильно принятых пакетов данных к общему количеству пакетов, которые были переданы за определенный промежуток времени.

3.5. Максимальное время задержки при переходе на резервный канал - максимально допустимое значение времени между моментом обнаружения

потери или неприемлемым ухудшением связи по основному каналу и установлением соединения по резервному каналу связи.

3.6. Микросегментирование - более детальное, в отличие от сегментирования, разделение сети связи по функциональному назначению информационных систем, для которых предоставляются телекоммуникационные услуги.

3.7. Неоперативная технологическая информация - технологическая информация, не используемая для задач оперативно-диспетчерского и оперативно-технологического управления.

3.8. Объекты ОТУ ЦУС - линии электропередачи, оборудование и устройства энергообъектов, отнесенные к объектам диспетчеризации, в отношении которых ЦУС выполняет операционные функции (или планируется прием операционных функций).

3.9. Объект РУОТ - один из узлов связи входящих в состав РУОТ.

3.10. Оперативно-технологическая информация - технологическая информация, используемая для задач оперативно-диспетчерского и оперативно-технологического управления.

3.11. Распределенный узел обмена трафиком (РУОТ) - два или более узлов связи, расположенных на географически разнесенных площадках, объединенных в телекоммуникационную инфраструктуру, обеспечивающую гарантированный обмен достоверной информацией между сетями связи ДЗО.

3.12. Сегментирование сети связи - логическое или физическое разбиение сети на сегменты/подсети с целью оптимизации сетевого трафика и повышения безопасности сети в целом.

3.13. Сервис связи - комплекс/ набор телекоммуникационных услуг, объединенный для решения определённых задач.

3.14. Сеть связи электросетевого комплекса (ССЭСК) - комплекс взаимодействующих сетей связи ДЗО ПАО «Россети», включающий в себя средства связи и линии связи и предназначенный для обеспечения управления технологическими процессами в передаче и распределении электроэнергии, диспетчерского управления и производственной деятельности электросетевого комплекса.

3.15. Телекоммуникационная услуга - деятельность по приему, обработке, передаче, доставке информации с заданными параметрами.

3.16. Технологическая информация - информация различного вида и назначения, содержащая сведения об электроэнергетическом режиме и состоянии электрической сети и электросетевого оборудования.

4. Обозначения и сокращения

В настоящем Стандарте применены следующие обозначения и сокращения:

4.1. АРМ - автоматизированное рабочее место.

4.2. АСТУ - автоматизированная система технологического управления.

4.3. АСУД - автоматизированная система управленческого документооборота.

4.4. АСУЭ - автоматизированная система учета электроэнергии.

4.5. ВКР - вынужденное комбинационное рассеяние.

4.6. ВОЛС - волоконно-оптическая линия связи.

4.7. ГДП - городской диспетчерский пункт.

4.8. ГИС - геоинформационная система.

4.9. ДЗЛ - дифференциальная защита линии электропередачи.

4.10. ДЗО - дочерние и зависимые общества ПАО «Россети».

4.11. ДЦ - диспетчерский центр.

4.12. ЛАПНУ - локальная автоматика предотвращения нарушения устойчивости.

4.13. ЛЭП - линия электропередачи.

4.14. МРСК - межрегиональная распределительная сетевая компания.

4.15. МЭК - международная электротехническая комиссия.

4.16. ОВБ - оперативно-выездная бригада.

4.17. ОДУ - объединенное диспетчерское управление.

4.18. ОМП - система определения места повреждения на ВЛ.

4.19. ОТУ - оперативно-технологическое управление.

4.20. ПА - противоаварийная автоматика.

4.21. ПО - производственное отделение.

4.22. ПС - подстанция.

4.23. РАС - регистратор аварийных событий.

4.24. РДУ - региональное диспетчерское управление.

4.25. РЗ - релейная защита.

4.26. РП - распределительный пункт.

4.27. РУОТ - распределенный узел обмена трафиком.

4.28. РЦОД - распределенный центр обработки данных.

4.29. РЭС - район электрических сетей.

4.30. СКЗИ - средства криптографической защиты информации.

4.31. СМПР - система мониторинга переходных режимов.

4.32. ССОП - сеть связи общего пользования.

4.33. ССЭСК - сеть связи электросетевого комплекса.

4.34. СУПА - система управления производственными активами.

4.35. ТП - трансформаторная подстанция.

4.36. ФСТЭК - федеральная служба по техническому и экспортному контролю.

4.37. ЦС АРЧМ - централизованная система автоматического регулирования частоты и перетоков мощности.

4.38. ЦУС - центр управления сетями.

4.39. ЦУСС - центр управления сетями связи электросетевого комплекса.

4.40. APN - Access Point Name.

4.41. AVoIP - Audio and Video over Internet Protocol.

4.42. BER - Bit Error Rate.

4.43. CBWFQ+LLQ - Class-Based Weighted Fair Queuing + Low-Latency Queue.
4.44. CE - customer edge router.
4.45. CESoPSN - Structure-Aware Time Division Multiplexed Circuit Emulation Service over Packet Switched Network.
4.46. CoS - Class of Service.
4.47. CWDM - Coarse Wavelength Division Multiplexing.
4.48. DMR - Digital Mobile Radio.
4.49. DSCP - Differentiated Services Code Point.
4.50. DWDM - Dense Wavelength Division Multiplexing.
4.51. EXP - Experimental Use.
4.52. FEC - Forward Error Correction.
4.53. GRE - Generic Routing Encapsulation.
4.54. IP - Internet Protocol.
4.55. IS-IS - Intermediate System to Intermediate System.
4.56. LAN - Local Area Network.
4.57. LDP - Label Distribution Protocol.
4.58. LLDP - Link Layer Discovery Protocol.
4.59. LPWAN - Low-power Wide-area Network.
4.60. MAC - Media Access Control.
4.61. MBGP - Multiprotocol Border Gateway Protocol.
4.62. MMF - Multi Mode Fiber.
4.63. MPLS-TP - Multiprotocol Label Switching - Transport Profile.
4.64. MSTP - Multiple Spanning Tree Protocol.
4.65. NAT - Network Address Translation.
4.66. ODU - Optical Data Unit.
4.67. OSI - Open Systems Interconnection.
4.68. OSNR - Optical Signal-to-Noise-Ratio.
4.69. OSPF - Open Shortest Path First.
4.70. OTU - Optical Transport Unit.
4.71. PB-DWRR - Priority Based Deficit Weighted Round Robin.
4.72. PHB - Per-Hop Behavior.
4.73. PLC - Power Line Communication.
4.74. PE/P - Provider Edge / Provider router.
4.75. QoS - Quality of Service.
4.76. RCP - Rich Client Platform.
4.77. RD - Route Distinguisher.
4.78. RED - Random Early Detection.
4.79. ROPA - Remote Optically Pumped Amplifier.
4.80. RT - Route Target.
4.81. RSPAN - Remote Switch Port Analyzer.
4.82. RSVP-TE - Resource Reservation Protocol - Traffic Engineering.
4.83. RSTP - Rapid Spanning Tree Protocol.
4.84. SAToP - Structure-Agnostic Time Division Multiplexing over Packet.
4.85. SDH - Synchronous Digital Hierarchy.

4.86. SDH NG - Synchronous Digital Hierarchy New Generation.
4.87. SLA - Service Level Agreement.
4.88. SMF - Single Mode Fiber.
4.89. SoIP - Serial over Internet Protocol.
4.90. SNMP - Simple Network Management Protocol.
4.91. SPAN - Switch Port Analyzer.
4.92. SSH - Secure Shell.
4.93. TDM - Time Division Multiplexing.
4.94. TE - Traffic Engineering.
4.95. TFF - Thin-Film Filter.
4.96. TFTP - Trivial File Transfer Protocol.
4.97. TMN - Telecommunications Management Network.
4.98. ToIP - Text over Internet Protocol.
4.99. TS - Time-Slot.
4.100. VC - Virtual Container.
4.101. VLAN - Virtual Local Area Network.
4.102. VoIP - Voice over Internet Protocol.
4.103. VPN - Virtual Private Network.
4.104. VPLS - Virtual Private LAN Service.
4.105. VPWS - Virtual Private Wire Service.
4.106. VRF - Virtual Routing and Forwarding.
4.107. VRRP - Virtual Router Redundancy Protocol.
4.108. Wi-Fi - Wireless Fidelity.
4.109. WRED - Weighted Random Early Detection.
4.110. Взаимно рез. каналов - взаимно резервируемые каналы связи.
4.111. гор. рез. - горячее резервирование.
4.112. Коэф. готовности - коэффициент готовности канала связи для периода эксплуатации равного одному календарному году.
4.113. Маг. линия связи - магистральная линия связи.
4.114. Макс. время задержки при переходе на рез. канал - максимальное время задержки при переходе на резервный канал связи.
4.115. н.р. - не регламентируется.
4.116. рек. - рекомендуется.
4.117. Сост. ССЭСК - составляющая ССЭСК.
4.118. Терм. узел связи - терминальный узел связи.

5. Порядок разработки и внесения изменений в стандарт

5.1. Все изменения в Стандарт вносятся согласно организационно-распорядительным документам ПАО «Россети».

5.2. В настоящий Стандарт должны быть внесены изменения в случаях ввода в действие новых технических регламентов, национальных и международных стандартов, содержащих неучтенные в данном документе требования, а также при необходимости введения новых требований и рекомендаций.

5.3. Рекомендуется поводить работы по оценке актуальности Стандарта не реже одного раза за три года.

6. Типовые сегменты ССЭСК

6.1. ССЭСК должна создаваться и развиваться как конвергентная телекоммуникационная основа для построения единой информационной инфраструктуры с целью обеспечения всех видов информационного взаимодействия, необходимых для надежного функционирования электросетевого комплекса.

6.2. ССЭСК должна обеспечивать передачу всех видов информации (голос, аудио, видео, текст, данные, мультимедийные и многокомпонентные данные).

6.3. Для исключения межсистемных влияний различных систем управления технологическими процессами, административно-хозяйственной деятельности и служебной связи ССЭСК должна разделяется на сегменты.

6.4. В составе ССЭСК выделяется четыре сегмента:

- Технологический - сегмент ССЭСК, предназначен для обеспечения телекоммуникационными услугами с заданными показателями качества обслуживания, включая уровень надежности, необходимый и достаточный для нормального функционирования систем управления технологическими процессами электросетевого комплекса;
- Корпоративный - сегмент ССЭСК, предназначен для обеспечения телекоммуникационными услугами систем административно-хозяйственной деятельности ПАО «Россети» и их ДЗО;
- Мультимедийный - сегмент ССЭСК, предназначен для обеспечения телекоммуникационными услугами в режиме реального времени мультимедийных систем ПАО «Россети» и их ДЗО;
- Служебный - сегмент ССЭСК, предназначен для обеспечения функционирования, управления и мониторинга сети связи.

6.5. Для решения конкретных задач на уровне ДЗО, например, оптимизация сетевого трафика или повышения безопасности сети связи и так далее, возможно более детальное разделение сети связи на сервисы и микросегменты, предоставляющие телекоммуникационные услуги различным системам электроэнергетики. Перечень типовых сервисов и микросегментов ССЭСК приведен в Приложении А, и при необходимости может быть, как дополнен, так и обобщен, в зависимости от нужд конкретного ДЗО.

6.6. Деление на сервисы и микросегменты производится в соответствии с функциональным назначением технологических, корпоративных, мультимедийных и служебных информационных систем, для которых предоставляются телекоммуникационные услуги.

6.7. Применяемые механизмы сегментирования и микросегментирования должны обеспечить решение следующих задач:

- Организовать передачу трафика между узлами;

- Обеспечить идентификацию трафика данного сегмента или микросегмента;
- Обеспечить изоляцию трафика, передаваемого в данном сегменте или микросегменте;
- Исключить пересечение адресных пространств различных сегментов или микросегментов.

6.8. Данные задачи должны решаться на всем пути следования трафика, обеспечивая сквозное сегментирование или микросегментирование (организация сегментирования или микросегментирования в составном канале, проходящем через сети, использующие различные технологии связи).

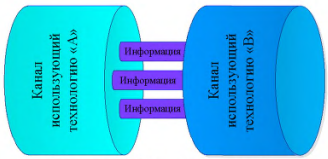
6.9. Составные каналы связи работают либо за счет инкапсуляции одного канала в другой, либо за счет переноса полезной информационной нагрузки.

6.10. В случае инкапсуляции канала (Вариант А), наиболее оптимальным решением является сегментирование или микросегментирование на уровне вложенного канала, при этом на границе между каналами во время инкапсуляции атрибуты сегмента/микросегмента, не должны редактироваться или удаляться.

6.11. В случае переноса полезной информационной нагрузки (Вариант Б) к сегментированию или микросегментированию должен применяться дифференцированный подход (отдельное сегментирование или микросегментирование в каждой составной части канала и соотнесение атрибутов, для того чтобы сегмент/микросегмент рассматривался как единое целое). Для обеспечения изоляции трафика внутри сегмента/микросегмента на границе между каналами информационные потоки должны быть разделены на физическом уровне.



Вариант А. Инкапсуляция канала



Вариант Б. Перенос полезной информационной нагрузки

Рисунок 1. Принципы построения составных каналов связи.

6.12. Выбор механизмов сегментирования или микросегментирования осуществляется исходя из необходимого для предоставления

телекоммуникационной услуги уровня обслуживания и применяемых технологий передачи.

6.13. Для каждого из сервисов ССЭСК должен быть выделен свой диапазон атрибутов, таких как номера VLAN, RD, RT, перечень имен VRF, пул IP-адресов.

7. Требования и особенности предоставления услуг ССЭСК

7.1. При проектировании каналов связи, для предоставления определенной телекоммуникационной услуги должны соблюдаться требования, изложенные в следующих документах:

- Постановление Правительства РФ от 08.06.2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры»;
- Технические требования по организации каналов связи для оперативных переговоров и передачи телеметрической информации при выполнении ЦУС операционных функций в отношении объектов диспетчеризации от 29.12.2017;
- Типовое соглашение о технологическом взаимодействии в целях обеспечения надежности функционирования ЕЭС России между АО «СО ЕЭС» и территориальной сетевой организацией, являющейся дочерним обществом ПАО «Россети»;
- Требования к каналам связи для функционирования релейной защиты и автоматикия, утвержденные Приказом Минэнерго России от 13.02.2019 № 97;
- СТО 34.01-9.2-004-2019 «Каналы связи для РЗА. Технические решения для сетей 35-220 кВ»;
- СТО 01.Б6.04-2019 Издание 2 «Технические требования к организации АСТУ и технологическому оснащению диспетчерских пунктов ЕЦУС»;
- СТО 56947007-33.060.40.134-2012 «Типовые технические решения по системам ВЧ связи»;
- Письмо ОАО «Россети» БР/74/2207 от 24.11.2014 «О согласовании частот ВЧ по ВЛ»;
- ГОСТ Р 55890-2013 Единая энергетическая система и изолированно работающие энергосистемы. Оперативно-диспетчерское управление регулирование частоты и перетоков активной мощности. Нормы и требования;
- ГОСТ 34045-2017 Электроэнергетические системы оперативно-диспетчерское управление. Автоматическое противоаварийное управление режимами энергосистем. Противоаварийная автоматика энергосистем. Нормы и требования;

- Нормы на электрические параметры цифровых каналов и трактов магистральной и внутризоновых первичных сетей (приказ Минсвязи Российской Федерации № 92 от 10.08.1996);
- ГОСТ Р 62443 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы;
- ГОСТ Р 56498-2015 МЭК 62443-3:2008 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления.

7.2. Пропускная способность каналов связи должна выбираться по результатам расчетов и обеспечивать передачу требуемых видов и объемов информации.

7.3. Сводная таблица с требованиями к каналам связи, рекомендованными на момент написания стандарта, приведена в Приложении Б.

8. Качества обслуживания трафика ССЭСК

8.1. Для соблюдения требований каналов связи к таким параметрам как максимальное время задержки, вариация задержки (джиттер), пропускная способность канала, вероятность потери трафика в ССЭСК должен применяться набор технологий обеспечения качества обслуживания (QoS).

8.2. Для обеспечения качества обслуживания должна применяться модель, отвечающая следующим требованиям:

- Каждый узел (устройство) в сети сам определяет, как обеспечить нужное качество обслуживания, независимо от других узлов (устройств).
- Модель должна быть основана на агрегированной классификации трафика;
- Модель должна иметь ограниченный и детерминированный набор действий по обработке трафика данных классов.

8.3. Для повышения гибкости ССЭСК должна разделяться на домены QoS, организованные в рамках сетей связи ДЗО ПАО «Россети».

8.4. В каждом домене QoS должен применяться унифицированный набор классов трафика и PHB (модель поведения по отношению к конкретному классу трафика) для них, а также должна применяться маркировка трафика в соответствии с их классом.

8.5. На входе в домен QoS трафик должен классифицироваться и маркироваться с применением алгоритмов Interface-Based (классификация трафика на основе входного порта) или MultiField (классификация трафика на основе анализа заголовков кадров/пакетов/сегментов канального, сетевого и транспортного уровня модели OSI), приоритетным считается алгоритм Interface-Based, поскольку вносит меньшую задержку при классификации трафика.

8.6. Внутри домена QoS каждый узел (устройство) должен принимать решение по классификации на основе имеющейся маркировки (алгоритм Behavior Aggregate).

8.7. Для взаимодействия между доменами QoS должно производиться согласование применяемых политик. При полном согласовании на стыке доменов QoS должен применяться алгоритм Behavior Aggregate. При частичном согласовании должны быть определены маркеры (классы трафика) для которых применим алгоритм Behavior Aggregate, для всего остального трафика происходит перемаркировка в соответствии с заданными правилами или применяется алгоритм MultiField. На стыке доменов QoS между которыми нет согласования применяемых политик должен применяться алгоритм MultiField.

8.8. Выделение классов трафика должно производиться на основании анализа информационных потоков сети связи и их требований к качеству обслуживания. Рекомендуется выделять следующие классы трафика[1]:

- Управление сетью связи (Network control);
- Голосовые данные оперативных переговоров (Voice DC);
- Голосовые данные (Voice);
- Видео данные (Video);
- Данные сигнализации производственно-технологической телефонии и унифицированных коммуникаций (Call-Signaling);
- Технологические и критичные для работы основных информационных систем данные (Critical Data);
- Данные других внутренних информационных систем (Bulk Data);
- Не идентифицированный, некритичный для задачи предприятия трафик (Scavenger).

8.9. Для трафика информационного обмена с сетью интернет не выделяется отдельный класс и не применяются политики качества обслуживания, передача идет по мере возможности, данный трафик отбрасывается в первую очередь.

8.10. Рекомендуемые правила маркировки классов трафика и применяемые к ним PHB приведены в Таблице 1.

Таблица 1 - Правила маркировки классов трафика и применяемые к ним PHB

Класс трафика	PHB[2]	IP	Ethernet	MPLS	Класс трафика в сети оператора связи
		DSCP	CoS	EXP	
Network control	CS6	48	6	6	Priority
Voice	EF	46	6	6	Real time
Voice DC	CS5	40	5	5	Real time
Video	CS4	32	4	4	Ordinary
Call-Signaling	CS3	24	3	3	Priority

[1] Трафик систем РЗ и ПА передается в выделенных телекоммуникационных инфраструктурах и к нему не применяются политики качества обслуживания, из-за задержек вносимых QoS.

[2] Перечисленные PHB описаны в RFC 4594.

Класс трафика	PHB[2]	IP	Ethernet	MPLS	Класс трафика в сети оператора связи
		DSCP	CoS	EXP	
Critical Data	AF23	16	2	2	Priority
Bulk Data	AF11	10	1	1	Ordinary
Scavenger	CS1	8	1	1	Ordinary

8.11. Если устройство поддерживает меньше восьми классов обслуживания (меньше восьми очередей), то трафик из классов Video и Critical Data должен оказаться в разных очередях.

8.12. В очереди класса Critical Data трафик не должен отбрасываться при переполнении исходящего интерфейса, в остальных очередях должны быть настроены механизмы, отбрасывающие трафик при приближении к порогу переполнения (рекомендуется для очередей Network control, Voice DC, Voice, Video - использовать механизм Head Drop; для очереди Call-Signaling - механизм RED; для очередей Bulk Data и Scavenger - механизм WRED). Рекомендуемые механизмы обработки очередей CBWFQ+LLQ или PB-DWRR (с ограничением полосы для приоритетной очереди).

8.13. Классификация трафика и применяемые PHB для различных видов трафика сервиса связи для взаимодействия с АО «СО ЕЭС» должны быть согласованны с ДЦ АО «СО ЕЭС», с учетом классификации и применяемых PHB к данному трафику в транзитных сетях связи сторонних организаций и /или операторов связи при их наличии.

8.14. Качество обслуживание трафика в сетях, использующих технологии коммутации каналов, достигается за счет соблюдения требований к каналам связи, определяющих качество передачи информации (показатели по ошибкам, допустимое значение фазового дрожания и т. п.) и определяются следующими документами:

- Методика расчета показателя по ошибкам PDH трактов определена в НПА № 92 «Норм на электрические параметры основных цифровых каналов и трактов магистральной и внутризоновых сетей ВСС России» утвержденные Приказом Минкомсвязи России от 10.08.1996. Данный документ распространяется на PDH тракты как проводных, так и радиорелейных линий связи и определяет методику расчета долговременных и оперативных норм;
- Методика расчета показателя по ошибкам SDH трактов определяется на основании рекомендаций ITU-T G.828 (долговременные нормы) и ITU-T M.2101 (оперативные нормы);
- Методика расчета оперативных норм показателя по ошибкам SDH трактов с использованием радиорелейных линий связи описана в РД 45.199 - 2001 «Нормы оперативные на показатели качества цифровых трактов СЦИ, образованные в цифровых магистральных РРЛ»;
- Методика расчета долговременных норм показателя по ошибкам SDH трактов с использованием радиорелейных линий связи описана в РД 45.183-01 «Долговременные нормы на цифровые тракты СЦИ, образованные в цифровых магистральных РРЛ»;

- Методика расчета показателя по ошибкам OTN трактов определяется на основании рекомендации ITU-T G.8201;
- Согласно СТО 56947007-33.060.40.178-2014 «Технологическая связь. Руководство по эксплуатации каналов высокочастотной связи по линиям электропередачи 35 - 750 кВ» максимально допустимое число ошибок на бит в общем цифровом потоке канала ВЧ связи при отсутствии особых требований не должно превышать 10^{-6}.
- Максимально допустимое значение фазового дрожания в PDH тракте определено в рекомендации ITU-T G.823;
- Максимально допустимое значение фазового дрожания в SDH тракте определено в рекомендации ITU-T G.825;
- Максимально допустимое значение фазового дрожания в OTN тракте определено в рекомендации ITU-T G.8251;
- Максимально допустимое значение фазового дрожания в радиорелейной линии связи (PDH и SDH тракты) определено в ГОСТ Р 50765-95 «Аппаратура радиорелейная. Классификация. Основные параметры цепей стыка»;

8.15. Для оказания телекоммуникационных услуг надлежащего качества интерфейсы и каналы связи должны соответствовать требованиям, изложенным в следующих документах:

- Правила применения приемопередающих устройств для волоконно-оптических и атмосферных оптических линий передачи, утвержденные Приказом Минкомсвязи России от 27.02.2007 № 23;
- Правила применения оборудования проводных и оптических систем передачи абонентского доступа, утвержденные Приказом Минкомсвязи России от 24.08.2006 № 112;
- Правила применения оборудования цифровых систем передачи плезиохронной цифровой иерархии. Часть I. Правила применения оборудования временного группообразования плезиохронной цифровой иерархии, утвержденные Приказом Минкомсвязи России от 16.10.2006 № 132;
- Правила применения оборудования цифровых систем передачи плезиохронной цифровой иерархии. Часть II. Правила применения оборудования кроссовой коммутации плезиохронной цифровой иерархии, утвержденные Приказом Минкомсвязи России от 27.02.2007 № 24;
- Правила применения оборудования цифровых систем передачи плезиохронной цифровой иерархии. Часть III. Правила применения каналообразующего оборудования плезиохронной цифровой иерархии, утвержденные Приказом Минкомсвязи России от 06.06.2007 № 60;
- Правила применения оборудования цифровых систем передачи плезиохронной цифровой иерархии. Часть IV. Правила применения оборудования оконечных и промежуточных пунктов линейного тракта плезиохронной цифровой иерархии, утвержденные приказом Минкомсвязи России от 12.12.2007 № 147;

- Правила применения оборудования с асинхронным режимом переноса информации, утвержденные приказом Минкомсвязи России от 28.10.2008 № 85;
- Правила применения цифровых систем передачи синхронной цифровой иерархии, утвержденные приказом Минкомсвязи России от 23.11.2006 № 151;
- Правила применения оконечного оборудования, выполняющего функции систем коммутации, утвержденные приказом Минкомсвязи России от 24.08.2006 № 113;
- Правила применения оборудования коммутации и маршрутизации пакетов информации, утвержденные приказом Минкомсвязи России от 06.12.2007 № 144;
- Правила применения оборудования, реализующего технологии коммутации кадров», утвержденные приказом Минкомсвязи России от 07.12.2006 № 158;
- Правила применения земных станций спутниковой связи и вещания единой сети электросвязи Российской Федерации, утвержденные приказом Минкомсвязи России от 22.08.2007 № 99;
- Правила применения систем радиорелейной связи. Часть I. Правила применения цифровых радиорелейных систем связи плезиохронной цифровой иерархии, утвержденные приказом Минкомсвязи России от 27.02.2007 № 25;
- Правила применения систем радиорелейной связи. Часть II. Правила применения цифровых радиорелейных систем связи синхронной цифровой иерархии, утвержденные приказом Минкомсвязи России от 27.02.2007 № 26;
- Правила применения систем радиорелейной связи. Часть III. Правила применения аналоговых радиорелейных систем связи, утвержденные Приказом Минкомсвязи России от 27.02.2007 № 27;
- Правила применения систем радиорелейной связи. Часть IV. Правила применения аналогово-цифровых радиорелейных систем связи, утвержденные Приказом Минкомсвязи России от 15.08.2007 № 98;
- РД 34.48.404-96 «Рекомендации по приемке в эксплуатацию каналов высокочастотной телефонной связи и телемеханики по линиям электропередачи»;
- СТО 56947007-33.060.40.052-2010 Методические указания по расчету параметров и выбору схем высокочастотных трактов по линиям электропередачи 35-750 кВ переменного тока.

9. Архитектура ССЭСК

Основными принципами, определяющими архитектуру ССЭСК должны быть:

- Мультисервисность - независимость технологий предоставления услуг от транспортных технологий сети связи;

- Мультимедийность - способность сети передавать многокомпонентную информацию с необходимой синхронизацией этих компонентов в реальном времени и использованием сложных конфигураций соединений;
- Широкополосность - возможность динамического изменения скорости передачи информации в широком диапазоне в зависимости от текущих потребностей;
- Интеллектуальность - возможность управления услугой, вызовом и соединением со стороны пользователя, а также заказ новых услуг с использованием автоматизированных систем управления;
- Производительность - характеристика сети связи, определяющая такие параметры как время реакции, пропускная способность, задержка передачи, джиттер, распределение работы между несколькими элементами сети;
- Надежность - способность сети связи корректно и бесперебойно работать в течение продолжительного периода времени;
- Отказоустойчивость - способность сети связи сохранять свою работоспособность после отказа одного или нескольких составных компонентов;
- Масштабируемость - возможность расширения сети без изменения основополагающих технических принципов её построения и полной замены каналообразующего оборудования;
- Управляемость - возможность централизованно контролировать состояние основных элементов сети, выявлять и разрешать проблемы, возникающие при работе сети;
- Безопасность - обеспечение информационной безопасности сети связи и её ресурсов, в частности, передающихся по ней данных и работающих с ней пользователей.

9.1. Основные положения построения и развития ССЭСК

9.1.1. Основными положениями, определяющими направление развития ССЭСК должны быть:

- Внедрение современных телекоммуникационных технологий пакетной коммутации с соблюдением технических требований к предоставляемым услугам;
- Предоставление всего спектра телекоммуникационных услуг на единой транспортной платформе и с использованием единого интерфейса;
- Снижение капитальных и операционных затрат за счёт использования унифицированных типовых решений и автоматизации процессов диагностики и управления;
- Внедрение политик качества обслуживания сети связи;
- Разработка и внедрение единой системы управления и мониторинга сетями связи электросетевого комплекса;
- Внедрение технологий информационной безопасности;

- Использование только открытых и стандартизированных протоколов и интерфейсов;
- Применение политик балансировки нагрузки (распределение трафика по всем имеющимся сетевым ресурсам);
- Внедрение единого плана IP-адресации ССЭСК;
- Создание и применение единой номенклатуры сетевых имен телекоммуникационного оборудования;
- Учет перспективных потребностей в телекоммуникационных услугах;
- Обеспечение взаимодействия с существующими сетями связи электросетевого комплекса.

9.1.2. В настоящее время сети связи электросетевого комплекса построены в основном с применением технологий коммутации каналов, а пакетный трафик передается поверх этих сетей (IP over SDH и т. п.). Переход к полностью пакетным сетям рекомендуется проводить поэтапно:

- Первый этап - по мере развития сеть связи должна становиться гибридной (состоящей из каналов связи использующих пакетную коммутацию и TDM каналов связи);
- Второй этап - перевод пакетного трафика в каналы связи, использующие пакетную коммутацию, при соблюдении требований к каналам связи;
- Третий этап - перевод TDM трафика в каналы связи, использующие пакетную коммутацию посредствам псевдопроводных технологий, при соблюдении требований к каналам связи (перевод осуществляется только когда есть возможность организовать основной и резервный каналы в пакетной части сети или при применении гибридного оборудования, позволяющего взаимно резервировать TDM и пакетные каналы связи, а также когда резервирование не требуется);
- Четвертый этап - по мере освобождения TDM каналы связи демонтируются, освобождая сетевые ресурсы.

9.2. Функциональный состав ССЭСК

9.2.1. Пакетные сети связи ДЗО ПАО «Россети» должны обеспечивать работу различных сервисов и приложений через транспортную сеть связи ДЗО».

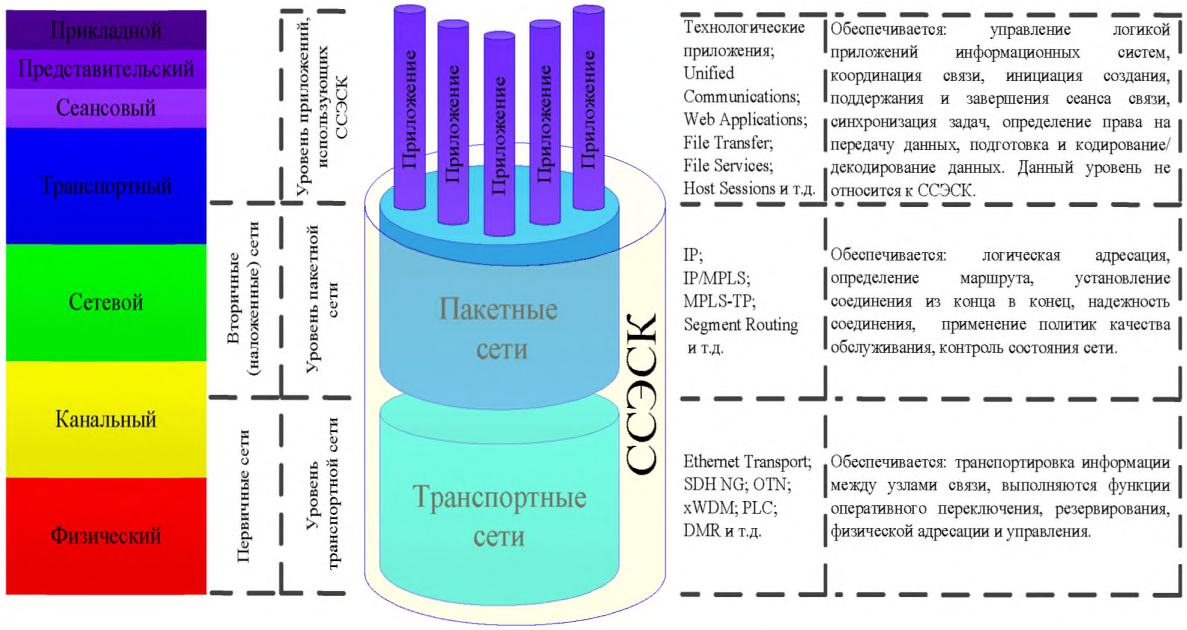


Рисунок 2. Структура ССЭСК.

9.2.2. В соответствии с «Положением ПАО «Россети» о единой технической политике в электросетевом комплексе» сеть связи состоит из следующих составляющих:

- Первичная сеть связи, представляющая собой совокупность сетей, линий и каналов связи, обеспечивающих доставку всех видов информации;
- Вторичные (наложенные) сети, представляющие собой совокупность средств, обеспечивающих передачу, коммутацию и распределение информации определённого вида.

9.2.3. Транспортная сеть связи является совокупностью всех ресурсов, выполняющих функции транспортирования трафика, включая не только системы передачи, но и относящиеся к ним средства контроля, оперативного переключения, резервирования и управления. С позиции «классической» семиуровневой модели OSI, транспортная сеть связи работает на двух нижних уровнях - физическом и канальном. Соответственно транспортная сеть является первичной сетью связи.

9.2.4. Полноценными вторичными сетями связи по праву могут считаться только пакетные сети передачи данных, поскольку они работают на третьем уровне «классической» семиуровневой модели OSI - сетевом, а также частично на втором (применение технологий коммутации по меткам) - канальном и частично на четвертом (установление TCP и UDP сессий) - транспортном, и строятся как наложенные на транспортную сеть связи.

9.2.5. Тенденция развития других существующих наложенных сетей (корпоративные телефонные сети, сети видеоконференцсвязи, производственно-технологическая телефонная связь, технологические сети связи и т. д.) - перевод их в разряд приложений[3] использующих ССЭСК и

[3] Приложения пользуются телекоммуникационными услугами и сервисами, предоставляемыми ССЭСК, но не являются её частью.

работающих поверх пакетной сети связи (обеспечение их взаимодействия на прикладном, представительском, сеансовом и частично на транспортном уровнях OSI, а функции установления и поддержания соединения, определения маршрута, установление логической адресации и т. п. возлагаются на пакетные сети посредством таких технологий, как VoIP, AVoIP ToIP, SoIP, SAToP, CESoPSN и т. д.).

9.2.6. Взаимодействие существующих наложенных сетей с пакетной сетью передачи данных должно производиться через шлюз, выполняющий следующие функции:

- Преобразование трафика между телекоммуникационными сетями различных типов;
- Конвертирование протоколов сигнализации;
- Проведение аналого-цифрового преобразования при необходимости подключения к пакетной сети аналогового оборудования.

9.2.7. Взаимодействие абонентов, подключенных к существующей наложенной сети, и абонентов, использующих приложение и подключенных к пакетной сети, должно производиться через управляющее устройство (SoftSwitch), выполняющее следующие функции:

- Обработку всех видов сигнализации, используемых в его домене;
- Управление абонентскими данными пользователей, подключенных к его домену непосредственно или через оборудование шлюзов доступа;
- Взаимодействие с серверами приложений для оказания дополнительных услуг пользователям сети.

9.2.8. Транспортная сеть связи имеет сложную структуру и объединяет большое количество объектов электросетевого комплекса, поэтому предлагается выделить три иерархических уровня транспортной сети:

- Уровень А1 - обеспечивает доступ с узлов связи энергообъектов ДЗО ПАО «Россети» не имеющих в своем составе объектов диспетчеризации (как правило, это такие объекты, как ТП, РП, ПС низкого и среднего класса напряжения и т. п.) к ресурсам транспортной сети более высоких уровней;
- Уровень А2 - обеспечивает транспортировку информации между узлами связи энергообъектов ДЗО ПАО «Россети» имеющих в своем составе объекты диспетчеризации[4] (как правило, это такие объекты, как РЭС, ПО, ГДП, ПС среднего и высокого класса напряжения и т. п.) и ЦУС филиала ДЗО ПАО «Россети», а также на данном уровне обеспечивается информационный обмен с ДЦ АО «СО ЕЭС», при необходимости организуются узлы агрегации трафика передаваемого в ДЦ АО «СО ЕЭС», кроме того данный уровень обеспечивает функции оперативного переключения, резервирования и управления;
- Уровень А3 - обеспечивает транспортировку информации между ЦУС филиала ДЗО ПАО «Россети», исполнительным аппаратом ДЗО ПАО

[4] На данном уровне так же могут использоваться узлы связи энергообъектов ДЗО ПАО «Россети» не имеющих в своем составе объектов диспетчеризации ввиду своего выгодного географического расположения.

«Россети» и прочими инфраструктурными объектами, такими как ЦОД/РЦОД, ЦУСС[5].

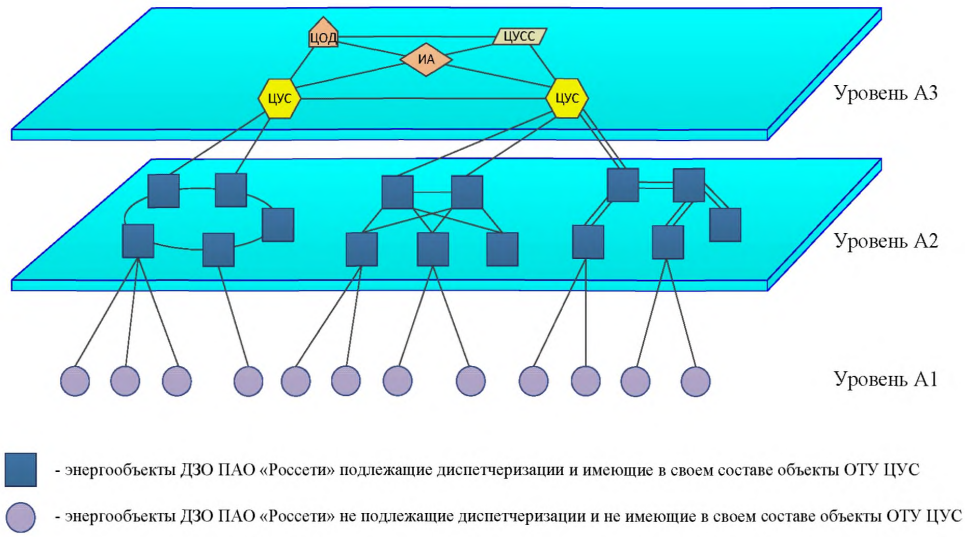


Рисунок 3. Иерархические уровни транспортной сети.

9.2.9. Для построения транспортных сетей уровня А1 возможно применение как собственных линий и средств проводной (ВОЛС, ВЧ-связь)[6] и беспроводной связи так и арендованных ресурсов связи (ОВ и каналы)[7].

9.2.10. Для построения транспортных сетей связи уровня А1 возможно применение следующих технологий:

- Ethernet Transport (10BASE-FL; 100BASE-SX, 100BASE-FX, 100BASE-FXWDM, 1000BASE-SX, 1000BASE-LX, 1000BASE-LH);
- Спектральное уплотнение (CWDM);
- Высокочастотная связь (PLC);
- Цифровая подвижная радиосвязь (DMR);
- Беспроводной широкополосный доступ (Wi-Fi; WiMAX);
- Беспроводной узкополосный доступ (LPWAN; NB-IoT);
- Мобильная связь (стандарты различных поколений сотовой связи (2G/3G/4G/5G) с применением технологии APN);

---

[5] В некоторых случаях (наличие подготовленной телекоммуникационной инфраструктуры на уровне А2, не выгодное географическое размещение объектов, экономической нецелесообразности организации отдельного уровня транспортной сети для указанных объектов и т. п.) возможно использование функций уровня А3 на уровне А2.

[6] Применение медных кабельных линий связи и технологии xDSL допускается только при соответствующем технико-экономическом обосновании.

[7] Обеспечение безопасности информации при использовании арендованных ресурсов связи на всех уровнях транспортной сети осуществляется в соответствии с требованиями действующего законодательства в сфере информационной безопасности, а также организационно-распорядительных документов ПАО «Россети».

- Спутниковая связь[8].

9.2.11. Транспортные сети связи уровня А1 должны быть организованны как правило по топологии «звезда» или «дерево», не исключается и применение других топологий («кольцо», «ячеистая», «гибридная» (комбинация нескольких базовых топологий)).

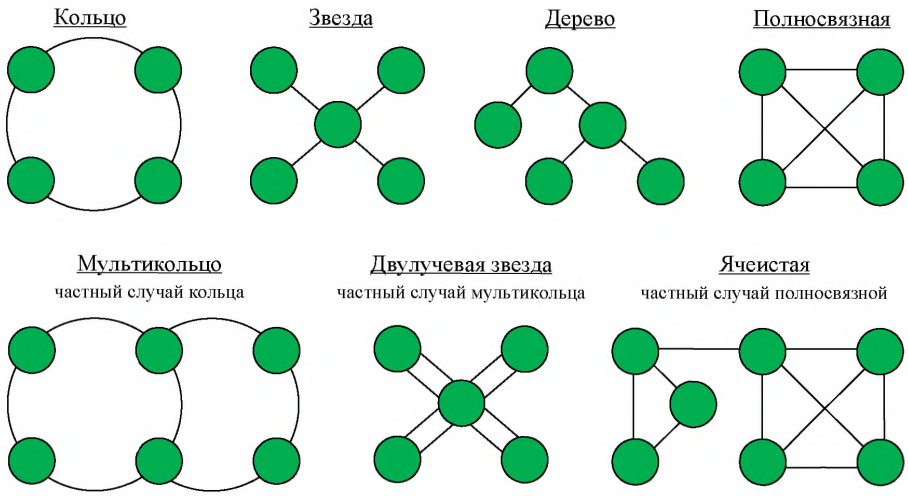


Рисунок 4. Топологии сети связи.

9.2.12. Основным критерием выбора технологии и топологии транспортных сетей связи уровня А1 должна являться стоимость реализации и последующего технического обслуживания.

9.2.13. Резервирование каналов и/или оборудования связи на уровне А1 реализуется только при соответствующем технико-экономическом обосновании.

9.2.14. Для построения транспортных сетей уровня А2 возможно применение как собственных линий и средств проводной[9] и беспроводной связи (ВОЛС, ВЧ-связь, РРЛ), так и арендованных ресурсов связи (ОВ и каналы). Приоритетной средой передачи на уровне А2 является ВОЛС.

9.2.15. Для построения транспортных каналов связи уровня А2 возможно применение следующих технологий:

- Ethernet Transport (100BASE-SX, 100BASE-FX, 100BASE-FXWDM, 1000BASE-SX, 1000BASE-LX, 1000BASE-LH, 10GBASE-SR, 10GBASE-LX4, 10GBASE-LR, 10GBASE-ER);
- Оптическая транспортная сеть (OTN);
- Спектральное уплотнение (CWDM, DWDM)[10];

---

[8] Каналы спутниковой связи, мобильной связи, беспроводного узкополосного доступа используют сети операторов связи и являются арендованными.

[9] Применение медных кабельных линий связи и технологии xDSL допускается только при соответствующем технико-экономическом обосновании.

[10] Технологии плотного спектрального уплотнения целесообразно применять на участках магистральной сети требующих большой пропускной способности или имеющей

- Синхронная цифровая иерархия нового поколения (SDH NG)[11];
- Цифровые каналы высокочастотной связи;
- Радиорелейные линии связи;
- Спутниковая связь.

9.2.16. Транспортные сети связи уровня А2 должны предоставлять резервированные линии и средства связи, поэтому наиболее подходящей топологией для данного уровня является «кольцо» или «мультикольцо», не исключается и применение других топологий («двулучевая звезда», «ячеистая», «полносвязная», «гибридная»).

9.2.17. Основным критерием выбора технологии и топологии транспортных сетей связи уровня А2 является соблюдение требований к каналам связи с учетом обеспечения требований концепции «Цифровая трансформация 2030» в среднесрочной перспективе и минимизации капитальных затрат на реализацию и последующее техническое обслуживание как самой сети так и её инфраструктуры.

9.2.18. Топология транспортной сети связи уровня А2 должна обеспечивать минимальную общую протяженность сети, что повысит её надежность, так как распределённые элементы являются наиболее вероятной точкой отказа сети связи.

9.2.19. В топологии транспортной сети связи уровня А2 должны быть использованы ресурсы существующих транспортных сетей ДЗО ПАО «Россети», в случае если они удовлетворяют текущим потребностям и отвечают требованиям, предъявляемым к каналам связи.

9.2.20. Для построения транспортных сетей уровня А3 возможно применение как собственных линий и средств связи, так и арендованных ВОЛС (SMF), либо арендованных у операторов ресурсов (ОВ, каналы связи).

9.2.21. Для построения транспортных каналов связи уровня А3 возможно применение следующих технологий:

- Ethernet Transport (1000BASE-SX, 1000BASE-LX, 1000BASE-LH, 10GBASE-SR, 10GBASE-LX4, 10GBASE-LR, 10GBASE-ER)[12];
- Оптическая транспортная сеть (OTN);
- Спектральное уплотнение (DWDM).

9.2.22. Наиболее подходящей топологией транспортных сетей связи уровня А3 является ячеистая топология (в сетях с ячеистой топологией непосредственно связываются только те узлы, между которыми происходит интенсивный обмен данными, а для обмена данными с остальными узлами, используются транзитные передачи через промежуточные узлы), возможно и применение других топологий («кольцо», «звезда», «полносвязная», «гибридная»).

перспективы по увеличению трафика, а также для организации однопролетного тракта протяженностью выше 200 км.

[11] Применение технологии SDH NG допускается только при соответствующем технико-экономическом обосновании.

[12] Допускается и применение стандартов 40G и 100G при соответствующем технико-экономическом обосновании.

9.2.23. Основным критерием выбора технологии и топологии транспортных сетей связи уровня А3 является соблюдение требований к каналам связи с учетом обеспечений требований концепции «Цифровая трансформация 2030» в среднесрочной и долгосрочной перспективах и минимизации капитальных затрат на реализацию и последующее техническое обслуживание как самой сети, так и её инфраструктуры.

9.2.24. Транспортные сети связи должны объединять распределенные по огромной территории энергообъекты и покрывать большие расстояния. Наиболее подходящими технологиями для покрытия больших расстояний являются спутниковые системы связи и ВОЛС.

9.2.25. Типовые решения построения усилительных трактов по ВОЛС приведены в Приложении В.

9.2.26. Пакетные сети связи должны строиться на базе протокола IP с применением технологий коммутации по меткам (MPLS-TP; IP/MPLS; Segment Routing, SDN[13]).

9.2.27. Для сохранения ранее сделанных инвестиций рекомендуется использовать существующие транспортные сети с достаточной пропускной способностью для организации наложенной MPLS сети.

9.2.28. В качестве протоколов внутренней маршрутизации рекомендуется применять OSPF или IS-IS.

9.2.29. В качестве протокола внешней маршрутизации рекомендуется применять MBGP.

9.2.30. Для создания логической полносвязной топологии в пакетной сети должны быть использованы Route Reflectors.

9.2.31. Дублируемое оборудование пакетных сетей, для повышения надежности, должно быть объединено в общую логическую структуру протоколом VRRP.

9.2.32. Для построения пакетных сетей возможно применение и арендованных у операторов связи сервисов L2 VPN, L3 VPN, IP VPN, APN с последующей организацией MPLS сети поверх арендованных сервисов.

9.2.33. Рекомендуемое значение MTU арендованного сервиса - 1700 байт. MTU данной величины позволит использовать дополнительный MPLS заголовок и средства криптографической защиты информации.

9.2.34. В случае аренды сервиса L2 VPN VPLS есть возможность сразу формировать полносвязную MPLS сеть.

9.2.35. В случае аренды сервиса IP VPN необходимо использовать подход MPLS over GRE.

9.2.36. Типовые механизмы микросегментирования сети связи приведены в Приложении А.

9.2.37. Примеры типовых узлов транспортной сети приведены в Приложении Г, которые должны быть уточнены при конкретном проектировании.

---

[13] Segment Routing и SDN предлагаются как перспективные технологии в пилотных внедрениях.

9.3. Требования к разрабатываемой системе управления ССЭСК

9.3.1. Система управления ССЭСК должна представлять территориально-разнесенную структуру, построенную в соответствии с принципами концепции TMN, описанной в рекомендации ITU-T M.3010, со следующими уровнями:

- Управление сетями связи ПАО «Россети»;
- Управление сетями связи ДЗО ПАО «Россети».

9.3.2. Система управления сетью связи на каждом уровне должна иметь свой единый многофункциональный головной центр управления, организованный на базе ЦУСС, который должен осуществлять контроль сети связи выделенной зоны и взаимодействие с другими центрами управления.

9.3.3. Архитектура и принципы построения системы управления сетью связи должны обеспечивать реализацию задач управления услугами сети связи, оперативно-технического контроля, эксплуатации, технического обслуживания и администрирования разнородного телекоммуникационного оборудования и систем связи, изготовленных различными фирмами-производителями.

9.3.4. Система управления сетью связи должна использовать только открытые протоколы и стандарты.

9.3.5. Система управления сетью связи должна обеспечить выполнение следующих функций:

- Управление процессом устранения отказов;
- Управление конфигурацией сети связи;
- Управление расчетами;
- Управление качеством;
- Управление защитой информации.

9.3.6. При управлении процессом устранения отказов решаются задачи контроля состояния сети связи и её элементов в реальном времени, обнаружения и локализации повреждений, восстановления трафика, оперативного перестроения сети, устранения повреждений, оповещения пользователей о проводимых работах.

9.3.7. При управлении конфигурацией решаются задачи формирования и развития сети связи, создание и сопровождение плана нумерации, реконфигурация сети связи и отдельных её элементов (маршрутизаторов, мультиплексоров, построение карты сети связи и т. д.), планирования услуг, ведения банка данных.

9.3.8. При управлении расчётами решаются задачи сбора данных по предоставляемым средствам и телекоммуникационным услугам, проведения взаимозачётов между участниками предоставления услуг, технических расчётов, касающихся возможностей сетей, регистрации и учёта абонентов.

9.3.9. При управлении качеством решаются задачи сбора и анализа статистических данных по функционированию сетей и их элементов, регулирования трафика, расширения диапазона телекоммуникационных услуг, а также задачи разработки и контроля исполнения соглашений об уровне качества предоставленных услуг (SLA).

9.3.10. При управлении защитой информации решаются задачи разработки мер по обеспечению закрытости информации и контроля их осуществления, защиты баз данных от злонамеренного доступа, мер технической безопасности и охраны объектов связи, составления отчётов о попытках несанкционированного доступа к услугам, защиты целостности и сохранности данных.

9.3.11. В системе управления сетью связи должны поддерживаться следующие логические уровни, описанные в концепции TMN:

- Уровень элементов сети;
- Уровень управления элементами сети;
- Уровень управления сетью связи;
- Уровень управления услугами.

9.3.12. Уровень элементов сети - представляет собой саму сеть связи, то есть объект управления. В качестве сетевых элементов могут рассматриваться каналы связи, коммутаторы, маршрутизаторы, мультиплексоры, усилители и т. д.

9.3.13. Уровень управления элементами сети - представляет собой элементарные системы управления, которые автономно управляют отдельными элементами сети. Этот уровень ответственен за моделирование поведения оборудования и функциональных ресурсов уровня элементов. Атрибуты этих моделей позволяют управлять различными аспектами поведения управляемых ресурсов.

9.3.14. Уровень управления сетью координирует работу элементарных систем управления, позволяя контролировать конфигурацию составных каналов, согласовывать работу транспортных подсетей разных технологий и т. п.

9.3.15. Уровень управления услугами обеспечивает контроль и управление над телекоммуникационными услугами. В задачу этого уровня входит подготовка сети к предоставлению определенной услуги и её активизации. Формирование услуги заключается в фиксации в базе данных значения параметров услуги, например, требуемой средней пропускной способности, максимальных величин задержек и т. п. В функции этого уровня входит также выдача уровню управления сетью задания на конфигурирование виртуального или физического канала связи для поддержания услуг. После формирования услуги данный уровень занимается контролем качества её реализации.

9.3.16. На всех уровнях решаются задачи одних и тех же пяти функциональных групп (управление устранением отказов, управление конфигурацией сети, управление расчётами, управление качеством, управление защитой информации), однако, на каждом уровне эти задачи имеют свою специфику: чем выше уровень, тем более общий и агрегированный характер должна приобретать собираемая о сети информация.

9.3.17. Степень автоматизации управления должна понижаться с повышением логического уровня управления сетью связи.

9.4. Функциональный состав единого центра управления ССЭСК

9.4.1. Система управления ССЭСК должна разрабатываться как единая информационная система.

9.4.2. Разрабатываемая система управления сетью связи должна строиться по схеме «менеджер - агент». «Менеджер» - часть распределённой системы управления, которая выдаёт указания по работе управления и получает извещения «Менеджер» может работать сразу с группой «агентов» или сам выступать в роли «агента» для «менеджеров» более высокого уровня. «Агент» - часть прикладного процесса, которая управляет взаимосвязанными с ней управляемыми объектами.

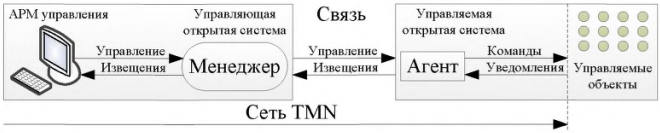


Рисунок 5. Схема взаимодействия между «менеджером», «агентом» и управляемыми объектами.

9.4.3. В едином центре управления ССЭСК должна размещаться разрабатываемая аппаратно-программная часть «менеджера» и оперативно-технический персонал, отвечающий за оперативный контроль состояния и организацию работ по оперативному купированию последствий отказов элементов ССЭСКС.

9.4.4. «Менеджер» должен обладать следующим функционалом:

- Поддержка проводных и беспроводных устройств связи;
- Мониторинг работы сети, поиск и устранение неисправностей;
- Управление конфигурациями сетевых устройств;
- Инвентаризация сетевых устройств;
- Создание отчетов;
- Централизованный просмотр данных о сетевых неисправностях и событиях, включая syslog (регистрации сообщений о происходящих в системе событиях, то есть создания событийных журналов), events (сообщений о происходящих в системе событиях), traps (сообщения о производимых действиях над системой или её элементами, а также попытка действий) и alarms (сообщения об аварийном или предаварийном состоянии системы или её элементов);
- Встроенная визуальная интерактивная модель сети, отображающая топологию сети, соединения, бизнес-подразделения и иерархическую структуру контролируемых организации;
- Встроенная процедура поиска неисправностей;
- Встроенная процедура устранения неисправностей;
- Встроенная процедура поиска уязвимостей ПО сетевого оборудования и планирования мероприятий по их устранению;

- Возможность опроса устройств по SNMP для определения доступности и производительности;
- Возможность интеграции с модулями сетевого мониторинга устанавливаемыми непосредственно в сетевые устройства;
- Обнаружение типичных проблем самостоятельно, без необходимости задания пользовательских правил, SNMP-трапов или задания интервалов опроса устройств;
- Поддержка управления конфигурациями устройств;
- Обеспечение применения рекомендованных производителем сетевого оборудования шаблонов конфигураций устройств;
- Поддержка дистанционного обновление системного программного обеспечения;
- Формирование VLAN, VPN, VRF, VPLS, VPWS, TE-туннелей;
- Обнаружение различий в рабочей и стартовой конфигурации;
- Выполнение работ на основе заданного расписания;
- Хранение архивов конфигураций сетевых устройств;
- Регистрация изменений в конфигурационных файлах и формирование отчетов об изменениях;
- Создание шаблонов конфигурации;
- Поддержка конфигурации объединения двух физических коммутаторов в один виртуальный коммутатор;
- Поддержка работы с коммутаторами, объединенными в стек;
- Проведение периодической инвентаризации сетевого аппаратного и программного обеспечения;
- Поддержка интеллектуального автоматического обнаружения сетевых устройств, в том числе с использованием протокола LLDP, соединений канального уровня между ними и информации о VLAN от протокола управления виртуальными сетями и обмена информацией о виртуальных сетях между сетевыми устройствами, входящими в административный домен;
- Возможность создавать, удалять и редактировать VLAN, VPN, VRF, VPLS, VPWS, TE-туннели;
- Возможность отслеживать маршруты, построенные OSPF, IS-IS, MBGP, LDP, RSVP-TE;
- Набор инструментов, коррелирующих соответствие MAC-адреса, IP-адреса и порта коммутатора конечного пользователя;
- Поддержка интеграции с пользовательскими доменами и системами аутентификации для более эффективного поиска и локализации пользователя/устройства по его идентификатору/MAC-адресу;
- Инструментарий анализа пути сетевого трафика для второго и третьего уровня эталонной модели OSI с возможностью указания в качестве параметра имени устройства или IP-адреса. Результат поиска пути сетевого трафика должен отображаться на экране карты сети, в табличной форме или в виде вывода трассировки;

- Контроль производительности сети для обеспечения IP-сервисов (характеристик потери пакетов, задержки, вариации задержки, доступности сервиса), включающий сбор и анализ статистики, планирование развития сети;
- Поддержка функционала анализа трафика;
- Сбор статистики по сетевому трафику на сеансовом уровне OSI и ниже при помощи специализированных протоколов (Netflow, sFlow, NetStream, Cflow, Jflow и т.п.) работающих по принципу сенсор - коллектор - анализатор. Сенсор собирает статистику по проходящему через него трафику (детектирование потоков, характеризуемых следующими параметрами: адрес источника/назначения (MAC, IP), порты источника/назначения (TCP, UDP), тип и код сообщения для ICMP, источник/назначение AS, Source Peer AS, URL источника/назначения и т. п.). Коллектор агрегирует полученные данные от сенсоров. Анализатор проводит анализ данных собранных коллектором и формирует пригодные для чтения человека отчеты;
- Подсчет передаваемого трафика;
- Анализ и планирование пропускной способности сети;
- Отслеживание качества обслуживания (QoS) в сети для произвольного типа приложения;
- Мониторинг производительности и выполнение соглашения об уровне сетевых услуг (IP SLA);
- Поддержка анализа производительности сети путем настройки на сетевом оборудовании обмена с другими сетевыми устройствами синтезируемым трафиком различных типов, в том числе с характеристиками видео трафика, измерения его характеристик, в том числе данных о задержке, вариации задержки, потерях пакетов, порядке отсылки и приема пакетов, пути пакета, времени загрузки данных и анализа полученных результатов. Должна поддерживаться установка пороговых значений и создание аварийных сообщений при переходе порога;
- Поддержка формирования отчетов о результатах функционирования устройств, а также получение и сортировку отчетов о событиях;
- Отображение и автоматическое обновление карт сети с отображением текущего состояния сетевых устройств;
- Управление сетевыми устройствами с использованием графических средств, а также протоколов Telnet, SSH, SNMP, TFTP, RCP;
- Поддержка ролевого доступа администраторов с возможностью назначения полномочий для каждой роли;
- Взаимодействие с серверами RADIUS, TACACS для аутентификации администраторов;
- Графический пользовательский интерфейс, обеспечивающий централизованный мониторинг событий, настройку всех компонентов системы, работу с этажными планами и диагностику неисправностей беспроводной сети;
- Поддержка интеграции с средствами обнаружения вторжений уровня сети;

- Совместимость с контроллерами беспроводной сети и точками беспроводного доступа;
- Поддержка установки на системы виртуализации.

9.5. Требования к элементам архитектуры ССЭСК

9.5.1. При построении ССЭСК должно применяться оборудование, сертифицированное в соответствии с требованиями Минкомсвязи РФ, а также средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании». Применяемое оборудование должно соответствовать текущим техническим требованиям ПАО «Россети».

9.5.2. Применяемое при построении ССЭСК оборудование должно отвечать требованиям следующих стандартов и отраслевых документов:

ГОСТ Р МЭК 60950-1-2014 Оборудование информационных технологий. Требования безопасности. Часть 1. Общие требования;

ГОСТ 12.2.007.0-75 Изделия электротехнические. Общие требования безопасности (с Изменениями №1-4);

ГОСТ 15150-69 Машины, приборы и другие технические изделия. Исполнения для различных климатических районов;

ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи;

ГОСТ 16962.1-89 Изделия электротехнические. Методы испытаний на устойчивость к климатическим внешним воздействующим факторам;

ГОСТ 17516.1-90 Изделия электротехнические. Общие требования в части стойкости к механическим внешним воздействующим факторам;

ГОСТ 30631-99 Общие требования к машинам, приборам и другим техническим изделиям в части стойкости к механическим внешним воздействующим факторам при эксплуатации;

ГОСТ 23216-78 Изделия электротехнические. Хранение, транспортирование, временная противокоррозионная защита, упаковка. Общие требования и методы испытаний;

ГОСТ 30804.4.2-2013 Совместимость технических средств электромагнитная. Устойчивость к электростатическим разрядам. Требования и методы испытаний;

ГОСТ 30804.4.3-2013 Совместимость технических средств электромагнитная. Устойчивость к радиочастотному электромагнитному полю. Требования и методы испытаний;

ГОСТ 30804.4.4-2013 Совместимость технических средств электромагнитная. Устойчивость к наносекундным импульсным помехам. Требования и методы испытаний;

ГОСТ Р 51317.4.5-99 Совместимость технических средств электромагнитная. Устойчивость к микросекундным импульсным помехам большой энергии. Требования и методы испытаний;

ГОСТ Р 51317.4.6-99 Совместимость технических средств электромагнитная. Устойчивость к кондуктивным помехам, наведенным радиочастотными электромагнитными полями. Требования и методы испытаний;

ГОСТ IEC 61000-4-12-2016 Электромагнитная совместимость (ЭМС). Часть 4-12. Методы испытаний и измерений. Испытание на устойчивость к звенящей волне;

ГОСТ Р 51317.4.16-2000 Совместимость технических средств электромагнитная. Устойчивость к кондуктивным помехам в полосе частот от 0 до 150 кГц. Требования и методы испытаний;

ГОСТ Р 51317.4.17-2000 Совместимость технических средств электромагнитная. Устойчивость к пульсациям напряжения электропитания постоянного тока. Требования и методы испытаний;

ГОСТ Р 51317.6.5-2006 Совместимость технических средств электромагнитная. Устойчивость к электромагнитным помехам технических средств, применяемых на электроподстанциях и подстанциях. Требования и методы испытаний;

ГОСТ 30805.22-2013 Совместимость технических средств электромагнитная. Оборудование информационных технологий. Радиопомехи индустриальные. Нормы и методы измерений;

ГОСТ Р 51320-99 Совместимость технических средств электромагнитная. Радиопомехи индустриальные. Методы испытаний технических средств - источников индустриальных помех;

ГОСТ Р 50648-94 Совместимость технических средств электромагнитная. Устойчивость к магнитному полю промышленной частоты. Технические требования и методы испытаний;

ГОСТ Р 50649-94 Совместимость технических средств электромагнитная. Устойчивость к импульсному магнитному полю. Технические требования и методы испытаний;

ГОСТ Р 50652-94 Совместимость технических средств электромагнитная. Устойчивость к затухающему колебательному магнитному полю. Технические требования и методы испытаний;

ГОСТ IEC 61000-4-29-2016 Электромагнитная совместимость (ЭМС). Часть 4-29. Методы испытаний и измерений. Испытания на устойчивость к провалам напряжения, кратковременным прерываниям и изменениям напряжения на входном порте электропитания постоянного тока;

ГОСТ 13109-97 Электрическая энергия. Совместимость технических средств электромагнитная. Нормы качества электрической энергии в системах электроснабжения общего назначения;

ГОСТ Р 52863-2007 Защита информации. Автоматизированные системы в защищенном исполнении. Испытания на устойчивость к преднамеренным силовым электромагнитным воздействиям. Общие требования;

ГОСТ Р МЭК 60605-6-2007 Надежность в технике. Критерии проверки постоянства интенсивности отказов и параметра потока отказов.

ГОСТ 21552-84 Средства вычислительной техники. Общие технические требования, приемка, методы испытаний, маркировка, упаковка, транспортирование и хранение;

ГОСТ 14254-2015 Степени защиты, обеспечиваемые оболочками;

ГОСТ Р ИСО/МЭК 15408 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий;

ГОСТ Р МЭК 60605-6-2007 Надежность в технике. Критерии проверки постоянства интенсивности отказов и параметра потока отказов;

ГОСТ IEC 60825-2-2013 Безопасность лазерной аппаратуры. Часть 2. Безопасность волоконно-оптических систем передачи;

Правила применения оборудования цифровых систем передачи плезиохронной цифровой иерархии. Часть III. Правила применения каналообразующего оборудования плезиохронной цифровой иерархии, утвержденные приказом Минкомсвязи России от 06.06.2007 № 60;

Правила применения оборудования автоматизированных систем управления и мониторинга средств связи, выполняющих функции транспортных систем, утвержденные приказом Минкомсвязи России от 19.06.2007 № 68;

Об утверждении требований к каналам связи для функционирования релейной защиты и автоматики, утвержденные приказом Минэнерго России от 13.02.2019 № 97;

Правила применения оборудования проводных и оптических систем передачи абонентского доступа, утвержденные приказом Минкомсвязи России от 24.08.2006 № 112;

Правила применения оконечного оборудования, выполняющего функции систем коммутации, утвержденные приказом Минкомсвязи России от 24.08.2006 № 113;

Правила применения оборудования коммутации и маршрутизации пакетов информации, утвержденные приказом Минкомсвязи России от 06.12.2007 № 144;

Правила применения цифровых систем передачи синхронной цифровой иерархии, утвержденные приказом Минкомсвязи России от 23.11.2006 № 151;

Правила применения оборудования, реализующего технологии коммутации кадров, утвержденные приказом Минкомсвязи России от 07.12.2006 № 158;

СТО 34.01-9.3-003-2019 Технические требования к диспетчерским системам цифровой радиосвязи стандарта DMR;

СТО 34.01-6-005-2019 Коммутаторы энергообъектов. Общие технические требования;

СТО 34.01-9.1-002-2018 Оборудование ВЧ-связи для передачи сигналов по сетям низкого и среднего напряжения. Общие технические условия;

СТО 34.01-9.1-001-2018 Волоконно-оптические кабели связи. Общие технические требования;

СТО 56947007-33.060.40.125-2012 Общие технические требования к устройствам обработки и присоединения каналов ВЧ связи по ВЛ 35-750 кВ;

СТО 56947007-33.060.70.213-2016 Технологическая связь. Типовые технические требования. Аппаратура малых земных станций спутниковой связи;

СТО 56947007-33.180.10.239-2016 Технологическая связь. Типовые технические требования. Аппаратура цифровых систем передачи информации по ВОК (SDH, PDH, WDM);

СТО 56947007-33.180.10.240-2016 Технологическая связь. Типовые технические требования. Оборудование сети передачи данных. Коммутаторы, маршрутизаторы, межсетевые экраны.

СТО 56947007-33.060.40.177-2014 Технологическая связь. Типовые технические требования к аппаратуре высокочастотной связи по линиям электропередачи;

СТО 56947007-33.060.65.214-2016 Технологическая связь. Типовые технические требования. Аппаратура радиорелейных линий передачи синхронной (SDH) и плезиохронной цифровой иерархий (PDH).

9.5.3. Системы и параметры энергоснабжения элементов ССЭСК должны соответствовать требованиям, указанным в Приказе Минкомсвязи России № 24 от 30.01.2018 «Об утверждении правил применения оборудования электропитания средств связи».

9.6. Обеспечение устойчивости ССЭСК

9.6.1. ССЭСК должна сохранять устойчивость как при воздействии внутренних, так и внешних дестабилизирующих факторов.

9.6.2. Для обеспечения устойчивости сеть связи и её элементы должны отвечать следующим требованиям:

- Структура сети связи должна иметь не менее двух каналов связи между элементами сети (в части каналов связи, используемых для ОТУ объектов диспетчеризации);
- Обеспечение возможности перераспределения каналов связи на основных направлениях передачи;
- Дублирование каналообразующего и сетевого оборудования на объекте по схеме 1+1 (в части каналов связи, используемых для ОТУ объектов диспетчеризации);

- Георезервирование важных сетевых элементов, таких как Route Reflectors, базы данных и сервера системы управления и т. п.;
- Организация мониторинга активного телекоммуникационного оборудования и каналов связи;

9.6.3. Рекомендуется организовывать мониторинг ВОЛС на важных направлениях передачи (при соответствующем технико-экономическом обосновании);

9.6.4. Внесение изменений в архитектуру сети или в настройки важных сетевых элементов должно сопровождаться предварительным тестированием при помощи технологии «песочница»;

9.6.5. Использование в сети связи протоколов, обеспечивающих быструю сходимость (RSTP, MSTP, mcLAG) и ремаршрутизацию (IS-IS, OSPF, LDP, RSVP-TE);

9.6.6. Организация передачи критически важных данных с верификацией (использование не менее двух равнозначных, независимых каналов связи и сверки полученных данных на приемной стороне);

9.6.7. Организация электропитания оборудования связи на узлах уровня А1 по второй категории электроснабжения, на узлах уровня А2 и А3 по первой категории особой группы электроснабжения.

10. Принципы межсетевого взаимодействия ССЭСК

Взаимодействие сетей связи ДЗО ПАО «Россети», АО «СО ЕЭС», сетей связи иных организаций и ССОП необходимо для полноценной реализации сервисов ССЭСК.

10.1. Принципы и условия взаимодействия сегментов ССЭСК

10.1.1. Взаимодействие сегментов ССЭСК определяется необходимостью обмена информацией между различными технологическими, корпоративными, мультимедийными и служебными информационными системами.

10.1.2. Взаимодействие между сегментами ССЭСК должно происходить на сетевом уровне модели OSI или выше, причем перечень портов взаимодействия и протоколов маршрутизации должен быть минимизирован.

10.1.3. В качестве граничных маршрутизаторов с информационно-телекоммуникационной сетью «Интернет», а также при организации сетевого взаимодействия объектов критической информационной инфраструктуры с другими ДЗО ПАО «Россети», АО «СО ЕЭС», сетями связи иных организаций должны применяться межсетевые экраны, сертифицированные ФСТЭК России на соответствие требованиям по безопасности информации (тип «А», тип «Б» и тип «Г» в терминах приказа ФСТЭК России от 9 февраля 2016 г. N 9), а также средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети.

10.1.4. При организации каналов связи через сети связи общего пользования или использования ресурсов сети электросвязи, не

принадлежащих субъекту критической информационной инфраструктуры на праве собственности, должна обеспечиваться защита передаваемой по сети связи информации от несанкционированного доступа за счет использования технологии VPN и средств криптографической защиты информации (СКЗИ), если применение СКЗИ обусловлено требованиями действующего законодательства в сфере защиты информации и актуальной моделью угроз безопасности информации.

10.1.5. Для предотвращения отправки несанкционированных команд на аппаратуру телеуправления, работающую по протоколу DNP3, OPC, ICCP, Modbus, МЭК61850/60870-101/104, Profibus, CAN, HART и других, инкапсулированных в протокол TCP/IP, необходимо использовать межсетевые экраны уровня промышленной сети (тип «Д» в терминах приказа ФСТЭК России от 9 февраля 2016 г. N 9).

10.1.6. Для взаимодействия с технологического сегмента сети передачи данных с внешними сетями и системами должны создаваться «демилитаризованные» зоны - сегменты сети, которые обслуживают внешние сетевые запросы и соединения и из которых исключена возможность инициации соединений в технологические сегменты сети ДЗО ПАО «Россети». При этом «демилитаризованные» зоны должны быть выделены физически на канальном уровне (при наличии технической возможности без нанесения ущерба технологическому процессу).

10.1.7. В настройках телекоммуникационного оборудования должны быть включены функции, защищающие от подмены сетевых адресов и меры защиты от внедрения ложной маршрутной информации в протоколы маршрутизации, а также функции журналирования в объеме, достаточном для проведения расследований технологических нарушений.

10.1.8. Все предустановленные «по умолчанию» в настройках телекоммуникационного оборудования пароли, а также учетные записи должны быть изменены до включения оборудования в состав ССЭСК.

10.1.9. Все функции телекоммуникационного оборудования незадействованные в процессе передачи информации должны быть отключены, физические сетевые интерфейсы заблокированы.

10.2. Принципы и условия взаимодействия сетей связи ДЗО ПАО «Россети», входящих в состав ССЭСК

10.2.1. В рамках сети связи ДЗО и для обеспечения возможности выполнения ЦУС операционных функций должно быть организовано не менее двух независимых цифровых каналов связи достаточной пропускной способности для ведения оперативных переговоров и передачи телеинформации в каждом канале. Указанные каналы должны быть организованы:

- Между ЦУС ДЗО и ЦУСС;
- Между ЦУС ДЗО и ДЦ АО «СО ЕЭС»;
- Между ЦУС и энергообъектами, имеющими в своем составе объекты оперативно-технологического управления ЦУС;

- Между ДЦ АО «СО ЕЭС» и энергообъектами, имеющими в своем составе объекты оперативно-технологического управления ЦУС;
- Между ЦУС и ЭЧ для организации передачи команд оперативного персонала ЦУС оперативному персоналу подстанций ОАО «РЖД» через оперативный персонал соответствующей ЭЧ и передачи телеинформации в ЦУС с подстанций ОАО «РЖД» путем ретрансляции из ЭЧ;
- Между ЦУС ДЗО в местах географического пересечения;
- Между смежными ЦУС (в случае организации передачи команд оперативного персонала ЦУС оперативному персоналу энергообъектов, находящихся в зоне эксплуатационной ответственности смежной сетевой организации, через оперативный персонал ЦУС этой сетевой организации, выполняющего операционные функции в отношении таких энергообъектов, а также при организации передачи телеинформации в ЦУС с таких энергообъектов путем ретрансляции из смежного ЦУС).

10.2.2. Для организации каналов связи могут быть использованы телекоммуникационные ресурсы субъектов электроэнергетики или иных владельцев на основании Соглашений об обмене технологической информации или договоров на оказание услуг связи.

10.2.3. Таким образом, взаимодействие между ДЗО осуществляется на уровне ЦУС ДЗО.

10.2.4. ССЭСК является системой взаимодействующих сетей связи ДЗО ПАО «Россети». Для взаимного обмена трафиком обособленных сетей связи ДЗО ПАО «Россети», должны быть организованны распределенные узлы обмена трафиком (РУОТ).

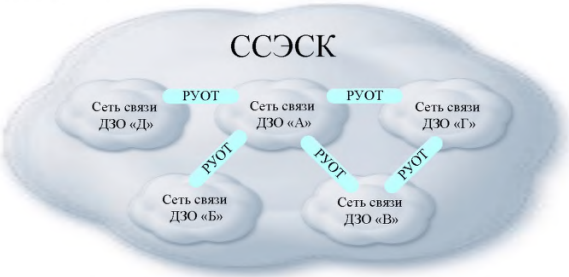


Рисунок 6. ССЭСК как система взаимодействующих сетей связи.

10.2.5. Успешная реализация РУОТ позволяет организовать взаимный обмен трафиком между любыми объектами, подключенными к сети связи ДЗО.

10.2.6. Перед организацией РУОТ необходимо провести работы по нормализации состояния сети связи ДЗО. Для этого необходимо выполнить следующие мероприятия:

- Обеспечить соответствие используемых IP-адресов плану IP-адресации ДЗО (каждому филиалу ДЗО выделяется пул IP-адресов и на каждом

объекте данного филиала используются только IP-адреса из выделенного пула, за исключением реальных IP-адресов);

- Предусмотреть в плане IP-адресации ДЗО пул IP-адресов для взаимодействия с другими ДЗО и сторонними организациями;
- Обеспечить маршрутизацию выделенных пулов IP-адресов не только в рамках отдельного филиала, но и во всей сети связи ДЗО;
- При обмене маршрутной информацией между узлами сети связи ДЗО, необходимо обеспечить передачу от объектов сетевых префиксов, выделенных для этих объектов;
- Передача более специфичных префиксов (с длиной маски больше выделенного сетевого префикса) допускается только для обеспечения нестандартной маршрутизации для отдельных хостов или их групп.
- Каждый филиал должен обмениваться суммарной маршрутной информацией со своими непосредственно подключенными соседями, передавая информацию обо всех выделенных филиалу подсетях или префиксах и получая информацию обо всех подсетях ДЗО, доступных через данный филиал.
- Исключить трансляцию IP-адресов (NAT) внутри сети связи ДЗО.

10.2.7. РУОТ должен выполнять следующие функции:

- Организовать и обеспечивать гарантированную передачу технологической, корпоративной, мультимедийной и служебной информации между сетями связи ДЗО;
- Беспрепятственную передачу и прием всех видов информации без искажения с заданными параметрами;
- Обеспечивать достаточную пропускную способность и производительность оборудования связи для необходимого информационного взаимодействия между ДЗО в нормальном и аварийном режимах работы РУОТ (пропускная способность каналов выбирается на основании расчетов);
- Обеспечивать автоматический обмен и фильтрацию маршрутной информацией между сетями связи ДЗО;
- Производить трансляцию IP-адресов (NAT) в связи с пересечением (наложением) планов IP-адресации ДЗО;
- При необходимости, производить перемаркировку трафика, на основании соглашения между взаимодействующими ДЗО о применяемых политиках QoS;

10.2.8. В целях обеспечения надежного взаимного обмена трафиком между ДЗО должно организовано не менее двух географически разнесенных объектов РУОТ и поддерживаться круглосуточная работа минимум двух независимых, географически разнесенных трактов между сетями связи ДЗО. Применение указанных мер резервирования для организации пропуска транзитного трафика определяется соглашением о транзите трафика между ДЗО.

10.2.9. Связи между объектами РУОТ должны быть организованны по собственным или арендованным ВОЛС. В случае отсутствия возможности

организации связи по ВОЛС, возможно использование арендованных каналов у операторов связи.

10.2.10. Арендованные каналы для связи между объектами РУОТ должны быть организованны на физическом или канальном уровне «классической» семиуровневой модели OSI.

10.2.11. Стыки между сетями связи ДЗО должны быть организованны на сетевом уровне «классической» семиуровневой модели OSI.

10.2.12. Выбор протокола маршрутизации трафика между сетями связи ДЗО должен учитывать специфику существующих сетей связи ДЗО и технические характеристики применяемого маршрутизирующего оборудования.

10.2.13. Маршрутизация трафика между сетями связи ДЗО должна проходить через демилитаризованную зону с применением межсетевого экранирования.

10.2.14. При организации контроля управления трафиком между сетями связи ДЗО на стыковочном маршрутизирующем оборудовании должны применяться стандартные и расширенные списки доступа (access-list, prefix-list, route-map), что позволит решать такие задачи как:

- Обеспечение функционирования NAT;
- Фильтрация трафика;
- Управление обменом маршрутной информацией между сетями связи ДЗО;
- Фильтрация обновлений маршрутной информации;
- Маршрутизация входящего трафика в сети связи ДЗО на основе определенных заданных правил;
- Фильтрации маршрутов;
- Изменение метрики маршрутов.

10.2.15. Инфраструктурные решения на стыке ДЗО не должны влиять на логику работы телекоммуникационной инфраструктуры ДЗО.

10.2.16. Типовая архитектура РУОТ приведена в Приложении Д.

10.2.17. В случае необходимости организации TDM канала между транспортными сетями связи ДЗО особых требований не выдвигается. Правила передачи/транзита TDM трафика между сетями связи ДЗО определяются на основании соглашения.

10.3. Принципы и условия взаимодействия ССЭСК с сетями связи сторонних организаций

10.3.1. С целью оперативного взаимодействия с АО «СО ЕЭС» ДЗО ПАО «Россети» обязано организовать и обеспечивать круглосуточную работу двух независимых (основного и резервного) каналов связи между подстанциями, ЦУС и соответствующим РДУ для передачи в режиме реального времени команд и информации о технологическом режиме работы объектов диспетчеризации, необходимой для управления электроэнергетическим режимом ЕЭС России.

10.3.2. В случае отсутствия (потери) связи между подстанцией и/или ЦУС и соответствующим РДУ оперативный персонал РСК и диспетчерский персонал РДУ (в пределах зоны эксплуатационной ответственности РДУ) обязаны принять меры к восстановлению связи. При этом должны быть использованы любые виды связи.

10.3.3. Каждый канал связи, обеспечивающий функционирование устройств РЗ, осуществляющих функцию основной защиты ЛЭП, должен быть организован по выделенному каналу, независимому от каналов связи для других устройств РЗ той же ЛЭП.

10.3.4. Передача сигналов и команд РЗ должна осуществляться без промежуточной обработки.

10.3.5. При необходимости ДЗО ПАО «Россети» может организовать обмен телеметрической информацией между ЦУС ДЗО ПАО «Россети» с диспетчерскими центрами/центрами управления сетью сторонних организаций, в составе которых имеются объекты диспетчеризации. При этом должна быть обеспечена круглосуточная работа двух независимых (основного и резервного) каналов связи для передачи телеметрической информации.

10.3.6. Для организации каналов связи могут быть использованы телекоммуникационные ресурсы субъектов электроэнергетики или иных владельцев на основании Соглашений об обмене технологической информации или договоров на оказание услуг связи.

10.3.7. Узлы связи ЦУС, ПС, узлы связи электросетевых компаний и других субъектов электроэнергетики должны подключаться к Сети связи ЭСК в сетевых узлах сети связи ЭСК не менее чем двумя взаимно резервируемыми независимыми каналами связи с пропускной способностью определяемой проектом и действующей НТД. При этом для организации информационного обмена должны взаимно использоваться ресурсы телекоммуникационных инфраструктур ПАО «Россети» и ДЗО, АО «СО ЕЭС» и других субъектов электроэнергетики.

10.3.8. Технологическая информация, необходимая для планирования и управления электроэнергетическим режимом энергосистемы, может передаваться посредством каналов связи, организованных в сетях операторов связи или технологических сетях связи иных лиц, в том числе субъектов электроэнергетики. В соответствии с Правилами технологического функционирования электроэнергетических систем, утвержденных Постановлением Правительства Российской Федерации от 13.08.2018 № 937:

- Владельцы объектов электроэнергетики и потребители организуют наличие и обеспечивают функционирование двух независимых каналов связи объекта электроэнергетики с каждым ДЦ, к объектам диспетчеризации которого относятся соответствующие линии электропередачи, оборудование и устройства;
- Сетевые организации, иные владельцы объектов электросетевого хозяйства организуют наличие и обеспечивают функционирование двух независимых каналов связи объекта электросетевого хозяйства высшим классом напряжения 110 киловольт и более с ЦУС, в технологическом

управлении и технологическом ведении которого находятся оборудование или устройства указанного объекта электросетевого хозяйства или отходящие от него линии электропередачи.

10.3.9. В случае осуществления деятельности ДЗО ПАО «Россети» по передаче технологической информации в интересах сторонних владельцев объектов электроэнергетики, в т.ч объектов другого ДЗО ПАО «Россети», возникающие при этом взаимоотношения между ДЗО ПАО «Россети», а также между ДЗО ПАО «Россети» и иными владельцами объектов электроэнергетики должны оформляться в соответствии с действующими нормами гражданского законодательства РФ соответствующими возмездными договорами, предметом которых должна быть передача технологической информации в вышеуказанных целях.

10.3.10. Деятельность ДЗО ПАО «Россети» по передаче технологической информации в интересах сторонних владельцев объектов электроэнергетики не требует лицензии на осуществление деятельности в области оказания услуг связи.

10.4. Принципы и условия взаимодействия ССЭСК с сетью связи общего пользования

10.4.1. Для организации независимых цифровых каналов связи могут использоваться собственные или арендованные каналы, каналы субъектов электроэнергетики или иных владельцев, организованные по волоконно-оптическим линиям связи (ВОЛС), ВЧ-связи по ВЛ с цифровой обработкой сигналов, цифровым радиорелейным линиям связи (ЦРРЛ), каналы виртуальной частной сети.

10.4.2. В случае использования арендованных ресурсов ССОП, к каналам связи предъявляются требования, описанные п. 7 настоящего стандарта. В случае, если с использованием арендованных каналов связи предполагается организация нескольких сервисов ССЭСК, то применяются наиболее жесткие требования из перечня.

10.5. Основные положения предоставления сторонним организациям сетевых ресурсов ССЭСК и доступа к инфраструктурным объектам ДЗО

10.5.1. Сетевые ресурсы ССЭСК приоритетно используются в интересах ПАО «Россети» и ДЗО ПАО «Россети».

10.5.2. При наличии свободных сетевых ресурсов ССЭСК ДЗО ПАО «Россети» могут предоставлять сторонним субъектам электроэнергетики на договорной основе услуги по передаче технологической информации.

10.5.3. Предоставление сторонним организациям доступа к инфраструктурным объектам ДЗО ПАО «Россети» для размещения элементов сетей электросвязи (включая ВОК) в случае отнесения ДЗО к субъектам естественной монополии, регулирование деятельности которого осуществляется в соответствии с Федеральным законом от 17 августа 1995 г. № 147-ФЗ «О естественных монополиях», должно осуществляться на

договорной основе в соответствии с Правилами недискриминационного доступа к инфраструктуре для размещения сетей электросвязи, утвержденных постановлением Правительства Российской Федерации от 29.11.2014 № 1284.

10.5.4. В случае, если предполагаемая трасса размещения ВОК на инфраструктурных объектах ДЗО ПАО «Россети» представляет интерес для ДЗО в рамках развития собственной сети связи, ДЗО может предусмотреть в договоре на предоставление доступа к инфраструктурным объектам передачу ОВ в качестве оплаты.

10.5.5. Сетевые ресурсы ССЭСК используются только в интересах ПАО «Россети» и ДЗО ПАО «Россети».

10.5.6. При наличии свободных сетевых ресурсов ССЭСК ДЗО ПАО «Россети» могут предоставлять сторонним субъектам электроэнергетики на договорной основе услуги по передаче технологической информации.

10.5.7. Предоставление сторонним организациям доступа к инфраструктурным объектам ДЗО ПАО «Россети» для размещения элементов сетей электросвязи (включая ВОК) в случае отнесения ДЗО к субъектам естественной монополии, регулирование деятельности которого осуществляется в соответствии с Федеральным законом от 17 августа 1995 г. № 147-ФЗ «О естественных монополиях», должно осуществляться на договорной основе в соответствии с Правилами недискриминационного доступа к инфраструктуре для размещения сетей электросвязи, утвержденными постановлением Правительства Российской Федерации от 29.11.2014 № 1284.

10.5.8. В случае, если предполагаемая трасса размещения ВОК на инфраструктурных объектах ДЗО ПАО «Россети» представляет интерес для ДЗО в рамках развития собственной сети связи, ДЗО может предусмотреть в договоре на предоставление доступа к инфраструктурным объектам передачу ОВ в качестве оплаты.

11. Информационная безопасность ССЭСК

11.1. Граница раздела ССЭСК и внутриобъектовых локальных сетей связи проходит через порты доступа (физические или виртуальные) каналообразующего или коммутационного оборудования ССЭСК, на которых должны применяться политики, описывающие тот перечень ресурсов ССЭСК к которым имеет доступ конкретная внутриобъектовая сеть.

11.2. Объектами защиты (объектам критической информационной инфраструктуры) в контексте обеспечения безопасности информационной инфраструктуры и обрабатываемой информации ССЭСК являются:

- корпоративные и технологические информационно-телекоммуникационные сети (в том числе телекоммуникационное оборудование, программное обеспечение, система управления,), формирующие единое информационное пространство и цифровую среду взаимодействия;
- сети электросвязи, используемые для организации взаимодействия объектов КИИ;

- архитектура и конфигурация информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, персональные данные, иная критически важная (технологическая) информация, в том числе представляющая коммерческую ценность в силу неизвестности третьим лицам.

11.3. Система безопасности ССЭСК должна создаваться в соответствии с требованиями и положениям Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», а также соответствующими подзаконными нормативно-правовыми актами как типовой территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения компьютерных атак и ликвидации последствий компьютерных инцидентов.

11.4. Принимаемые меры по обеспечению безопасности объектов ССЭСК не должны оказывать отрицательного влияния на функционирование АСТУ, обмен технологической информацией, функций дистанционного управления электросетевым оборудованием и интеллектуальными электронными устройствами.

11.5. Организационные и технические меры по обеспечению информационной безопасности объектов ССЭСК должны обеспечивать:

- предотвращение неправомерного доступа к обрабатываемой информации, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
- недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование системы и обеспечивающих (управляемых, контролируемых) им процессов;
- восстановление функционирования технических средств обработки информации, а также обрабатываемой информации.

11.6. На стадиях (этапах) жизненного цикла в ходе создания (модернизации) проводится:

- анализ угроз безопасности информации и разработка модели угроз безопасности или ее уточнение (при ее наличии), определение категории значимости, уровня защищенности элементов ССЭСК;
- проектирование организационных и технических мер по обеспечению информационной безопасности, разработка рабочей (эксплуатационной) документации;

- внедрение организационных и технических мер по обеспечению информационной безопасности, ввод в действие, оценка соответствия в форме испытаний или приемки;
- регламентация процессов эксплуатации.

11.7. Основные технические решения, проектная и рабочая (эксплуатационная) документация на создаваемые/модернизируемые элементы ССЭСК должна быть согласована с подразделением, выполняющим в ДЗО ПАО «Россети» функции обеспечения информационной безопасности.

В составе эксплуатационной документации на элементы ССЭСК предусмотреть разработку разделов:

- обеспечения информационной безопасности объекта в ходе его эксплуатации;
- действий персонала по восстановлению информации и штатного функционирования объекта в случае возникновения нештатных ситуаций в результате которых нарушено и (или) прекращено функционирование объектов информационной инфраструктуры;
- обеспечения информационной безопасности объекта при выводе его из эксплуатации.

11.8. Ввод в эксплуатацию ССЭСК или составных частей допускается только при наличии протокола (акта) приемочных испытаний с положительным заключением о соответствии и эффективности подсистемы безопасности установленным требованиям по обеспечению безопасности.

11.9. Для обеспечения безопасности информационно-телекоммуникационных сетей, входящих в состав элементы ССЭСК, настоящие требования применяются наряду с нормативными правовыми актами федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи, а также ГОСТ Р 62443 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы», ГОСТ Р 56498-2015 МЭК 62443-3:2008 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления.

11.10.В зависимости от их категории значимости и угроз безопасности информации в системе безопасности ССЭСК должны быть реализованы следующие организационные и технические меры защиты:

- идентификация и аутентификация (ИАФ);
- управление доступом (УПД);
- ограничение программной среды (ОПС);
- защита машинных носителей информации (ЗНИ);
- аудит безопасности (АУД);
- антивирусная защита (АВЗ);
- предотвращение вторжений (компьютерных атак) (СОВ);
- обеспечение целостности (ОЦЛ);

- обеспечение доступности (ОДТ);
- защита технических средств и систем (ЗТС);
- защита информационной (автоматизированной) системы и ее компонентов (ЗИС);
- планирование мероприятий по обеспечению безопасности (ПЛН);
- управление конфигурацией (УКФ);
- управление обновлениями программного обеспечения (ОПО);
- реагирование на инциденты информационной безопасности (ИНЦ);
- обеспечение действий в нештатных ситуациях (ДНС);
- информирование и обучение персонала (ИПО).

11.11. Технические меры по обеспечению информационной безопасности ССЭСК реализуются посредством использования программных и программно-аппаратных средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение).

11.12. Базовый набор технических мер защиты в системе безопасности ССЭСК включает:

- средства защиты информации от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение) к АРМ, промышленному серверному и телекоммуникационному оборудованию;
- межсетевые экраны уровня сети, средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети;
- средства антивирусной защиты потовых и веб-серверов, файловых хранилищ и рабочих станций;
- средства криптографической защиты информации, передающейся по каналам передачи данных, а также двухфакторной аутентификации удаленных абонентов;
- средства резервного копирования.

11.13. К элементам управления ССЭСК не допускается:

- наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками ДЗО ПАО «Россети»;
- наличие локального доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками ДЗО ПАО «Россети» без контроля со стороны ДЗО ПАО «Россети»;
- передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе средств защиты информации, или иным лицам без контроля со стороны ДЗО ПАО «Россети».

11.14. Удаленный доступ к интерфейсам управления ССЭСК предоставляется посредством средств криптографической защиты информации, а также двухфакторной аутентификации удаленных абонентов.

11.15. Удалённое управление элементами ССЭСК должно быть организовано по протоколам, обеспечивающим криптографическую защиту всего передаваемого трафика, включая пароли. Например, по протоколу SSH.

11.16. Входящие в состав ССЭСК программные и программно-аппаратные средства, осуществляющие хранение и обработку информации, должны размещаться на территории Российской Федерации (за исключением случаев, когда размещение указанных средств осуществляется в зарубежных обособленных подразделениях Субъекта (филиалах, представительствах), а также случаев, установленных законодательством Российской Федерации и (или) международными договорами Российской Федерации).

11.17.Входящие в состав ССЭСК программные и программно-аппаратные средства не должны иметь ограничений со стороны разработчиков (производителей) или иных лиц на применение этих средств на всей территории Российской Федерации.

11.18.Эксплуатационно-техническое обслуживание, техническая поддержка входящего в состав ССЭСК телекоммуникационного оборудования, программного обеспечения и СУБД должна оказываться Правообладателем или представителем Правообладателя (юридическим лицом), зарегистрированным на территории Российской Федерации.

11.19. Не допускается применение в составе ССЭСК алгоритмов SHA-1, протоколов SNMP v1, v2.

12. Техническое обслуживание и эксплуатация ССЭСК

12.1. Техническая эксплуатация ССЭСК осуществляется в соответствии с Правилами технической эксплуатации электрических станций и сетей Российской Федерации, Правилами технической эксплуатации первичных сетей взаимоувязанной сети связи Российской Федерации, Правилами организации технического обслуживания и ремонта объектов электроэнергетики и другими действующими НПА и НТД.

12.2. Техническая эксплуатация ССЭСК осуществляется на уровне ДЗО с учётом требований по предоставлению тех или иных сервисов.

12.3. Техническая эксплуатация ССЭСК включает в себя работы:

- Техническое обслуживание;
- Текущий ремонт;
- Капитальный ремонт;
- Устранение аварий.

12.4. Организацию технического обслуживания ССЭСК осуществляет соответствующие подразделения ДЗО ПАО «Россети». В состав мероприятий по ТО ССЭСК входят мероприятия по ТО линейных сооружений и мероприятия по ТО оборудования.

12.5. Перечень мероприятий по ТО линейных сооружений формируется исходя из физической реализации линии связи. Вне зависимости от физической реализации, планово-профилактические мероприятия должны выполняться не реже одного раза в год (осмотры, измерения, юстировка).

12.6. Перечень мероприятий по ТО оборудования определяется исходя из рекомендаций производителя оборудования.

12.7. Текущий ремонт - минимальный по объемам вид планового ремонта, при котором производятся работы по систематическому и своевременному предохранению линейных сооружений и оборудования от преждевременного износа.

12.8. Капитальный ремонт - наибольший по объему вид планового ремонта, при котором производится смена изношенных частей и конструкций линейных сооружений, замена или ремонт с выводом из эксплуатации оборудования связи.

12.9. Капитальный ремонт линейных сооружений и оборудования выполняется специализированными подрядными организациями.

12.10.Вне зависимости от сроков проведения планово-профилактических работ на ССЭСК, должна быть обеспечена работа по поддержанию круглосуточной аварийной готовности в режиме 24/7/365.

12.11.Аварийная готовность может осуществляться как силами ДЗО, так и с привлечением подрядных организаций.

12.12.С целью организации аварийных работ на ССЭСК рекомендуется применять алгоритм прохождения заявки, изображенный на Рисунке 7.

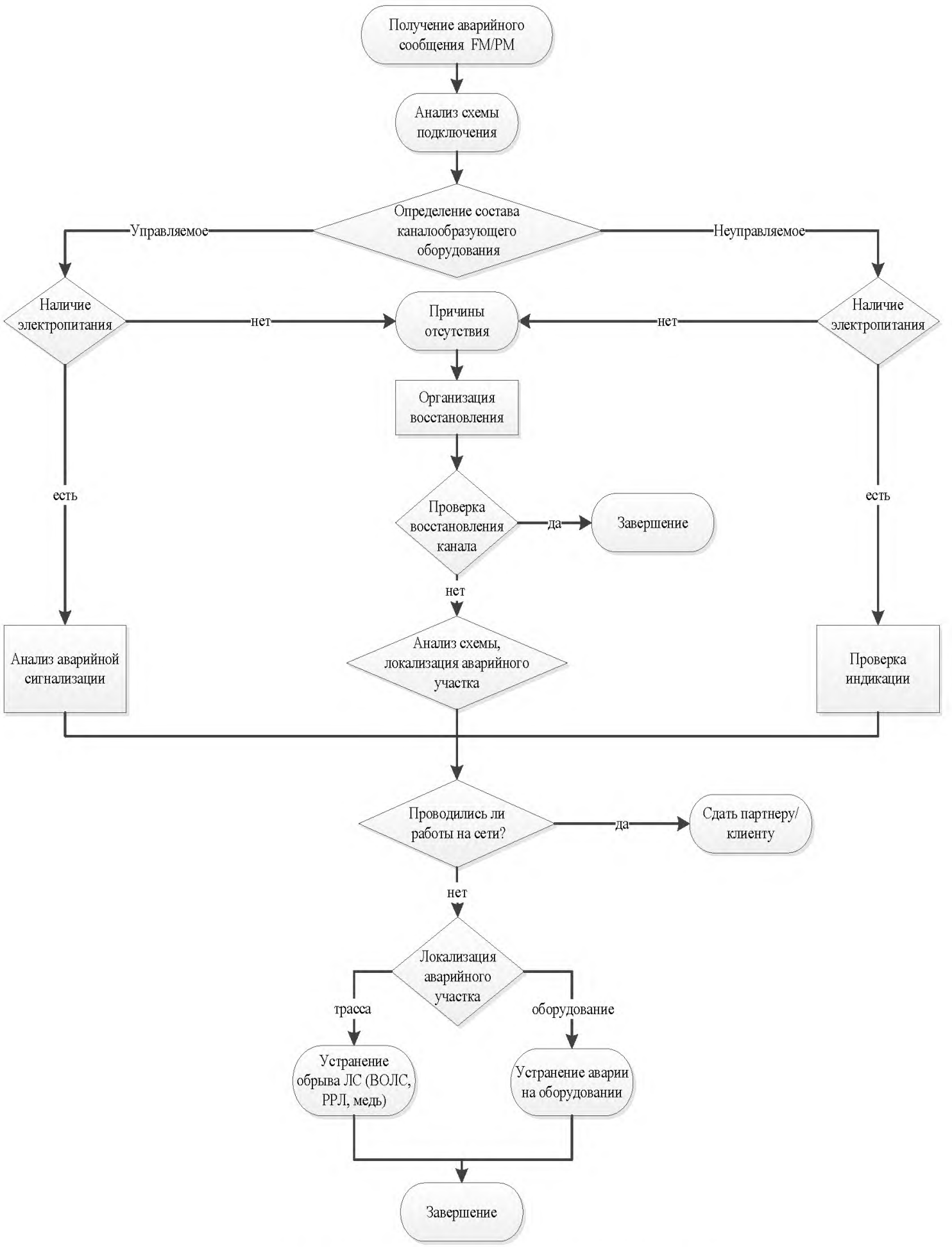


Рисунок 7. Алгоритм прохождения заявки.

13. Нормативно-правовое обеспечение деятельности ССЭСК

Таблица 2 - Нормативно-правовое обеспечение деятельности ССЭСК

п/п	Документ	Содержание документа в части рекомендаций (требований) по реализации технических решений
1.	СТО 34.01-21-005-2019 Цифровая электрическая сеть. Требования к проектированию цифровых распределительных электрических сетей 0,4-220 кВ	В данном стандарте установлены требования к цифровым электрическим сетям 0,4-220 кВ (далее ЦЭС) и их элементам; показана структура ЦЭС с определением в ней (структуре) места технологической сети передачи данных; заданы общие требования к организации информационных потоков подсистем программно-технического комплекса ЦЭС, а также заданы общие требования к системам связи ЦЭС и приведены требования по организации информационной безопасности ЦЭС. В приложении к данному стандарту приведено описание и состав информационных потоков в рамках цифровой электрической сети.
2.	СТО 34.01-21-004-2019 Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ	В данном стандарте установлены требования к технологическому проектированию цифровых питающих центров (цифровых подстанций высшим напряжением 110-220 кВ и узловых цифровых подстанций высшим напряжением 35 кВ); обозначены интерфейсы взаимодействия цифровых подстанций и узловых цифровых подстанций с цифровыми электрическими сетями; приведен перечень используемых протоколов передачи данных; заданы общие требования к системам связи и сети передачи данных между программно-техническим комплексом (далее ПТК) цифровой ПС и ПТК управления ЦЭС; задано требование по сегментированию услуг на уровне ЦПС по средствам виртуальных локальных сетей; приведены требования по организации информационной безопасности ЦПС.
3.	СТО 56947007-29.240.10.256-2018 Технические требования к аппаратно-программным средствам и электротехническому оборудованию цифровых подстанций	В данном стандарте установлены нормы и требования к аппаратно-программным средствам ЦПС, устройствам, обеспечивающим информационные связи ЦПС, устройствам и системам синхронизации времени для ЦПС, а также заданы требования по информационной безопасности предъявляемые к программно-аппаратному комплексу ЦПС.
4.	СТО 34.01-21.1-001-2017 Распределительные электрические сети напряжением 0,4-110 кВ. Требования к технологическому проектированию	В данном стандарте установлены основные требования к проектированию ВЛ, КЛ, КВЛ, ТП, РП, СП, ПС напряжением 0,4-110 (150) кВ. В главе 9.12 заданы общие требования к проектированию сетей и каналов связи для распределительных электрических сетей напряжением 0,4-110 (150) кВ, обобщающие и дополняющие Положения ПАО «Россети» о Единой технической политике в электросетевом комплексе.

п/п	Документ	Содержание документа в части рекомендаций (требований) по реализации технических решений
5.	СТО 56947007-29.240.10.248-2017 Нормы технологического проектирования подстанций переменного тока с высшим напряжением 35-750 кВ	В данном стандарте установлены основные требования по проектированию подстанций (ПС), распределительных пунктов (РП) и переключательных пунктов (ПП) переменного тока ПАО «ФСК ЕЭС» с высшим напряжением 35-750 кВ. В главе 15 заданы общие требования к каналам связи для объектов ПАО «ФСК ЕЭС» с высшим напряжением 35-750 кВ.
6.	СТО 56947007-29.240.10.167-2014 Информационно-технологическая инфраструктура подстанций. Типовые технические решения	В данном стандарте описаны основные технические решения по проектированию информационно-технологической инфраструктуры подстанций (далее ИТИ ПС); обозначены процессы агрегации и передачи данных прикладных информационных систем с объектового уровня на уровень узла связи транспортной сети; приведены решения по информационной безопасности ИТИ ПС; заданы решения по межсистемному взаимодействию и организации межсистемного обмена информацией.
7.	СТО 34.01-6.1-001-2016 Программно-технические комплексы подстанций 6-10 (20) кВ. Общие технические требования	В данном стандарте описаны основные технические требования к программно-техническим комплексам автоматизированной системы оперативно-технологического и ситуационного управления (далее ПТК) в части, обеспечивающей автоматизацию оперативного управления основным технологическим процессом ПС 6-10 (20) кВ и взаимодействия с обособленными системами ПС (ТП, РП, РТП) - РЗА, АСУЭ и пр. В главе 6.4 заданы требования по обмену информацией ПТК с обособленными системами и вышестоящими уровнями управления.
8.	СТО 34.01-6.1-002-2016 Программно-технические комплексы подстанций 35-110 (150) кВ. Общие технические требования	В данном стандарте описаны основные технические требования к программно-техническим комплексам автоматизированной системы оперативно-технологического и ситуационного управления в части, обеспечивающей автоматизацию оперативного управления основным технологическим процессом ПС 35-110 (150) кВ и взаимодействия с обособленными системами ПС - РЗА, АСУЭ и пр. В главе 6.3 заданы требования по обмену информацией ПТК с обособленными системами ПС и вышестоящими уровнями управления.
9.	СТО 70238424.17.220.20.006-2011 Системы связи для сбора и передачи информации в электроэнергетике. Организация эксплуатации и технического обслуживания. Нормы и требования	В данном стандарте описаны нормы и требования по организации эксплуатации и технического обслуживания оборудования систем связи для сбора и передачи информации в электроэнергетике, правила вывода из эксплуатации и утилизации оборудования связи. В приложении к данному стандарту указаны сроки эксплуатации систем и оборудования связи.

п/п	Документ	Содержание документа в части рекомендаций (требований) по реализации технических решений
10.	СТО 56947007-33.180.10.239-2016 Технологическая связь. Типовые технические требования. Аппаратура цифровых систем передачи информации по ВОК (SDH, PDH, WDM)	В данном стандарте установлены требуемые значения параметров интерфейсов и требования к оборудованию xWDM, OTN, Fast Ethernet, Gigabit Ethernet, SDH, V.24/V.28 (RS-232), X.21/V.11 (X.24/X.27, RS-485), RS-449 и электрического интерфейса 2048 кбит/с; требования к параметрам протоколов IP/MPLS; требования к оптическим усилителям xWDM; требования к системе сигнализации оборудовании и требования к контролю и управлению оборудованием, управлению безопасностью, а также различные методики проверки.
11.	СТО 56947007-29.240.036-2009 Руководящие указания по выбору объемов неоперативной технологической информации, передаваемой с подстанций ЕНЭС в центры управления электрическими сетями, а также между центрами управления	В настоящим стандарте приведены общие требования к объемам неоперативной технологической информации (НТИ) различного вида и назначения, передаваемой с подстанций ЕНЭС в центры управления электрическими сетями (ЦУС), а также между центрами управления. Рассматриваемая в настоящем документе технологическая информация является неоперативной, так как к времени и другим условиям её доставки пользователям не предъявляются «жесткие» нормативные требования, в отличии от оперативной информации (телеинформации).
12.	СТО 56947007-29.130.01.092-2011 Выбор видов и объемов телеинформации при проектировании систем сбора и передачи информации подстанций ЕНЭС для целей диспетчерского и технологического управления	В настоящим стандарте приведены общие требования к составу и объемам телеинформации, участвующей в информационном обмене объектов единой национальной (общероссийской) электрической сети (ЕНЭС) с центрами управления электрическими сетями (ЦУС) сетевых организаций и диспетчерскими центрами (ДЦ) ОАО «СО ЕЭС».
13.	СТО 56947007-35.240.01.188-2014 Устройства сбора и передачи данных автоматизированных информационно-измерительных систем коммерческого учета электроэнергии (АИИС КУЭ). Типовые технические требования	В данном стандарте описаны типовые технические требования к устройствам сбора и передачи данных автоматизированных информационно-измерительных систем коммерческого учета электроэнергии. В пункте 2 указаны требования по защищенности АИИС КУЭ, а в пункте 3 указаны функциональные требования по информационному обмену.

п/п	Документ	Содержание документа в части рекомендаций (требований) по реализации технических решений
14.	СТО 70238424.17.220.20.003-2011 Автоматизированные информационно-измерительные системы учета электроэнергии (АИИС УЭ). Условия создания. Нормы и требования	В данном стандарте определены единые правила, нормы и требования к автоматизированным информационно-измерительным системам учета электроэнергии электростанций и трансформаторных подстанций всех классов напряжения, а также Центров сбора информации АИИС УЭ, организуемые в структурах управления генерирующих и сетевых компаний. В главе 6.2.7 заданы технические требования к средствам передачи информации АИИС УЭ.
15.	СТО 56947007-33.060.20.233-2016 Технологическая связь. Руководящие указания по применению средств подвижной радиосвязи	В данном стандарте описаны основные требования и положения создания и эксплуатации систем подвижной радиосвязи, используемых на различных уровнях управления в подразделениях РЭО, ОТУ и СУ филиалов ПАО «ФСК ЕЭС».
16.	СТО 56947007-33.060.70.213-2016 Технологическая связь. Типовые технические требования. Аппаратура малых земных станции спутниковой связи	Стандарт устанавливает требования к основным параметрам и техническим характеристикам ЗС, включая, требования по электромагнитной совместимости, по электрической и биологической безопасности, механической прочности и устойчивости к внешним воздействующим факторам. Стандарт устанавливает рекомендованные методы испытаний ЗС и измерений их основных параметров на соответствие установленным требованиям.
17.	СТО 34.01-9.3-003-2019 Технические требования к диспетчерским системам цифровой радиосвязи стандарта DMR	В данном стандарте описаны основные технические требования к оборудованию диспетчерских систем цифровой радиосвязи стандарта DMR, используемого в сетях подвижной радиосвязи (СПР) на различных уровнях управления в подразделениях ПАО «Россети», а также устанавливает основные требования эксплуатации этих систем.
18.	СТО 56947007-33.060.40.125-2012 Общие технические требования к устройствам обработки и присоединения каналов ВЧ связи по ВЛ 35-750 кВ	СТО устанавливает нормы и требования к устройствам обработки и присоединения к ВЛ 35-750 кВ, используемым для организации каналов ВЧ связи с передачей сигналов речи, данных, релейной защиты и противоаварийной автоматики, Требования даны для каждого из устройств обработки и присоединения (фильтр присоединения, ВЧ заградитель и конденсатор связи).
19.	СТО 56947007-33.060.40.134-2012 Типовые технические решения по системам ВЧ связи	Типовые технические решения по системам ВЧ связи предназначены для использования при составлении технических заданий на проектирование, при проектировании и разработке конкурсной документации на поставку оборудования обработки и присоединения и аппаратуры систем ВЧ связи. СТО содержит основные требования к ВЧ аппаратуре, оборудованию обработки и присоединения, измерительным приборам, электропитанию, а также краткие характеристики оборудования обработки и присоединения, аппаратуры различных производителей, используемых при проектировании ВЧ каналов связи, РЗ и ПА.

п/п	Документ	Содержание документа в части рекомендаций (требований) по реализации технических решений
20.	СТО 34.01-9.1-002-2018 Оборудование ВЧ связи для передачи сигналов по сетям низкого и среднего напряжения. Общие технические условия	В данном стандарте установлены общие требования к оборудованию ВЧ-связи для передачи сигналов/ команд по распределительной сети низкого (до 1 кВ) и среднего (6-20 кВ и 35 кВ) напряжения.
21.	СТО 56947007-33.060.40.045-2010 Руководящие указания по выбору частот высокочастотных каналов по линям электропередачи 35,110,220,330,500 и 750 кВ	Выбор рабочих частот новых ВЧ каналов по ЛЭП производится при разработке проектов ЛЭП и ПС, а также при разработке предложений по реконструкции каналов ВЧ связи и реконструкции и развития сети связи. Требования стандарта направлены на обеспечение электромагнитной совместимости новых и реконструируемых ВЧ каналов с существующими каналами, для их работы без взаимных влияний, а также регламентируют методы электрических расчетов ВЧ каналов, обосновывающих их работоспособность на конкретной ВЛ.
22.	СТО 56947007-33.060.40.052-2010 Методические указания по расчету параметров и выбору схем высокочастотных трактов по линиям электропередачи 35-750 кВ переменного тока	Приведенные в СТО сведения позволяют выбрать оптимальную схему присоединения к фазам и тросам ВЛ; произвести упрощенными методами расчет параметров ВЧ тракта с достаточно простой схемой и выбранным типом присоединения; для быстрого определения параметров ВЧ тракта; производить анализ влияния тех или иных причин на численные значения параметров ВЧ трактов.
23.	СТО 56947007-33.180.10.172-2014 Технологическая связь. Правила проектирования, строительства и эксплуатации ВОЛС на воздушных линиях электропередачи напряжением 35 кВ и выше	В данном стандарте описаны нормы и требования по проектированию, строительству, приёмке в эксплуатацию, непосредственно технической эксплуатации, проведению работ по ремонту и аварийному восстановлению линейно-кабельных сооружений ВОЛС на ВЛ, КВЛ, вдоль сооружаемых КЛ электропередачи и на территории энергообъектов, а также правила стандартизируют требования к ГИС и системе удалённого контроля и мониторинга оптических волокон ВОЛС.

п/п	Документ	Содержание документа в части рекомендаций (требований) по реализации технических решений
24.	Концепция «Цифровая трансформация 2030»	Концепция определяет основные направления технологических и организационных изменений работы ПАО «Россети» и ДЗО для изыскания новых механизмов, способов, алгоритмов корпоративного и технологического управления процессами компании и их последующей трансформации для повышения эффективности и качества оказываемых услуг, их доступности. В концепции определены перспективные цифровые технологии из стека Индустрия 4.0 и технологии связи с возможными эффектами от их (технологий) внедрения. В концепции задано направление развития сети связи с основными вехами на данном пути. В концепции также рассмотрены основные положения и принципы обеспечения информационной безопасности.
25.	Концепция развития системы оперативно-технологического управления и ситуационного управления в электросетевом комплексе ПАО «Россети», утвержденная распоряжением от 21.09.2018 № 412р	Данная концепция определяет основные принципы построения и обеспечения функционирования системы ОТУ и СУ в электросетевом комплексе; задает основные цели, функции и структуру системы ОТУ и СУ в электросетевом комплексе для всех уровней системы; описывает основы взаимодействия дочерних обществ ПАО «Россети» (их филиалов, уровней системы оперативно-технологического управления) между собой, с иными субъектами электроэнергетики, потребителями электрической энергии, а также с диспетчерскими центрами АО «СО ЕЭС» при организации и осуществлении функций ОТУ и СУ; указывает основные направления развития системы ОТУ и СУ в электросетевом комплексе.
26.	Положение ПАО «Россети» о единой технической политике в электросетевом комплексе, утвержденное решением Совета директоров ПАО «Россети» от 08.11.2019 № 378	Положение ПАО «Россети» о единой технической политике в электросетевом комплексе определяет совокупность обязательных и рекомендуемых для применения технических решений и технологий, а также направлений их развития, выработанных на основании утвержденных и проверенных принципов и критериев, позволяющих обеспечить плановое изменение электрических сетей, находящихся под управлением Общества и его ДЗО. Глава 17 данного Положения посвящена сетям связи (как первичным, так и вторичным/наложенным). Глава 13 посвящена центрам обработки данных. Глава 28 посвящена информационной безопасности электросетевого комплекса.
27.	Политика в области информационных технологий, автоматизации и телекоммуникаций, утвержденная решением Совета директоров от 11.09.2017 № 276	Политика ПАО «Россети» в области информационных технологий, автоматизации и телекоммуникаций устанавливает цели, задачи и принципы реализации мероприятий по автоматизации бизнес-процессов ПАО «Россети» и ДЗО, развитию и обеспечению систем автоматизации управления и обеспечивающей ИТ-инфраструктуры и систем связи. Глава 7 данного документа посвящена сетям связи. Глава 5 посвящена информационной безопасности.

п/п	Документ	Содержание документа в части рекомендаций (требований) по реализации технических решений
28.	Политика инновационного развития, энергосбережения и повышения энергетической эффективности ПАО «Россети» утвержденная решением Совета директоров от 23.04.2014 № 150	Политика инновационного развития, энергосбережения и повышения энергетической эффективности ПАО «Россети» определяет совокупность принципов и правил поведения (действий) по следующим направлениям деятельности Общества: инновационное развитие; энергосбережение и повышение энергетической эффективности; экология.
29.	Технические требования по организации каналов связи для оперативных переговоров и передаче телеметрической информации при выполнении ЦУС операционных функций в отношении объектов диспетчеризации	В документе определены требования к организации каналов связи для оперативных переговоров и передачи телеинформации, типовой состав телеинформации в отношении объектов ОТУ ЦУС, подлежащий передаче в ЦУС с энергообъектов, а также описаны случаи временных отступлений при организации телефонной связи для оперативных переговоров и передачи телеинформации в отношении объектов ОТУ ЦУС.
30.	Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ	Федеральный закон определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации (далее - безопасность, национальная безопасность), полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации (далее - Совет Безопасности).

п/п	Документ	Содержание документа в части рекомендаций (требований) по реализации технических решений
31.	Федеральный закон «О связи» от 07.07.2003 № 126-ФЗ	Федеральный закон регламентирует правовые аспекты деятельности операторов, провайдеров и других организаций и служб, работа которых связана с предоставлением связи. Распространяется действие закона на агентов, действующих на территории РФ, а также находящихся под юрисдикцией нашей страны. Закон прописывает полномочия государства в сфере контроля и надзора за деятельностью в сфере связи, а также права и обязанности участников и лиц, пользующихся услугами (клиентов). Целями Федерального закона являются: создание условий для оказания услуг связи на всей территории Российской Федерации; содействие внедрению перспективных технологий и стандартов; защита интересов пользователей услугами связи и осуществляющих деятельность в области связи хозяйствующих субъектов; обеспечение эффективной и добросовестной конкуренции на рынке услуг связи; создание условий для развития российской инфраструктуры связи, обеспечения ее интеграции с международными сетями связи; обеспечение централизованного управления российскими радиочастотным ресурсом, в том числе орбитально-частотным, и ресурсом нумерации; создание условий для обеспечения потребностей в связи для нужд органов государственной власти, нужд обороны страны, безопасности государства и обеспечения правопорядка.
32.	Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ	Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры (далее КИИ) Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак; создает основу правового регулирования; определяет принципы обеспечения безопасности КИИ; вводит понятие Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее ГосСОПКА); вводит основу для создания Национального координационного центра по компьютерным инцидентам (далее НКЦКИ); описывает полномочия Президента и органов госвласти в области обеспечения безопасности КИИ; содержит базу для определения категорий объектов КИИ; создает законодательную основу ведения реестра значимых объектов КИИ; определяет права и обязанности субъектов КИИ; определяет задачи и требования системы обеспечения безопасности значимого объекта КИИ; закладывает основу оценки безопасности КИИ; распределяет права и обязанности по государственному контролю.

14. Реализация концепции развития ССЭСК

Развитие ССЭСК предполагает два направления деятельности:

- Модернизация существующих сетей связи ДЗО в соответствии с требованиями настоящего стандарта. Целесообразность модернизации определяется на стадии формирования ТЭО.
- Строительство новых сетей связи ДЗО в соответствии с требованиями настоящего стандарта.

Общее регулирование ССЭСК осуществляется соответствующими подразделениями ДЗО и ИА ПАО «Россети».

14.1. Процесс оценки и надзора за реализацией Стандарта

14.1.1. Оценить успешность реализации стандарта возможно путем анализа степени внедрения положений настоящего стандарта. Данный анализ проводится каждые три года соответствующими структурные подразделения ДЗО и ДТП ПАО «Россети».

14.1.2. Надзор за реализацией стандарта осуществляется соответствующими подразделениями ДЗО и ИА ПАО «Россети» путем проверки проектной и рабочей документации на модернизацию/строительство сетей связи ДЗО на предмет соответствия требованиям настоящего стандарта.

14.2. Индикативные показатели успешной реализации Стандарта

14.2.1. В целях определения успешности реализации Стандарта рекомендуется рассчитать и установить уровни цифровизации ДЗО ПАО «Россети» с учетом степени применения цифровых технологий по следующим направлениям:

- Технологические информационные системы;
- Корпоративные информационные системы;
- Телекоммуникационная инфраструктура;
- Системы безопасности объектов инфраструктуры.

14.2.2. Для оценки критериев требуется разработка методики (порядока) расчета и определения веса критерия в общем индексе уровня цифровизации.

14.2.3. Задача по разработке методик (порядка) расчёта уровней цифровизации, веса критерия должна быть реализована ПАО «Россети» в рамках «Цифровой трансформации 2030» и не входит с состав данного стандарта.

Библиография

1. Федеральный закон от 26.03.2003 № 35-ФЗ «Об электроэнергетике».

2. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи».

3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

4. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

6. Приказ Минкомсвязи России от 30.01.2018 № 24 «Об утверждении Правил применения оборудования электропитания средств связи».

7. Приказ Минэнерго России от 13.02.2019 № 97 «Об утверждении Требований к каналам связи для функционирования релейной защиты и автоматики».

8. Концепция «Цифровая трансформация 2030», утвержденная Советом директоров ПАО «Россети» (протокол Совета директоров ПАО «Россети» от 21.12.2018 № 336).

9. Положение о единой технической политике в электросетевом комплексе (протокол Совета директоров ПАО «Россети» от 08.11.2019 № 378).

10. Политика ПАО «Россети» в области информационных технологий, автоматизации и телекоммуникаций (протокол Совета директоров ПАО «Россети» от 11.09.2017 № 276).

11. Концепция развития системы оперативно-технологического управления и ситуационного управления в электросетевом комплексе ПАО «Россети» (распоряжение ПАО «Россети» от 21.09.2018 № 412р).

12. Политика инновационного развития, энергосбережения и повышения энергетической эффективности ПАО «Россети» (протокол Совета директоров ПАО «Россети» от 23.04.2014 № 150).

13. Типовое соглашение о технологическом взаимодействии между ОАО «СО ЕЭС» и межрегиональной распределительной сетевой компанией (МРСК) или иной территориальной сетевой организацией в целях обеспечения надежности функционирования ЕЭС России.

14. Технические требования по организации каналов связи для оперативных переговоров и передаче телеметрической информации при выполнении ЦУС операционных функций в отношении объектов диспетчеризации.

15. СТО 34.01-21-004-2019 Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ.

16. СТО 34.01-21-005-2019 Цифровая электрическая сеть. Требования к проектированию цифровых распределительных электрических сетей 0,4-220 кВ.

17. СТО 34.01-24-002-2018 Организация технического обслуживания и ремонта объектов электроэнергетики.

18. СТО 34.01-3.1-003-2017 Построение распределительной сети напряжением 0,4-10 кВ с применением столбовых трансформаторных подстанций 6-10/0,4 кВ.

19. СТО 34.01-6.1-001-2016 Программно-технические комплексы подстанций 6-10 (20) кВ. Общие технические условия.

20. СТО 34.01-6.1-002-2016 Программно-технические комплексы подстанций 35-110 (150) кВ. Общие технические условия.

21. СТО 34.01-9.1-001-2018 Волоконно-оптические кабели связи. Общие технические требования.

22. СТО 34.01-9.1-002-2018 Оборудование ВЧ-связи для передачи сигналов по сетям низкого и среднего напряжения. Общие технические условия.

23. СТО 34.01-9.3-003-2019 Технические требования к диспетчерским системам цифровой радиосвязи стандарта DMR.

24. СТО 34.01-21.1-001-2017 Распределительные электрические сети напряжением 0,4-110 кВ. Требования к технологическому проектированию.

25. СТО 56947007-25.040.80.266-2019 Типовые технические требования к ССПИ ПС с функцией удаленного управления ПС из ЦУС.

26. СТО 56947007-29.130.01.092-2011 Выбор видов и объемов телеинформации при проектировании систем сбора и передачи информации подстанций ЕНЭС для целей диспетчерского и технологического управления.

27. СТО 56947007-29.240.10.167-2014 Информационно-технологическая инфраструктура подстанций. Типовые технические решения.

28. СТО 56947007-29.240.10.248-2017 Нормы технологического проектирования подстанций переменного тока с высшим напряжением 35-750 кВ (НТП ПС).

29. СТО 56947007-29.240.10.256-2018 Технические требования к аппаратно-программным средствам и электротехническому оборудованию ЦПС.

30. СТО 56947007-29.240.036-2009 Руководящие указания по выбору объемов неоперативной технологической информации, передаваемой с ПС ЕНЭС в центры управления электрическими сетями, а также между центрами управления.

31. СТО 56947007-33.060.20.233-2016 Технологическая связь. Руководящие указания по применению средств подвижной радиосвязи.

32. СТО 56947007-33.060.40.045-2010 Руководящие указания по выбору частот высокочастотных каналов связи по линиям электропередачи 35, 110, 220, 330, 500 и 750 кВ.

33. СТО 56947007-33.060.40.052-2010 Методические указания по расчету параметров и выбору схем высокочастотных трактов по линиям электропередачи 35-750 кВ переменного тока.

34. СТО 56947007-33.060.40.125-2012 Общие технические требования к устройствам обработки и присоединения каналов ВЧ связи по ВЛ 35-750 кВ.

35. СТО 56947007-33.060.40.134-2012 Типовые технические решения по системам ВЧ связи.

36. СТО 56947007-33.060.70.213-2016 Технологическая связь. Типовые технические требования. Аппаратура малых земных станций спутниковой связи.

37. СТО 56947007-33.180.10.172-2014 Технологическая связь. Правила проектирования, строительства и эксплуатации ВОЛС на воздушных линиях электропередачи напряжением 35 кВ и выше.

38. СТО 56947007-33.180.10.239-2016 Технологическая связь. Типовые технические требования. Аппаратура цифровых систем передачи информации по ВОК (SDH, PDH, WDM).

39. СТО 56947007-33.180.10.240-2016 Технологическая связь. Типовые технические требования. Оборудование сети передачи данных. Коммутаторы, маршрутизаторы, межсетевые экраны.

40. СТО 56947007-35.240.01.188-2014 Устройства сбора и передачи данных АИИС КУЭ. Типовые технические требования.

41. СТО 70238424.17.220.20.003-2011 Автоматизированные информационно-измерительные системы учета электроэнергии (АИИС УЭ), условия создания, нормы и требования.

42. СТО 70238424.17.220.20.004-2011 Автоматизированные информационно-измерительные системы учета электроэнергии (АИИС УЭ), организация эксплуатации и технического обслуживания, нормы и требования.

43. СТО 70238424.17.220.20.005-2011 Системы связи для сбора и передачи информации в электроэнергетике. Условия создания. Нормы и требования.

44. СТО 70238424.17.220.20.006-2011 Системы связи для сбора и передачи информации в электроэнергетике. Организация эксплуатации и технического обслуживания. Нормы и требования.

45. RFC 768 Стандарт Интернета. User Datagram Protocol.

46. RFC 791 Стандарт Интернета. Internet Protocol.

47. RFC 793 Стандарт Интернета. Transmission Control Protocol.

48. RFC 894 Стандарт Интернета. A Standard for the Transmission of IP Datagrams over Ethernet Networks.

49. RFC 919 Стандарт Интернета. Broadcasting Internet Datagrams.

50. RFC 1180 Стандарт Интернета. A TCP/IP Tutorial.

51. RFC 1701 Стандарт Интернета. Generic Routing Encapsulation.

52. RFC 1812 Стандарт Интернета. Requirements for IP Version 4 Routers.

53. RFC 1966 Стандарт Интернета. BGP Route Reflection: An alternative to full mesh IBGP.

54. RFC 1997 Стандарт Интернета. BGP Communities Attribute.

55. RFC 2283 Стандарт Интернета. Multiprotocol Extensions for BGP-4.

56. RFC 2328 Стандарт Интернета. OSPF Version 2.

57. RFC 2474 Стандарт Интернета. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers.

58. RFC 2475 Стандарт Интернета. An Architecture for Differentiated Services.

59. RFC 2796 Стандарт Интернета. BGP Route Reflection - An Alternative to Full Mesh IBGP.

60. RFC 3031 Стандарт Интернета. Multiprotocol Label Switching Architecture.

61. RFC 3032 Стандарт Интернета. MPLS Label Stack Encoding.

62. RFC 3630 Стандарт Интернета. Traffic Engineering (TE) Extensions to OSPF Version 2.

63. RFC 3916 Стандарт Интернета. Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3).

64. RFC 3985 Стандарт Интернета. Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture.

65. RFC 4090 Стандарт Интернета. Fast Reroute Extensions to RSVP-TE for LSP Tunnels.

66. RFC 4182 Стандарт Интернета. Removing a Restriction on the use of MPLS Explicit NULL.

67. RFC 4271 Стандарт Интернета. A Border Gateway Protocol 4 (BGP-4).

68. RFC 4447 Стандарт Интернета. Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP).

69. RFC 4594 Стандарт Интернета. Configuration Guidelines for DiffServ Service Classes.

70. RFC 4761 Стандарт Интернета. Virtual Private LAN Service (VPLS) Using BGP for Auto-discovery and Signaling.

71. RFC 4762 Стандарт Интернета. Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling.

72. RFC 5036 Стандарт Интернета. LDP Specification.

73. RFC 5462 Стандарт Интернета. «EXP» Field Renamed to «Traffic Class» Field.

74. RFC 6624 Стандарт Интернета. Layer 2 Virtual Private Networks Using BGP for Auto-Discovery and Signaling.

75. RFC 7308 Стандарт Интернета. Extended Administrative Groups in MPLS Traffic Engineering (MPLS-TE).

76. RFC 7432 Стандарт Интернета. BGP MPLS-Based Ethernet VPN.

Приложение А
к СТО 34.01-9-005-2020
Типовые сегменты, сервисы и микросегменты ССЭСК

№	Сегмент	Сервис	Микросегмент	Типовые механизмы сегментирования	
				Терм. узел связи	Маг. линия связи
1.	Технологический	Сервис связи для взаимодействия с АО «СО ЕЭС» (Энергообъект - ОДУ/РДУ, ЦУС - ОДУ/РДУ)	Телефонная связь для оперативных переговоров (Энергообъект - ОДУ/РДУ, ЦУС - ОДУ/РДУ)	Физическое; TS; VLAN; VRF	TS; VC; VLAN; VPWS; VRF-lite
2.			Телеинформация, включая телеуправление, сигналы событий и аварийно-предупредительные сигналы (ТИ, ТС, ТУ) (Энергообъект - ОДУ/РДУ, ЦУС - ОДУ/РДУ)	Физическое; TS; VLAN; VRF	TS; VC; VLAN; VPWS; VRF-lite
3.			Данные ЦС АРЧМ (Энергообъект - ОДУ/РДУ)	Физическое; TS; VC; VLAN; VRF	TS; VC; VLAN; VPWS; VRF-lite
4.			Данные СМПР по протоколу С37.118.2 (on-line) доаварийная телеметрическая информация ПА (Энергообъект - ОДУ/РДУ)	Физическое; TS; VC; VLAN; VRF	TS; VC; VLAN; VPWS; VRF-lite
5.			Данные СМПР (off-line), РАС и ОМП, а также для межмашинного обмена неоперативной информацией (Энергообъект - ОДУ/РДУ, ЦУС - ОДУ/РДУ)	Физическое; TS; VC; VLAN; VRF	TS; VC; VLAN; VPWS; VRF-lite
6.	Технологический	Сервис технологической связи (Энергообъект - ЦУС)	Телефонная связь для оперативных переговоров (Энергообъект - ЦУС)	Физическое; TS; VLAN; VRF	TS; VC; VLAN; VPWS; VRF-lite
7.			Производственно-технологическая телефонная связь (Энергообъект - ЦУС)	Физическое; TS; VLAN; VRF	TS; VC; VLAN; VPLS; VRF-lite
8.			Телеинформация, включая телеуправление, сигналы событий и аварийно-предупредительные сигналы (ТИ, ТС, ТУ) (Энергообъект - ЦУС)	Физическое; TS; VLAN; VRF	TS; VC; VLAN; VPWS; VRF-lite
9.			Неоперативная информация, включая передачу дополнительного объема информации о состоянии схемы соединений и параметров режима функционирования оборудования ПС, передачу данных, характеризующих состояние основного оборудования объектов, получаемых от подстанционных средств и подсистем мониторинга, подсистем контроля	Физическое; TS; VC; VLAN; VRF	TS; VC; VLAN; VPWS; VRF-lite

№	Сегмент	Сервис	Микросегмент	Типовые механизмы сегментирования	
				Терм. узел связи	Маг. линия связи
			качества электроэнергии, данных о состоянии инженерных систем подстанции, межмашинного обмена неоперативной информацией, подсистем РАС и ОМП (Энергообъект - ЦУС)		
10.	Технологический	Сервис связи Для ДФЗ	ДФЗ (прием/передача сигналов и команд РЗ) (Энергообъект - Энергообъект)	Физическое;	Физическое; WDM
11.	Технологический	Сервис связи Для ДЗЛ	ДЗЛ (прием/передача сигналов и команд РЗ) (Энергообъект - Энергообъект)	Физическое; TS	Физическое; TS; VC; VPWS; WDM
12.	Технологический	Сервис связи для ПА	ПА (прием/передача аварийных сигналов и команд сетевой, противоаварийной и режимной автоматики	Физическое; TS	Физическое; TS; VC; VPWS; WDM
13.			Данные мониторинга оборудования РЗА и АСУТП, для передачи осциллограмм	Физическое; TS; VLAN; VRF	TS; VC; VLAN; VPWS; VRF-lite
14.	Технологический	Сервис связи для АИИСКУЭ	Данные АИИСКУЭ, ККЭ (контроль качества электроэнергии)	Физическое; VLAN; VRF	VLAN; VPWS; VRF-lite
15.	Мультимедийный	Сервис унифицированных коммуникаций	Данные серверов/телефонных станций унифицированных коммуникаций, на которых развернуты такие подсистемы как: корпоративная телефонная связь; факсимильная связь; аудиоконференцсвязь; корпоративные мессенджеры; видеоконференцсвязь; видеотелефония и т. д.[14]	Физическое; TS; VC; VLAN; VRF	TS; VC; ODU; VLAN; L3VPN

[14] сервис унифицированных коммуникаций, как правило, организуется на одном сервере или стеке серверов, поэтому выделение для каждой из подсистем отдельного сегмента не требуется.

№	Сегмент	Сервис	Микросегмент	Типовые механизмы сегментирования	
				Терм. узел связи	Маг. линия связи
16.			Данные абонентов унифицированных коммуникаций	Физическое; TS; VC; VLAN; VRF	TS; VC; ODU; VLAN; L3VPN
17.	Мультимедийный	Сервис связи для видеонаблюдения	Данные систем охранного и технологического видеонаблюдения	Физическое; VLAN; VRF	ODU; VLAN; L3VPN
18.			Данные абонентов систем охранного и технологического видеонаблюдения	Физическое; VLAN; VRF	ODU; VLAN; L3VPN
19.	Корпоративный	Сервис связи для ОВБ	Данные системы «Цифровой электромонтер»	Физическое; VLAN; VRF	Физическое; VLAN; VPWS
20.	Корпоративный	Сервис связи для корпоративных информационных систем	Данные серверов, на которых развернуты такие информационные системы как: e-mail; «Портал»; ГИС; АСУД; СУПА; единая информационно-справочная система; распределенный реестр; активный каталог; «Телескоп»; корпоративный документационный оборот и т. д.	Физическое; VLAN; VRF	ODU; VLAN; L3VPN
21.			Данные пользователей, имеющих доступ к корпоративным информационным системам	Физическое; VLAN; VRF	ODU; VLAN; L3VPN
22.	Корпоративный	Сервис связи для особо защищаемых данных	Данные серверов хранящих и обрабатывающих данные защищаемые в соответствии с федеральным законом «О персональных данных» от 27.07.2006 N 152-ФЗ	Физическое; VLAN; VRF	ODU; VLAN; L3VPN
23.			Данные серверов хранящих и обрабатывающих данные относящиеся к коммерческой тайне	Физическое; VLAN; VRF	ODU; VLAN; L3VPN
24.			Данные пользователей, имеющих доступ к особо защищаемым данным	Физическое; VLAN; VRF	VLAN; L3VPN

№	Сегмент	Сервис	Микросегмент	Типовые механизмы сегментирования	
				Терм. узел связи	Маг. линия связи
25.	Корпоративный	Сервис связи для «Фабрики данных»	Данные для магистральной коммуникационной инфраструктуры РЦОД и «Фабрики данных»	Физическое; VLAN; VRF	ODU; VLAN; EVPN; L3VPN
26.	Корпоративный	Сервис доступа К ССОП	Доступ к сетям связи общего пользования и сети Интернет	Физическое; VLAN; VRF	Физическое; VLAN; L3VPN
27.			Данные серверов, обеспечивающих взаимодействие с ССОП и сетью Интернет	Физическое; VLAN; VRF	Физическое; VLAN; L3VPN
28.	Служебный	Сервис управления и мониторинга ССЭСК	Управления и мониторинга телекоммуникационным оборудованием	VLAN; VRF	VLAN; L3VPN
29.			Управления и мониторинга серверным оборудованием	VLAN; VRF	VLAN; L3VPN
30.			Управления и мониторинга вспомогательным оборудованием сети связи	VLAN; VRF	VLAN; L3VPN
31.			Данные серверов системы управления и мониторинга ССЭСК	VLAN; VRF	VLAN; L3VPN
32.			Управления информационной безопасностью	VLAN; VRF	VLAN; L3VPN
33.			Данные серверов системы информационной безопасности	VLAN; VRF	VLAN; L3VPN

Приложение Б
к СТО 34.01-9-005-2020
Требования к каналам связи

Микросегмент	Необходимость резервирования	Коэф. готовности системы из двух взаимно рез. каналов	Коэф. готовности канала	Максимальное время задержки	Вариации задержки по всему тракту	Макс. время задержки при переходе на рез. канал	Допустимый коэффициент потери пакетов
Телефонная связь для оперативных переговоров (Энергообъект - ОДУ/РДУ, ЦУС - ОДУ/РДУ)	+	не ниже 0,9996	не ниже 0,98	рек. не более 150 мс	рек. не более 50 мс	н.р.	рек. не более 1%
Телеинформация, включая телеуправление, сигналы событий и аварийно-предупредительные сигналы (ТИ, ТС, ТУ) (Энергообъект - ОДУ/РДУ, ЦУС - ОДУ/РДУ)	+	не ниже 0,9996	не ниже 0,98	рек. не более 1-2 с	н.р.	н.р.	рек. не более 1%
Данные ЦС АРЧМ (Энергообъект - ОДУ/РДУ)	+	не ниже 0,9996	не ниже 0,98	рек. не более 1с	н.р.	н.р.	рек. не более 1%
Данные СМПР по протоколу С37.118.2 (on-line) доаварийная телеметрическая информация ПА (Энергообъект - ОДУ/РДУ)	+	не ниже 0,9996	не ниже 0,98	рек. не более 150мс	н.р.	н.р.	рек. не более 1%
Данные СМПР (off-line), РАС и ОМП, а также для межмашинного обмена неоперативной информацией (Энергообъект - ОДУ/РДУ, ЦУС - ОДУ/РДУ)	рек.	н.р.	не ниже 0,98	рек. не более 1 с	н.р.	н.р.	рек. не более 1%
Телефонная связь для оперативных переговоров (Энергообъект - ЦУС)	+	не ниже 0,9996	не ниже 0,98	рек. не более 150 мс	рек. не более 50 мс	н.р.	рек. не более 1%

Микросегмент	Необходимость резервирования	Коэф. готовности системы из двух взаимно рез. каналов	Коэф. готовности канала	Максимальное время задержки	Вариации задержки по всему тракту	Макс. время задержки при переходе на рез. канал	Допустимый коэффициент потери пакетов
Производственно-технологическая телефонная связь (Энергообъект - ЦУС)	н.р.	н.р.	н.р.	рек. не более 150 мс	рек. не более 50 мс	н.р.	рек. не более 1%
Телеинформация, включая телеуправление, сигналы событий и аварийно-предупредительные сигналы (ТИ, ТС, ТУ) (Энергообъект - ЦУС)	+[15]	не ниже 0,9996	не ниже 0,98	рек. не более 1-2 с	н.р.	н.р.	рек. не более 1%
Неоперативная информация, включая передачу дополнительного объема информации о состоянии схемы соединений и параметров режима функционирования оборудования ПС, передачу данных, характеризующих состояние основного оборудования объектов, получаемых от подстанционных средств и подсистем мониторинга, подсистем контроля качества электроэнергии, данных о состоянии инженерных систем подстанции, межмашинного обмена неоперативной информацией, подсистем РАС и ОМП (Энергообъект - ЦУС)	рек.	не ниже 0,9996	н.р.	рек. не более 5 с	н.р.	н.р.	рек. не более 1%
ДФЗ (прием/передача сигналов и команд РЗ) (Энергообъект - Энергообъект)	-	-	не ниже 0,98	не более 15-28 мс	н.р.	н.р.	н.р.
ДЗЛ (прием/передача сигналов и команд РЗ) (Энергообъект - Энергообъект)	рек.	н.р.	не ниже 0,98	не более 5-10 мс	не более 300-400 мкс	н.р.	н.р.

[15] Производится дублирование каналов связи.

Микросегмент	Необходимость резервирования	Коэф. готовности системы из двух взаимно рез. каналов	Коэф. готовности канала	Максимальное время задержки	Вариации задержки по всему тракту	Макс. время задержки при переходе на рез. канал	Допустимый коэффициент потери пакетов
ПА (прием/передача аварийных сигналов и команд сетевой, противоаварийной и режимной автоматики	+[16]	не ниже 0,9999	не ниже 0,99	не более 1 с	н.р.	не более 50 мс	н.р.
Данные АИИСКУЭ, ККЭ (контроль качества электроэнергии)	рек.	н.р.	н.р.	н.р.	н.р.	н.р.	н.р.
Данные системы «Цифровой электромонтер»	рек.	н.р.	н.р.	н.р.	н.р.	н.р.	н.р.
Данные серверов/телефонных станций унифицированных коммуникаций	рек.	не ниже 0,9996	н.р.	не более 100мс	не более 100мс	н.р.	рек. не более 5%
Данные абонентов унифицированных коммуникаций							
Данные систем охранного и технологического видеонаблюдения	рек.	не ниже 0,9996	н.р.	не более 400мс	не более 100мс	н.р.	рек. не более 5%
Данные абонентов систем охранного и технологического видеонаблюдения							
Данные серверов различных корпоративных информационных систем	рек.	не ниже 0,9996	н.р.	не более 100мс	не более 50 мс	н.р.	рек. не более 1%
Данные пользователей, имеющих доступ к корпоративным информационным системам							
Данные серверов хранящих и обрабатывающих данные защищаемые в соответствии с федеральным законом "О персональных данных" от 27.07.2006 N 152-ФЗ	н.р.	н.р.	н.р.	н.р.	н.р.	н.р.	н.р.
Данные серверов хранящих и обрабатывающих данные относящиеся к коммерческой тайне							
Данные пользователей, имеющих доступ к особо защищаемым данным							

[16] Производится дублирование каналов связи.

Микросегмент	Необходимость резервирования	Коэф. готовности системы из двух взаимно рез. каналов	Коэф. готовности канала	Максимальное время задержки	Вариации задержки по всему тракту	Макс. время задержки при переходе на рез. канал	Допустимый коэффициент потери пакетов
Данные для магистральной коммуникационной инфраструктуры РЦОД и «Фабрики данных»	рек.	н.р.	н.р.	н.р.	н.р.	н.р.	н.р.
Доступ к сетям связи общего пользования и сети Интернет	н.р.	н.р.	н.р.	н.р.	н.р.	н.р.	н.р.
Данные серверов, обеспечивающих взаимодействие с ССОП и сетью Интернет							
Управления и мониторинга телекоммуникационным оборудованием	рек.	не ниже 0,996	н.р.	не более 100мс	не более 100мс	н.р.	рек. не более 1%
Управления и мониторинга серверным оборудованием							
Управления и мониторинга вспомогательным оборудованием сети связи							
Данные серверов системы управления и мониторинга ССЭСК							
Управления информационной безопасностью							
Данные серверов системы информационной безопасности							

Приложение В
к СТО 34.01-9-005-2020
Альбом типовых решений по построению усилительных трактов в ВОЛС

В.1. На момент написания стандарта, выпускаемые трансиверы ВОЛС обладают оптическим бюджетом позволяющем перекрывать расстояния порядка 100 - 120 км[17] без усиления сигнала.

В.2. Для покрытия расстояний порядка 150 км[18], как правило, используются схемы с предусилением. Данная схема позволяет перекрывать оптические потери порядка 35 - 38 дБ[19].

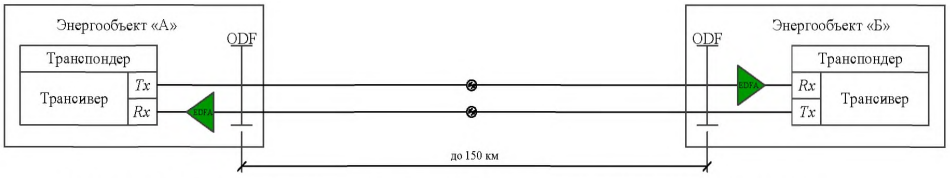


Рисунок 8. Типовая схема однопролетного тракта с предусилением.

В.3. Для покрытия расстояний порядка 200 км, как правило, используются схемы с бустером и предусилителем. Данная схема позволяет перекрывать оптические потери порядка 45 - 48 дБ.

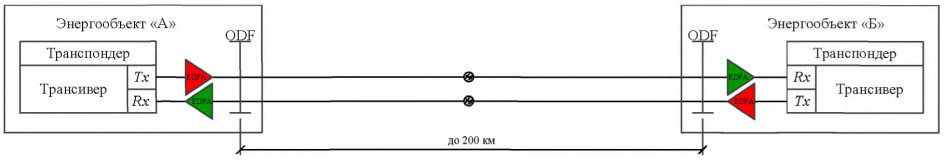


Рисунок 9. Типовая схема однопролетного тракта с бустером и предусилителем.

В.4. На длинах ВОЛС свыше 200 км начинают проявляться нелинейные искажения оптического сигнала, а также для покрытия столь больших расстояний требуется более значительное усиление в бустере, что приводит к снижению OSNR (за счет усиления шумов). Рекомендуемое решение данной проблемы - OTN + DWDM + бустер + предусилитель. Данная связка позволяет перекрывать оптические потери порядка 55 - 57 дБ и работает по следующему принципу:

---

[17] Расстояния, указанные в Приложении В, являются длинами по оптическому волокну, а не оптическому кабелю.

[18] Для высокоскоростных сигналов (10 - 100 Гбит/с) значительные ограничения по дальности передачи вносит накопленная хроматическая дисперсия, данная проблема решается применением модулей компенсации дисперсии либо использованием транспондеров со схемой электронной компенсации дисперсии, а также за счет применения волокна с ненулевой смещенной дисперсией (G.655). Предельно допустимые дисперсионные искажения зависят от многих факторов (тип волокна, скорость передачи, метода кодирования сигнала, гашений дисперсии за счет нелинейных искажений и т. д.), поэтому выбор способа компенсации дисперсии или их комбинация осуществляется на основании расчетов для каждого конкретного случая.

[19] Приведенные в Приложении В величины перекрываемых оптических потерь и длины ВОЛС даны оценочно, так как данные величины зависят от многих факторов (характеристик оборудования, тип волокна, скорость передачи, метода кодирования сигнала и т. д.), данные величины рассчитываются для каждого конкретного случая.

- Транспондер OTN упаковывает входящие информационные потоки в OTU с применением избыточного кодирования, что дает возможность применять механизмы упреждающей коррекции ошибок (FEC/SuperFEC/SoftFEC);
- В транспондере OTN несущая длина волны сигнала приводится в соответствие с частотным планом МСЭ-Т G.694.1 («окрашивается»). «Окрашенная» длина волны обладает стабильной несущей (незначительные флуктуации несущей длины волны), что позволяет применять DWDM мультиплексоры с шириной входного канала 25ГГц/50ГГц;
- DWDM мультиплексор используется как фильтр[20], отсекая шумы из остальной части спектра;
- Бустер[21] усиливает сигнал до уровня +15 - +23 дБм и передает в ВОЛС;
- На приемной стороне предусилитель усиливает сигнал до оптимального уровня;
- DWDM мультиплексор фильтрует сигнал;
- В транспондере OTN производится восстановление сигнала при помощи механизмов коррекции ошибок (к примеру, применение различных механизмов FEC для сигнала 10 Гбит/с позволяет понизить минимально допустимый OSNR (при BER=10^{-12}) с 21 дБ до 9 дБ).

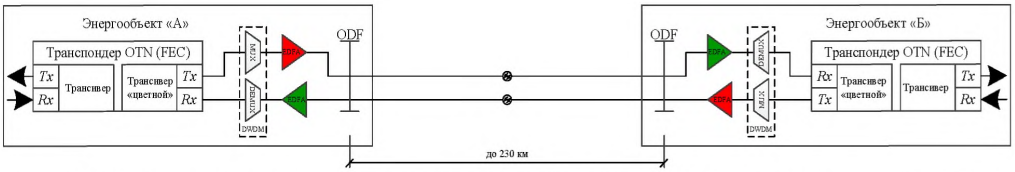


Рисунок 10. Типовая схема однопролетного тракта OTN + DWDM + бустер + предусилитель.

В.5. Для покрытия расстояний порядка 280 км, к схеме описанной в предыдущем пункте добавляется усилитель на основе ВКР эффекта (эффект Рамана)[22] со встречной накачкой, обеспечивающий распределенное усиление оптического сигнала в волокне. Данное решение позволит перекрыть оптические потери порядка 67 - 71 дБ.

[20] В случае, если не планируется наращивание пропускной способности за счет увеличения числа каналов связи, то возможно применение не полноценного DWDM мультиплексора, а тонкопленочного фильтра (TFF).

[21] В случае, если не планируется наращивание пропускной способности за счет увеличения числа каналов связи, рекомендуется применять бустеры и предусилители с узким спектром усиления (на 5-10 каналов).

[22] Поскольку в ВКР усилителях излучение накачки достигает уровней +33 дБм, для избегания несчастных случаев в ВОЛС должны быть применены разъемы типа E2000 с полировкой APC.

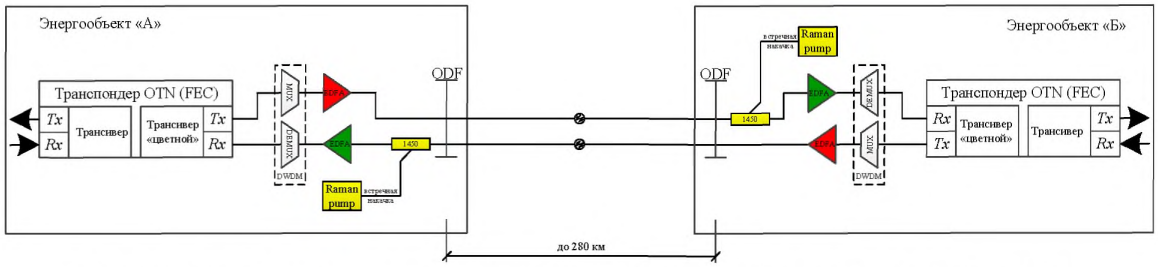


Рисунок 11. Типовая схема однопролетного тракта OTN + DWDM + бустер + предусилитель + ВКР усилитель.

В.6. Для покрытия расстояний порядка 380 км, поверх схемы описанной в предыдущем пункте должно быть организованно усиление по системе ROPA. Наиболее оптимальное место установки модулей усилителей ROPA на расстоянии 80 - 120 км от начала/конца ВОЛС. Количество волокон используемых для доставки излучения накачки может варьироваться от 0[23] до 4, в зависимости от типов накачки, используемых длин волн накачки, и характеристик самой системы. Данное решение позволит перекрыть оптические потери порядка 84 дБ.

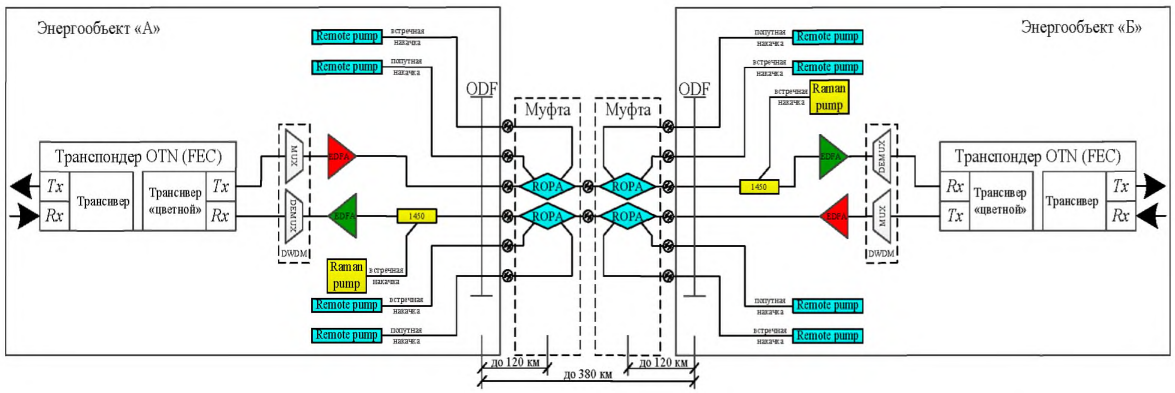
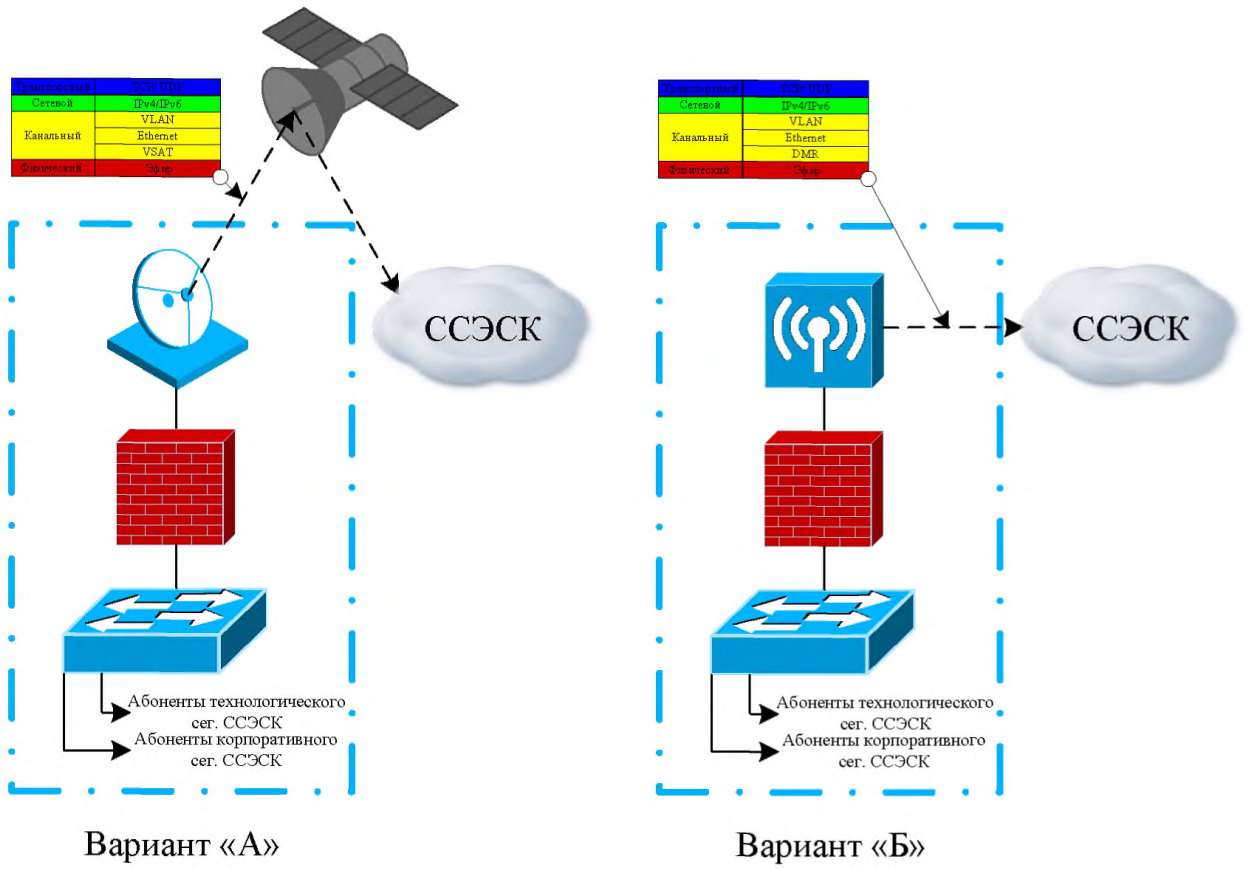


Рисунок 12. Типовая схема сверхдлинного однопролетного тракта с использованием системы ROPA.

В.7. Для покрытия расстояний больших, чем указанно в предыдущем пункте, линии связи строятся либо с использованием каскада усилителей, либо точек регенерации.

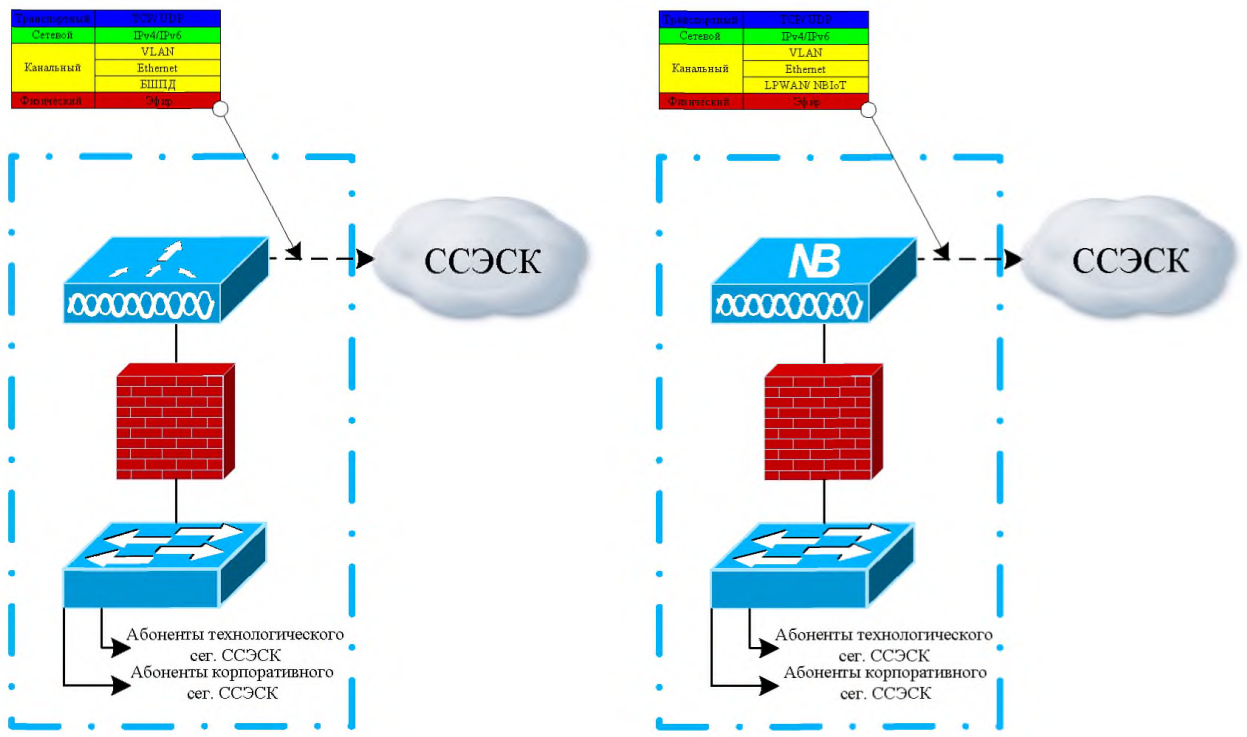
В.8. Параметр OSNR margin каналов связи, построенные с применением оптического усиления должен быть больше либо равен 2.

[23] В случае, если не используются дополнительные волокна (0 волокон), то излучение накачки усилителя доставляется при помощи WDM технологий по волокнам, в которых передается информационный сигнал.



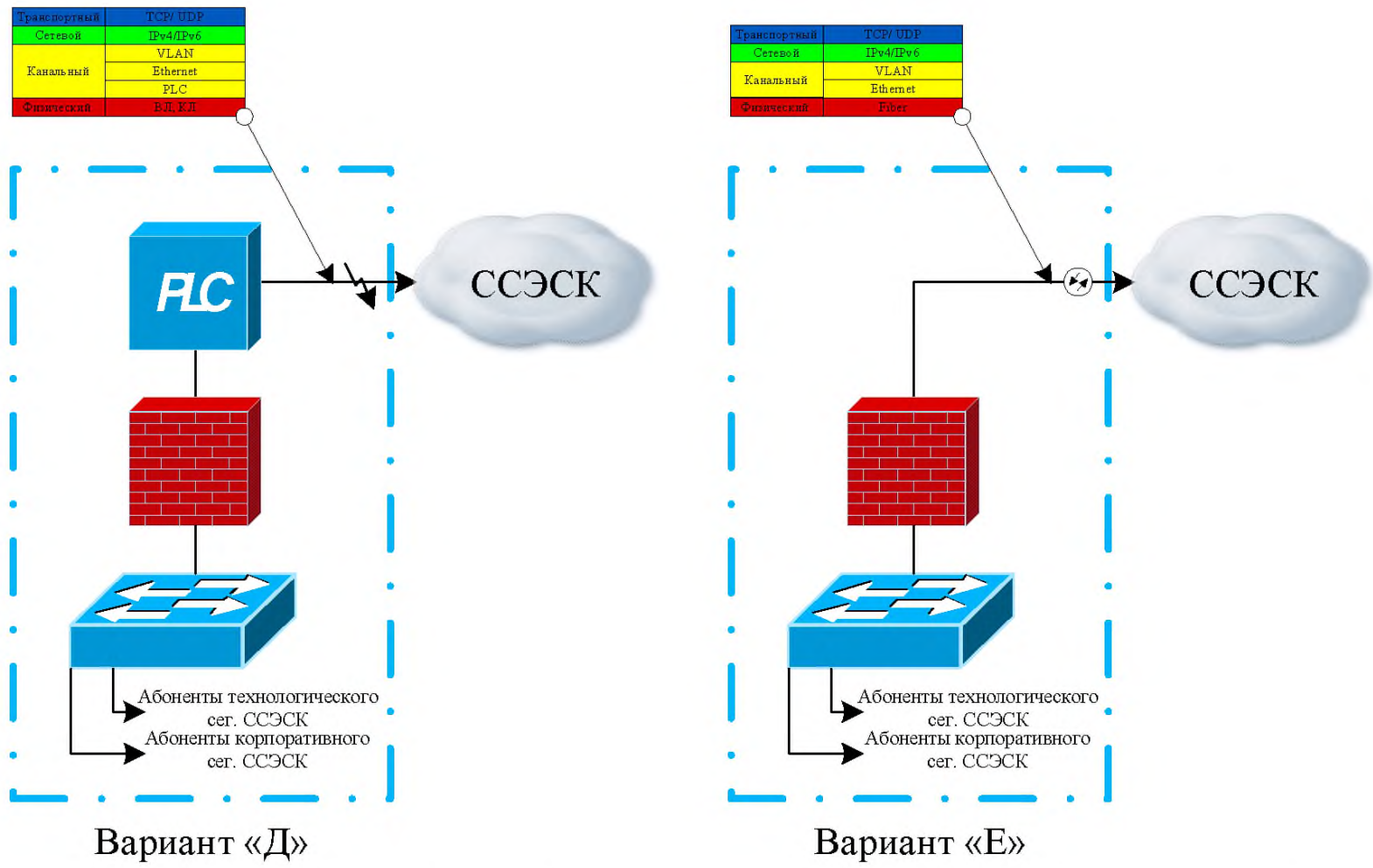
Вариант «А» Вариант «Б»

Рисунок 13.Типовой узел транспортной сети уровня А1. Вариант «А» с применением спутникового канала связи. Вариант «Б» с применением DMR канала связи.



Вариант «В» Вариант «Г»

Рисунок 14. Типовой узел транспортной сети уровня А1. Вариант «В» с применением БШПД канала связи. Вариант «Г» с применением узкополосного канала связи.



Вариант «Д» Вариант «Е»

Рисунок 15. Типовой узел транспортной сети уровня А1. Вариант «Д» с применением PLC канала связи. Вариант «Е» с применением ВОЛС.

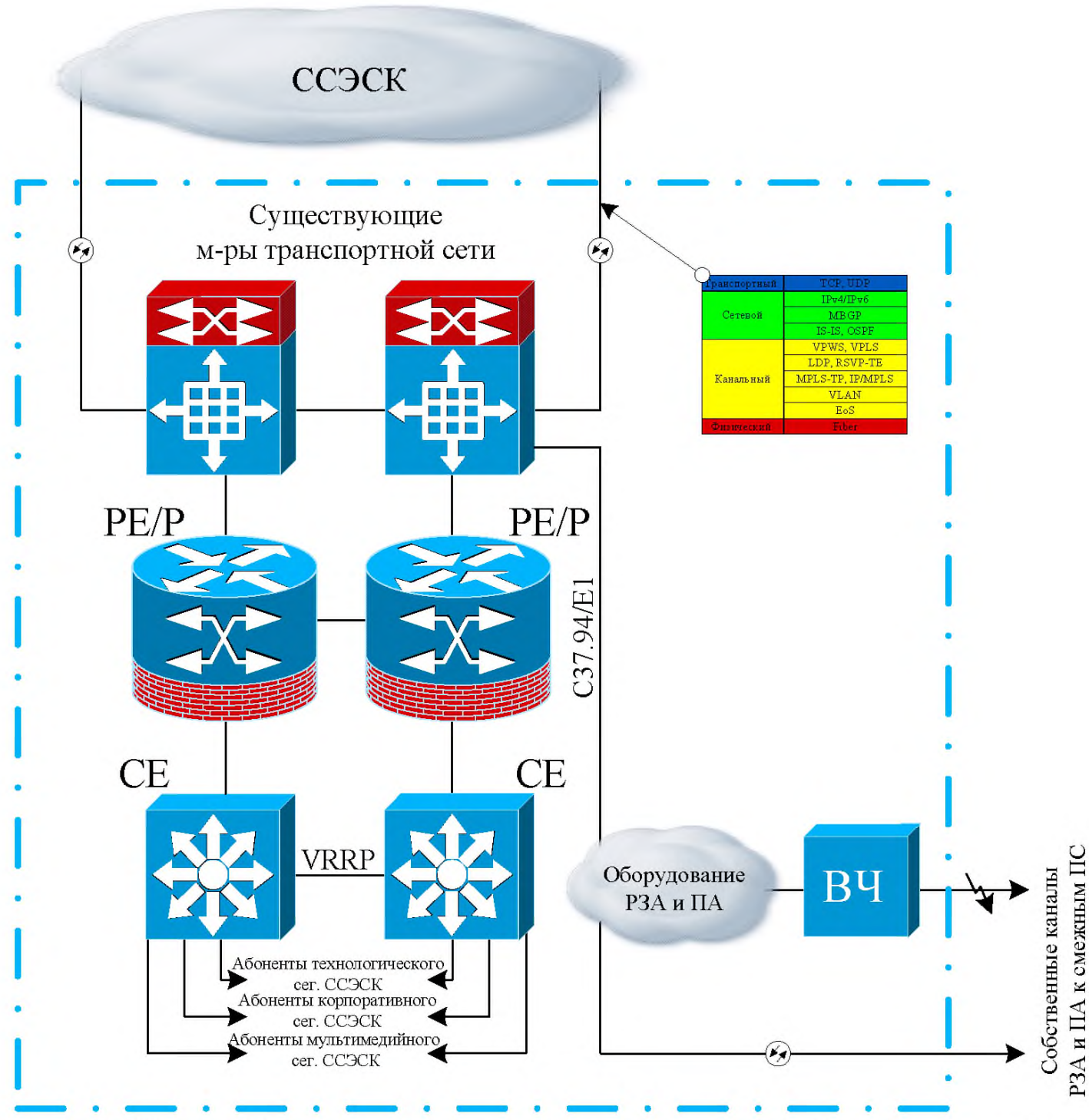


Рисунок 16. Типовой узел транспортной сети уровня А2. Вариант с использованием существующей транспортной сети.

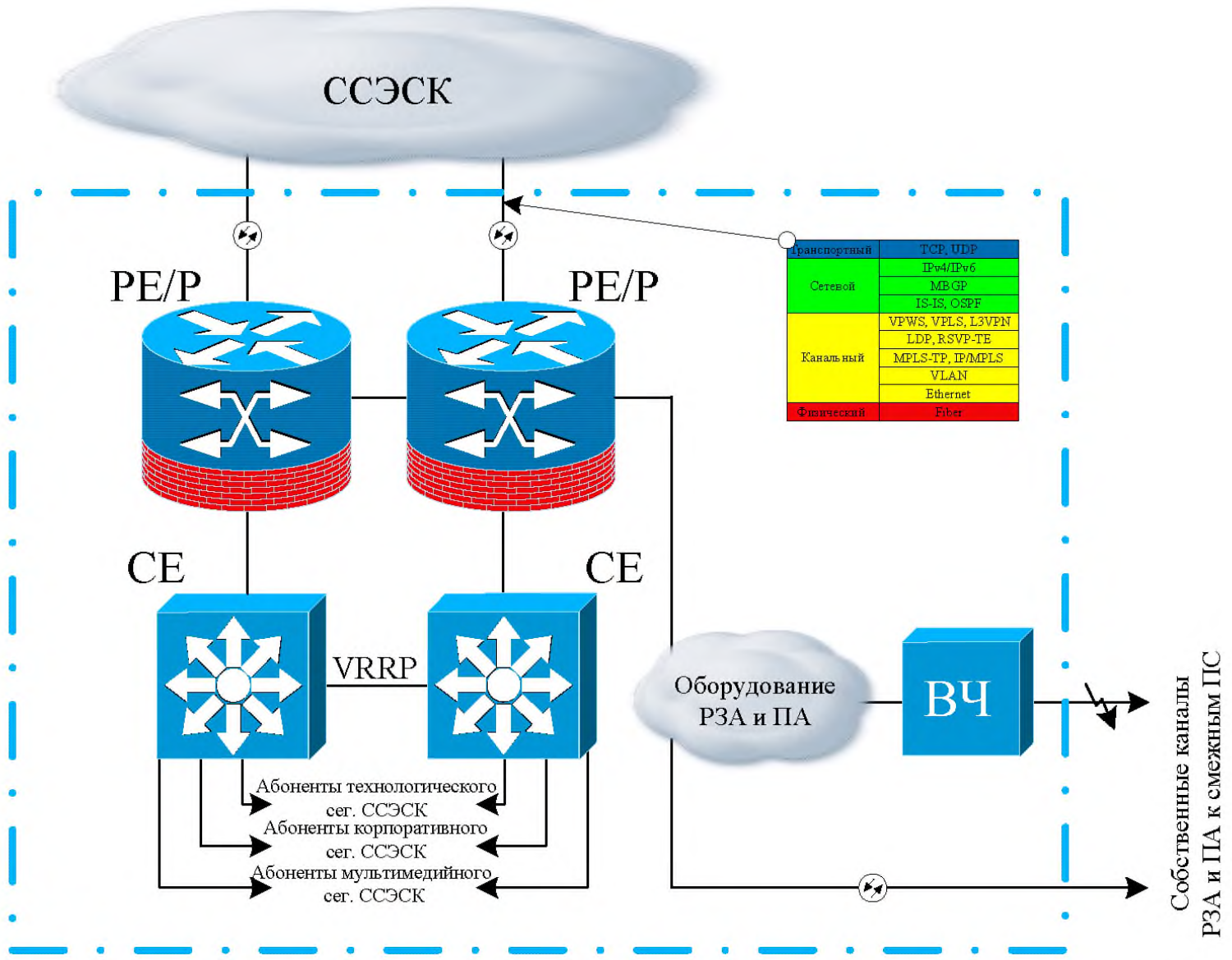


Рисунок 17. Типовой узел транспортной сети уровня А2. Вариант с использованием собственных и/или арендованных ВОЛС.

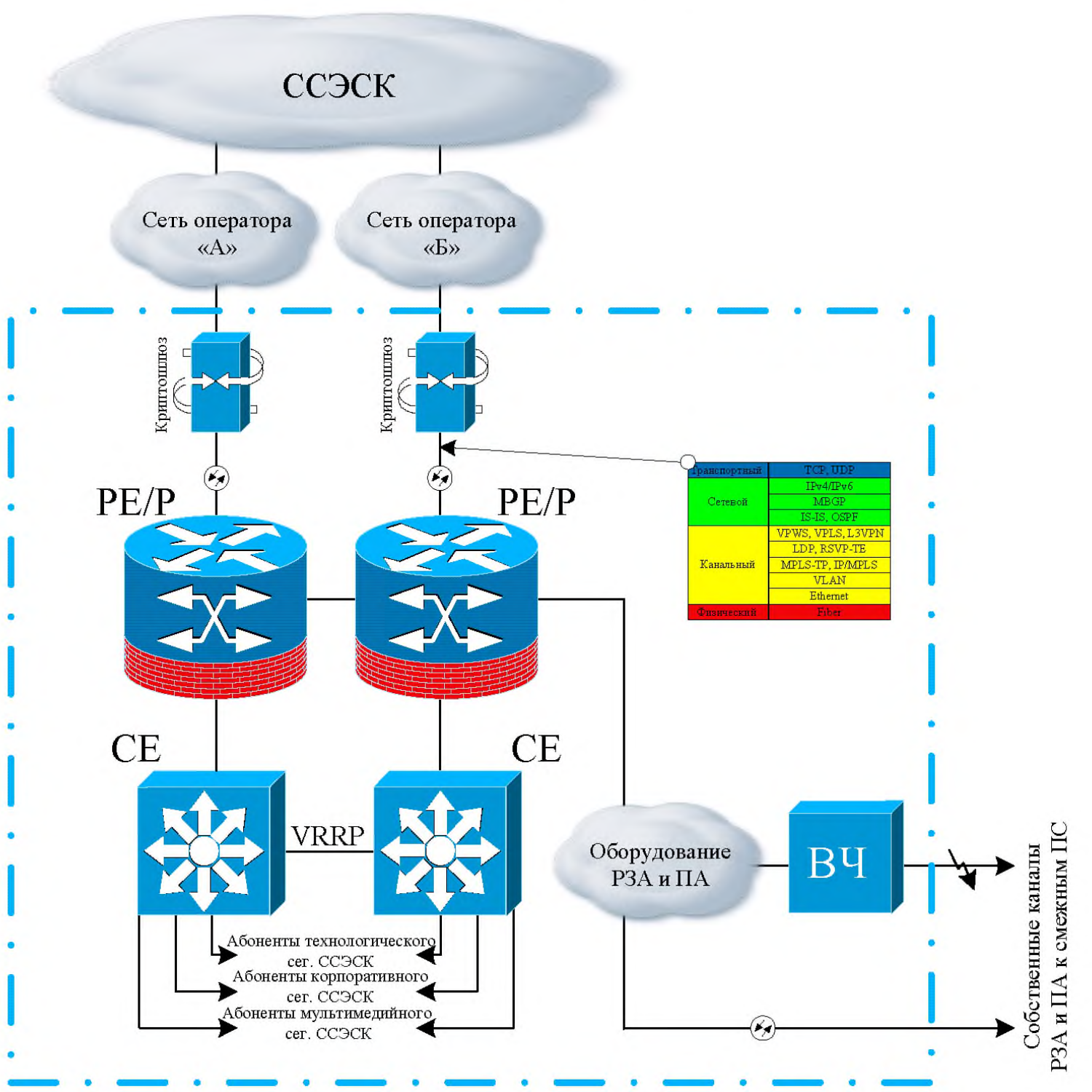


Рисунок 18. Типовой узел транспортной сети уровня А2. Вариант с использованием арендованных сервисов у операторов связи.

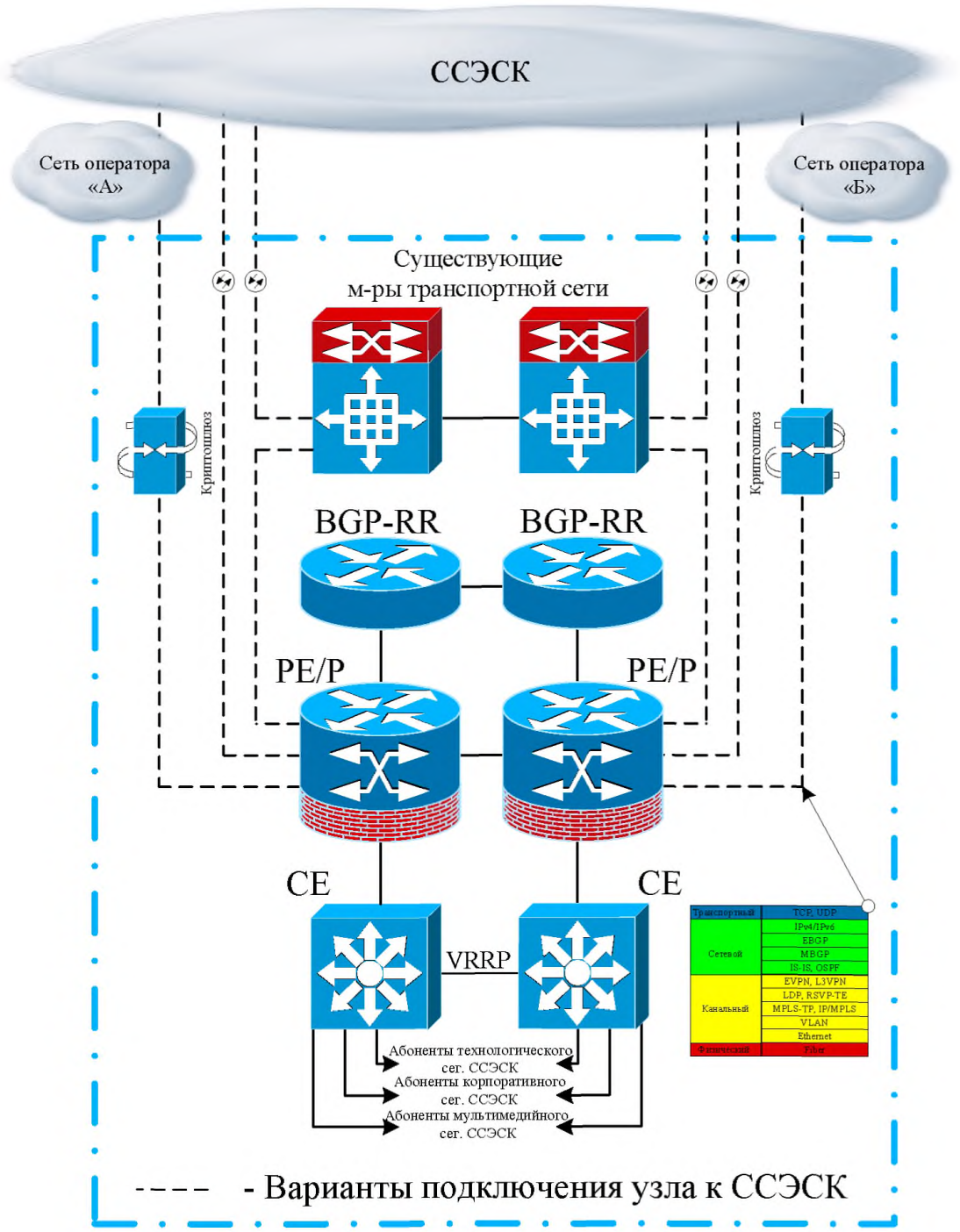


Рисунок 19. Типовой узел транспортной сети уровня А3.

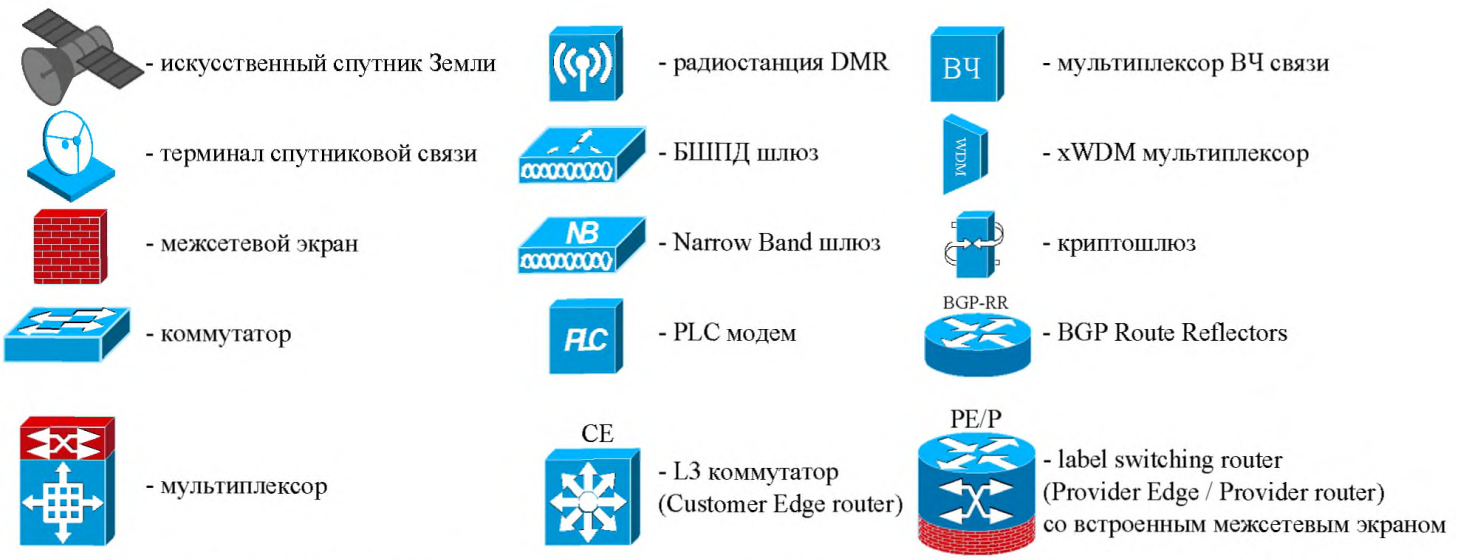


Рисунок 20. Условные обозначения, применяемые в Приложение Г.

Приложение Д
к СТО 34.01-9-005-2020
Типовая архитектура РУОТ

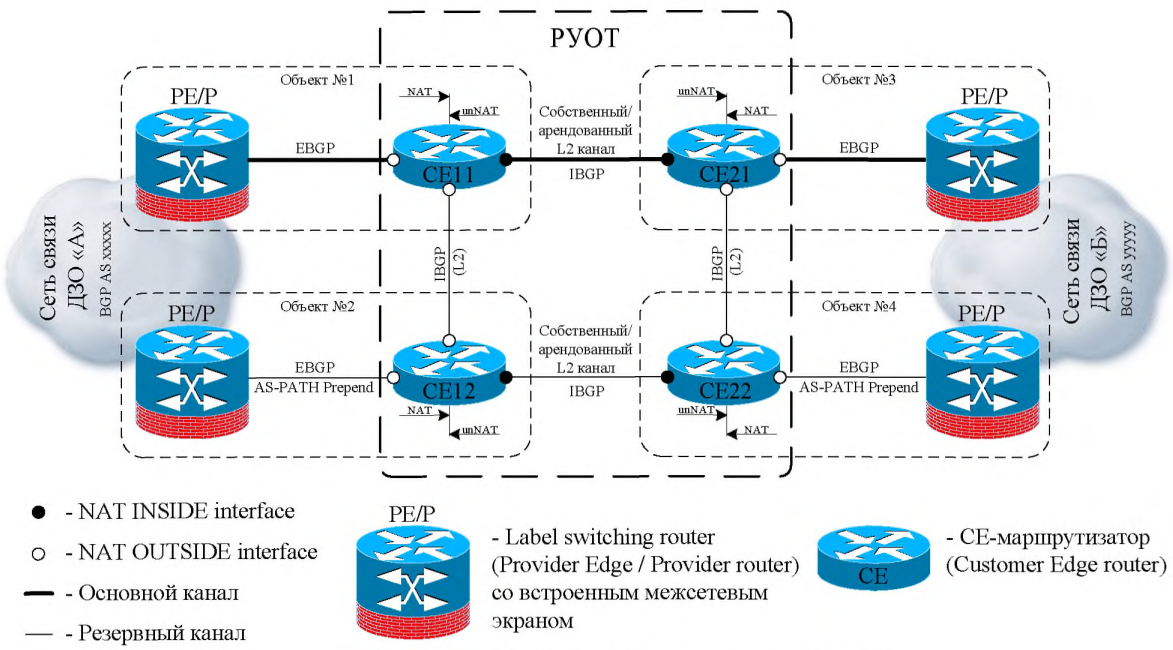


Рисунок 21. Типовая архитектура РУОТ.

Д.1. В целях обеспечения надежного взаимного обмена трафиком между ДЗО РУОТ должны резервироваться с использованием двух независимых, географически разнесенных каналов связи. Для прочих целей (включая транзит трафика) резервирование РУОТ и каналов применяется на основании соглашения между ДЗО.

Д.2. РУОТ состоит из выделенных CE-маршрутизаторов, связанных динамическими протоколами маршрутизации с каждой из сетей связи, в соответствии с техническими условиями ДЗО.

Д.3. Между CE-маршрутизаторами, непосредственно подключенными к сетям разных ДЗО (CE11 и CE21; CE12 и CE22), возможно использование как динамической, так и статической маршрутизации с элементами активного мониторинга состояния канала.

Д.4. Для реализации надежного резервирования передачи данных между объектами РУОТ должны быть организованы транспортные каналы уровня L2 (соединение на канальном уровне «классической» семиуровневой модели OSI), а для исключения петель маршрутизации между ними организовывается IBGP сессия.

Д.5. На CE-маршрутизаторах организовывается распределенная трансляция сетевых адресов с последовательным выполнением замены IP-адреса источника датаграммы (NAT) и IP-адреса назначения датаграммы (unNAT):

- В плане IP-адресации ДЗО выделяется, маршрутизируемый в рамках собственной сети, пул IP-адресов для непосредственно подключенных соседних ДЗО;
- ДЗО «А» использует выделенный для неё в ДЗО «Б» пул IP-адресов следующим образом: один IP-адрес используется для динамической трансляции собственных IP-адресов при обращении к ресурсам ДЗО «Б», а остальная часть выделенного пула используется для статической трансляции IP-адресов ДЗО «А», которые должны быть доступны из сети ДЗО «Б»;
- ДЗО «Б» использует аналогично выделенный для неё в ДЗО «А» пул IP-адресов: один IP-адрес используется для динамической трансляции собственных IP-адресов при обращении к ресурсам ДЗО «А», а остальная часть выделенного пула используется для

статической трансляции IP-адресов ДЗО «Б», которые должны быть доступны из сети ДЗО «А»;

- Трансляция IP-адресов (source) ДЗО «А» в IP-адреса из пула, выделенного ДЗО «Б» осуществляется на CE-маршрутизаторах непосредственно подключенных к сети ДЗО «А» (CE11 и CE12);
- Трансляция IP-адресов (destination) ДЗО «Б» из пула ДЗО «А» в реальные адреса ДЗО «Б» осуществляется на CE-маршрутизаторах непосредственно подключенных к сети ДЗО «Б» (CE21 и CE22);
- Трансляция IP-адресов (source) ДЗО «Б» в IP-адреса из пула, выделенного ДЗО «А» осуществляется на CE-маршрутизаторах непосредственно подключенных к сети ДЗО «Б» (CE21 и CE22);
- Трансляция IP-адресов (destination) ДЗО «А» из пула ДЗО «Б» в реальные адреса ДЗО «А» осуществляется на CE-маршрутизаторах непосредственно подключенных к сети ДЗО «А» (CE11 и CE12);

Д.6. По мере перехода к единому плану IP-адресации ССЭСК от трансляции IP-адресации на стыках между сетями связи ДЗО можно будет отказаться.

gost.e-ecolog.ru