БЕЗОПАСНОСТЬ ТЕХНОЛОГИЧЕСКОГО СЕГМЕНТА СЕТИ СВЯЗИ ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА

ТЕХНОЛОГИИ СВЯЗИ, СНИЖАЮЩИЕ РИСК ПОТЕРИ УПРАВЛЕНИЯ СОВРЕМЕННЫМИ ИНТЕЛЛЕКТУАЛЬНЫМИ ЭЛЕКТРИЧЕСКИМИ СЕТЯМИ НА ПРИМЕРЕ СЕТИ СВЯЗИ ОБЪЕКТОВ СРЕДНЕГО НАПРЯЖЕНИЯ И ТРАНСПОРТНОЙ СЕТИ СВЯЗИ ЭЛЕКТРОСЕТЕВЫХ КОМПАНИЙ

А.М. ЛИФШИЦ (ООО “НПЦ Приоритет”)

научно-производственный центр "Приоритет"

Развитие интеллектуальных технологий и цифровизация электросети предполагают переход на пакетные технологии и использование телекоммуникационных ресурсов различных операторов связи, тем самым значительно увеличивая периметр информационной безопасности. Кроме того, значительно выросла проблема безопасности функционирования самих телекоммуникационных сетей. В статье рассматриваются варианты создания защищенных сетей связи для энергообъектов среднего напряжения. Также рассмотрены наиболее важные проблемы безопасности при переходе на пакетные технологии транспортной сети связи электросетевого комплекса (ССЭСК). Предложены методы тестирования способности сети обеспечить стабильность параметров каналов связи существующего и перспективного оборудования РЗА.

Ключевые слова: *интеллектуальные технологии; цифровизация электросети; пакетные технологии; телекоммуникационные ресурсы; телекоммуникационные сети; сети связи электросетевого комплекса; SCADA; АСКУЭ; технология NBPLC.*

Инновационное развитие электроэнергетики потребовало преобразования информационной и телекоммуникационной инфраструктуры. Основой электросети станут цифровые подстанции, которые являются базовым элементом интеллектуальной электросети с системами управления и защиты, в основе которых лежит цифровая форма передачи информации. ПАО Россети планирует к 2030 году ввести в действие 1200 цифровых подстанций.

В тоже время интеллектуальные сети не заканчиваются на цифровых подстанциях, так как электрическая сеть нового поколения объединит информационные потоки от всех подключенных конечных пользователей, включая объекты распределенной генерации.

Кибербезопасность стала одной из главных проблем при внедрении интеллектуальных сетей, так как новая телекоммуникационная инфраструктура, обеспечивающая связь между конечными пользователями, значительно расширяет зону атаки на энергосистему.

Традиционно все энергетические компании имели свои собственные сети связи, предназначенные для технологического и административно-хозяйственного управления их деятельностью. Все технологические системы были изолированы от сети связи сторонних организаций или были к ним подключены лишь в отдельных узлах. Поэтому ответственность энергокомпаний за безопасность ограничивалась контролем своих систем, это касалось, главным образом, охраной объекта и оборудования, систем электропитания, климатики и т.д. Воздействие внешних корпоративных сетей и сетей общего пользования, а тем более Интернета, было невозможно. Системы мониторинга и управления телекоммуникационной сетью были ограничены конкретным оборудованием, и воздействовать на них извне было невозможно.

Понятно, что защититься от потенциальных угроз полностью не удастся, во всяком случае, в интеллектуальной сети. Однако, можно облегчить задачу ограничив периметр защищаемой сети и применяя сетевые технологии, параметры которых легче контролировать.

1. БЕЗОПАСНАЯ СЕТЬ СВЯЗИ ДЛЯ ЭНЕРГООБЪЕКТОВ СРЕДНЕГО НАПРЯЖЕНИЯ

Создание интеллектуальных сетей, цифровых РЭС и т.д. невозможно без обеспечения каналами связи этого сегмента электросети для передачи информации приложений SCADA и АСКУЭ. Объектов среднего напряжения в России насчитывается порядка одного миллиона. С точки зрения скорости развертывания сети связи и затрат, естественно желание электросетевых компаний использовать для управления и контроля этими объектами услуги операторов подвижной радиосвязи. Зона действия одного оператора связи, который предоставляет в аренду свои телекоммуникационные ресурсы, может охватывать регион, в котором находятся сотни и тысячи подстанций. Таким образом, возникает огромный периметр безопасности, защита которого остается на совести сторонней организации, а единственное средство собственной защиты это дополнительное оборудование криптографии. Возникшая возможность несанкционированного доступа к оборудованию этих подстанций через сеть оператора связи или выход из строя сегмента сети связи может привести к полной блокировке электроснабжения целых регионов. Ниже предложено одно из решений этой проблемы, которое предполагает создание комбинированной сети, использующей собственные каналы ВЧ связи, созданные на базе технологии NBPLC для энергообъектов, имеющих силовые автоматические выключатели и выключатели-разъединители. Подстанции, не имеющие автоматических выключателей (без телеуправления) или не являющиеся узловыми, могут передавать информацию через сети сторонних операторов связи без большого риска.

Использование технологии ВЧ связи по линиям среднего напряжения (NBPLC) кардинально решает проблему безопасности, так как есть отечественное оборудование, соответствующее СТО 34.01-9.1-002-2018 [1], с собственным физическим и сетевым уровнем, в котором не используется IP адресация и оригинальными методами помехоустойчивого кодирования [2]. Благодаря этому, а также распределенной архитектуре сети связи, в случае несанкционированного воздействия, исключается массовый вывод из строя электросетевых объектов.

Для примера, ниже приведена схема фрагмента сети 6 кв, в которой порядка 30-ти ТП и несколько КРН или реклоузеров, имеющих возможность управлять выключателями. Для выполнения задач телеуправления в этой схеме достаточно установить 3-4 NBPLC модема, а для телесигнализации и АСКУЭ более 30-ти. Информацию телесигнализации можно передавать, используя услуги операторов мобильной связи, а сигналы телеуправления – по собственной сети, применяя технологию NBPLC. Надо отметить, что возможности отечественного оборудования NBPLC позволяют создавать сети связи с любой топологией, быстро увеличить количество объектов управления в случае реконструкции электросети и добавления точек размыкания, используя уже установленные модемы в качестве ретрансляторов для вновь установленных. При массовом применении отечественных модемов NBPLC для собственной сети связи, время на развертывание сети и затраты будут соизмеримы с аналогичными показателями при использовании арендованных каналов связи операторов мобильной связи. При выполнении требований по защите информации и установке оборудования криптозащиты, затраты будут превосходить стоимость создания собственной сети связи на технологии NBPLC.

На представленных ниже рисунках показан фрагмент сети среднего напряжения в сельской местности. На рис. 1 изображена сеть связи с комбинацией проводной (NBPLC) и радио технологии. На рис. 2 все объекты используют только проводную технологию. В том и другом варианте криптозащита не требуется, так как управление энергообъектами осуществляется по собственным каналам ВЧ связи.

Комбинация проводной NBPLC и радиотехнологии позволяет не только снизить первоначальные расходы, обеспечив надежное управление сетью, но и получить при необходимости 100% резервирования каналов связи, а также обеспечить связь вне зоны покрытия сетей радиосвязи.

Как было отмечено ранее, такая конфигурация сети передачи данных для объектов с телеуправлением значительно уменьшает периметр безопасности и возможность перехвата управления электросетевым оборудованием.

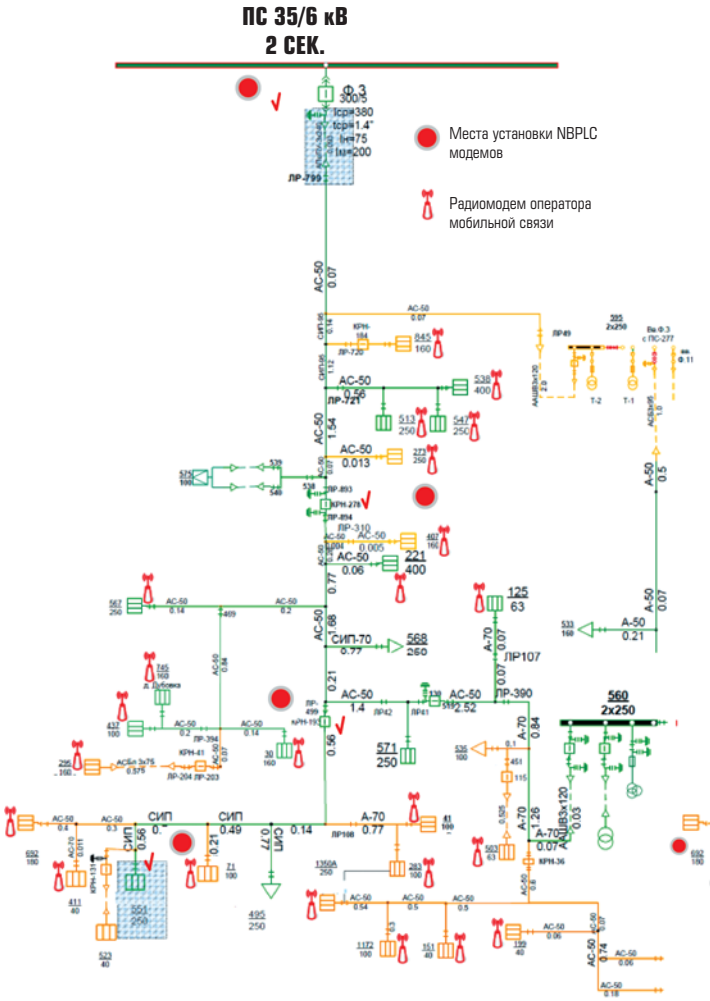

Рис. 1. Сеть связи с комбинацией ВЧ связи и арендованных каналов связи оператора мобильной связи

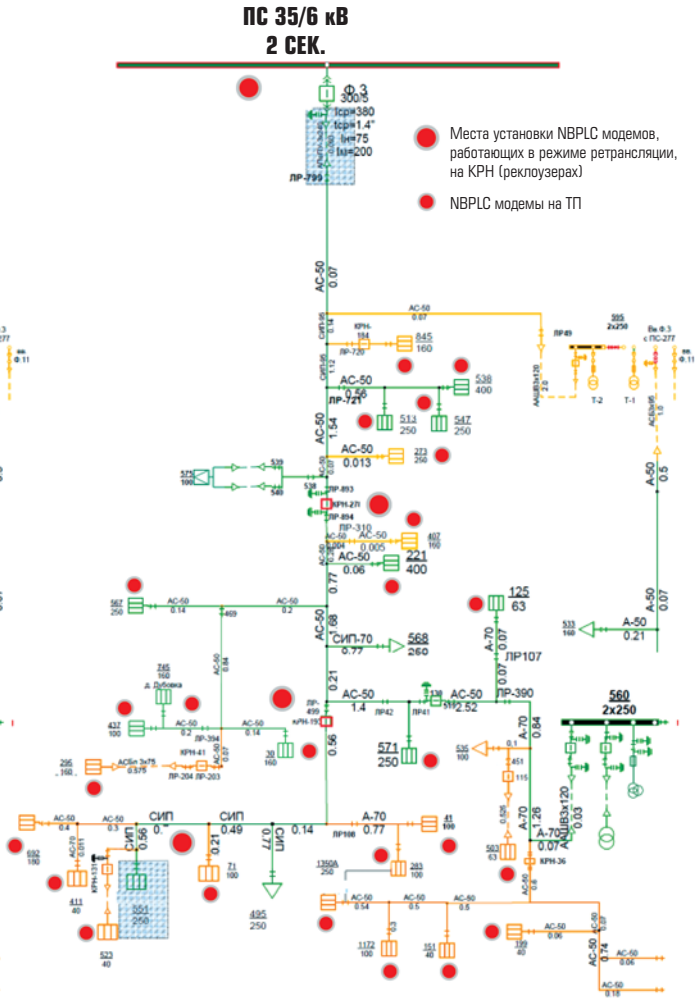

Рис. 2. Сеть собственной ВЧ связи (NBPLC)

2. ТРАНСПОРТНЫЕ СЕТИ СВЯЗИ ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА

Обеспечение безопасности этого сегмента корпоративной сети связи представляет чрезвычайно сложную задачу. Предполагается, что транспортная сеть и сеть агрегации являются собственностью электросетевой компании. В качестве базовой технологии используют кольцевые структуры SDH, а перспективной базовой технологией магистральной сети выбрана MPLS. Дополнительные проблемы возникают в условиях постепенного перехода на пакетные технологии с сохранением существующего оборудования, использующего временное мультиплексирование каналов связи (PDH и SDH). Технология такого гибридного варианта хорошо освоена, но сделала сеть связи значительно более уязвимой в случае несанкционированного воздействия на систему управления.

Базовая технология для транспортных сетей связи, сетей агрегации и сетей доступа – MPLS, позволяет интегрировать в новую сеть TDM каналы связи, которые обеспечивают взаимодействие существующего оборудования РЗА, используя протоколы туннелирования и приоритезации трафика. В большом количестве публикаций, посвященных MPLS, подробно описаны способы настройки параметров сети для обеспечения требуемых характеристик для передачи сигналов критически важного трафика [3, 4, 5]. Протоколы маршрутизации и оптимизации загрузки сетевых узлов, такие как OSPF, IS-IS и другие, позволяют поддерживать параметры каналов связи в заданных пределах. Для более простого и более надежного обеспечения заданных параметров сети была разработана технология MPLS-TP, в которой маршруты пакетов основного и резервного канала связи определены заранее. Решению о применении той или иной пакетной технологии для

транспортных технологических сетей должно предшествовать тестирование параметров сети в условиях реальной нагрузки и возможности реализации мер по защите самой сети от внешнего воздействия.

Проведенные испытания производителями оборудования и независимыми лабораториями показали возможность получить необходимые параметры, соответствующие требованиям энергетических приложений. В тоже время, целесообразно расширить тестовые задачи для полного понимания последствий воздействия на систему управления сетью изменения ряда ее параметров.

Расширенная программа тестирования, ориентированная на использование технологии MPLS в качестве базовой для корпоративных сетей связи, представлена ниже. Сравнению сетевых технологий посвящено много публикаций, поэтому ниже приведены только выводы и доводы.

Классификация протоколов MPLS. IP MPLS и MPLS–TP

Стандарт MPLS-TP является упрощенной версией изначально разработанного протокола MPLS. MPLS-TP разрабатывается совместными усилиями ITU-T и IETF. В MPLS-TP используются те же принципы построения архитектуры сети, что и в технологиях SDH или OTN. Отказ от некоторых технологий на сетевом уровне, позволяет существенно повысить надежность функционирования протоколов OAM, используемых для мониторинга и защитного переключения.

Основные различия между технологиями MPLS-TP и MPLS/IP представлены в таблице 1.

Таблица 1. Основные различия между технологиями MPLS-TP и MPLS/IP

MPLS-TP	IP MPLS
Симметричность пути (LSP). Пакеты из пункта А в пункт Б всегда идут по одному пути	Традиционно в IP сетях пакеты могут идти разными путями
Поддержка протокола IP не обязательна	Обязательная поддержка протокола IP
Расширенная поддержка кольцевой топологии	
Вынесение control plane в систему управления сетью (NMS)	control plane на каждом узле сети
Изоляция интерфейсов управления в отдельную сеть	Управление осуществляется по сети
Статическое назначение пути, без использования вспомогательных протоколов	Как правило, для построения путей используются протоколы LDP, RSVP

Отсутствие поддержки этих функций в MPLS-TP не является недостатком, а убирая из технологии динамичность, добавляет ей предсказуемость и надежность, что очень важно для РЗА!

Наименование разделов тестирования

1. Проверка возможности интеграции с сетью MPLS TP существующих мультиплексоров, используемых в качестве узлов агрегации различного технологического трафика, с помощью встроенного шлюза MPLS TP – вариант “гибридной сети. Рабочий и аварийный режим.
2. Тестирование сети MPLS TP при подключении технологического оборудования, использующего для взаимодействия TDM каналы связи, в порт SDH и PDH коммутаторов MPLS TP. Рабочий и аварийный режим.
3. Тестирование сети MPLS TP при DoS атаке.

Перечень функций, подлежащих испытаниям

1. Задержка (график нагрузка/задержка).
2. Асимметрия задержки канала (график нагрузка/а.задержки).
3. Измерение джиттера (график нагрузка/джиттер).
4. Целостность данных (график нагрузка/целостность).

   Тестирование проводится для следующих условий:
   - нормальные условия;
   - одиночный обрыв одного из соединений;
   - множественные обрывы в сети (связность сети не нарушена полностью);
   - перегруженность сети для пакетов низких приоритетов;
   - асимметрия задержки самого сервиса РЗА;
   - DoS атака направленная на Management Plane;
   - DoS атака направленная на Control Plane;
   - DoS атака направленная на Data Plane.
5. Реализация QoS в зависимости от производителя:
   - размер, количество аппаратных очередей;
   - количество программных очередей;
   - алгоритмы обработки очередей.

6. Проверка реализации дублирования пакетов и защитного переключения до 50 мс LSP 1+1 в соответствии с RFC6378.
7. Проверка реализации защитного переключения до 50 мс LSP 1:1 в соответствии с RFC6378.
8. Проверка на соответствие стандарту МЭК 60834-1 и параметрам производительности:
   - время передачи (меньше 10 мс);
   - надежность (оценивается вероятность пропустить команду – $< 10E^{-4}$ при BER = $10E^{-6}$);
   - безопасность (оценивается также через вероятность).
9. Проверка функциональных возможностей системы управления и мониторинга NMS:
   а. Соответствие FCAPS management functions (i.e., fault, configuration, accounting, performance, and security management):
      - сбор аварий;
      - настройка и управление;
      - мониторинг производительности;
      - контроль доступа;
      - инструменты поиска и устранения неисправностей;
      - отображение текущего состояния топологии сети.
   б. Проверка функционала NMS в части MPLS-TP OAM:
      - проверка целостности (Continuity Check);
      - проверка связности (Connectivity Verification);
      - проверка пути (traceroute);
      - индикаторы отказа (alarm reporting, отказ клиента, удаленный отказ);
      - мониторинг производительности (задержка, потери пакетов);
      - LSP ping.

Синхронизация

Требования по синхронизации к оборудованию:

- Длительное удержание точности синхронизации. При потере внешнего синхросигнала от источника оборудование должно сохранять точность без “уплывания” частоты и фазы с заданной точностью до восстановления внешнего источника синхронизации (для состояний free run).
- Поддержка протокола синхронизации IEEE 1588 2008 Precision Time Protocol (PTP) (Уровень поддержки зависит от местоположения и роли оборудования в сети – Grand Master, boundary, transparent).
- Поддержка получения синхросигнала от внешнего оборудования (источника), такого как Глонасс, GPS и пр., а также переключение на данный источник автоматически, в случае пропадания основного синхросигнала.
- Поддержка протокола Sync-E.

Система синхронизирует Sync-E, как и PTP с устройства Гранд Мастера. PTP реализуется как цепочка граничных часов (boundary clock).

И Sync-E, и PTP, работают в гибридном режиме и синхронизируются из единого источника.

Тестирование сети MPLS TP при DoS атаке

При функционировании в режиме атаки на отказ в обслуживании (DoS, DDoS) и других видов (трафик РЗ+симуляция атаки):

1. Измерение джиттера, задержки, асимметрии, задержки пакетов и целостности данных.
2. Проверка реализации дублирования пакетов и защитного переключения LSP 1+1 в соответствии с RFC6378.
3. Исследование различных политик QoS и механизмов обработки очередей при переполнении буфера.
4. Исследование влияния недоступности NMS.
5. Исследование устойчивости работы и времени восстановления узлов.

Возможность воздействия на систему управления и мониторинга телекоммуникационной сети, способно привести к полной блокировке оборудования РЗА и делает сеть связи и ее систему управления объектом информационной безопасности. Так, достаточно изменить такой параметр сети, как задержка, чтобы заблокировать основные функции оборудования РЗА. Встроенные в систему мониторинга и управления параметрами сети механизмы могут подвергаться внешнему воздействию или иметь незадекларированные возможности, которые активизируются извне. Это касается не только импортного оборудования, но и отечественного, использующего программные и аппаратные средства зарубежных производителей.

Решением этой проблемы может стать применение отдельной системы мониторинга параметров сети, которая имеет возможность удаленного контроля и изоляции неисправно-

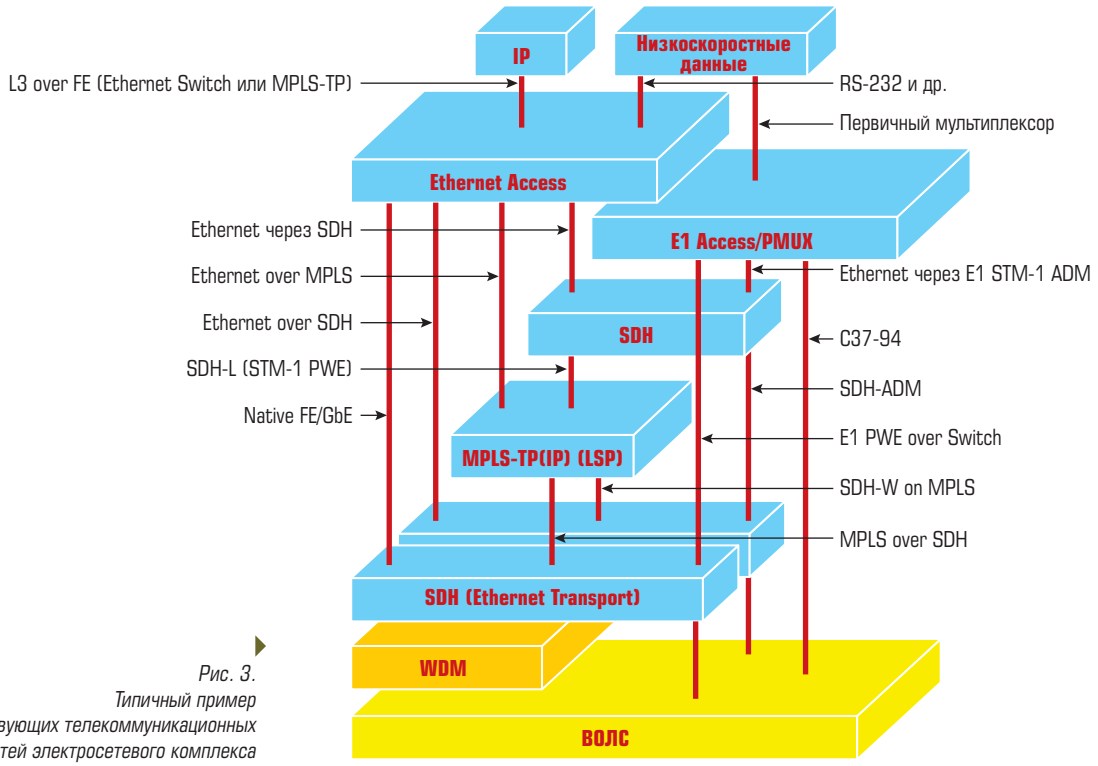

Рис. 3. Типичный пример существующих телекоммуникационных сетей электросетевого комплекса

стей, а также возможность удаленного захвата пакетов, постоянного контроля параметров пакетов, анализ изменений этих параметров, даже если они не превышают допустимую норму, для предиктивного анализа изменений и выдачи рекомендаций для анализа причин. Эти функции реализованы в ряде демаркационных устройств, которые применяются для оценки качества трафика.

Типичный пример существующих телекоммуникационных сетей электросетевого комплекса [4] представлен на рис. 3.

Перспективная телекоммуникационная сеть электросетевого комплекса на основе пакетных технологий с выделенной системой контроля параметров каналов связи для критически важных приложений представлена на рис. 4.

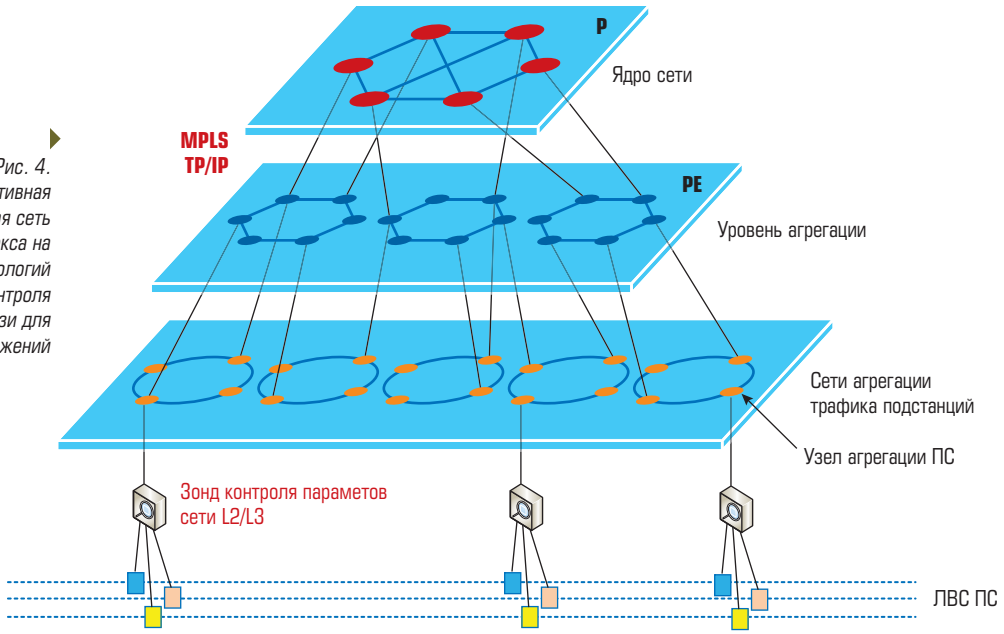

Рис. 4. Перспективная телекоммуникационная сеть электросетевого комплекса на основе пакетных технологий с выделенной системой контроля параметров каналов связи для критически важных приложений

ВЫВОДЫ

Интеллектуальные сети улучшают возможности традиционной электрической сети. Эти сети обеспечивают электроэнергию по требованию с использованием информационно-коммуникационных технологий, которые позволяют поставщикам контролировать подачу электроэнергии и обеспечивают эффективную подачу электроэнергии с меньшими затратами. Однако это делает сети более сложными и уязвимыми для различных типов атак и непреднамеренных сбоев из-за повышенной сложности систем. В тоже время, традиционные сети и интеллектуальные сети должны использовать телекоммуникационные технологии, снижающие возможности внешнего воздействия и облегчающие контроль состояния сети с целью предупреждения и ликвидации последствий этого воздействия. Применение в транспортной сети связи электросетевого комплекса технологии MPLS-TP и дополнительных средств мониторинга параметров сети значительно затрудняют воздействие на сеть внешних факторов, и упрощают задачи эксплуатационного персонала.

Сеть связи для объектов среднего напряжения – наиболее уязвимый сегмент ССЭСК с точки зрения ИБ. Использование комбинации ВЧ связи по ВЛ (NBPLC модемов российского производства, соответствующих СТО 34.01-9.1-002-2018), для передачи сигналов управления и модемов операторов мобильной связи для телесигнализации, делает сеть практически неуязвимой для внешнего воздействия.

Список литературы

1. *СТО 34.01-9.1-002-2018.* “Оборудование ВЧ-связи для передачи сигналов по сетям низкого и среднего напряжения. Общие технические условия”.
2. *С. Портной, О. Карандин, В. Гусев.* ПЕРВАЯ МИЛЯ 7-8/2020. Экспериментальное исследование помехоустойчивого кодека для системы связи по ЛЭП.
3. *СТО 34.01-9-005-2020.* “Концепция построения сети связи электросетевого комплекса”.
4. *CEN-CENELEC-ETSI.* Smart Grid Coordination Group. Smart Grid Reference Architecture. November 2012.
5. *TSAN:* Backbone Network Architecture for Smart Grid of P.R China International Journal of Advanced Computer Science and Applications. 2018, vol. 9, no. 1.

Лифшиц Александр Михайлович *– Председатель совета директоров ООО “НПЦ Приоритет”, академик МАС (Международная академия связи).*