ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО
«ФЕДЕРАЛЬНАЯ СЕТЕВАЯ КОМПАНИЯ
ЕДИНОЙ ЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ»

РОССЕТИ
ФСК ЕЭС

СТАНДАРТ ОРГАНИЗАЦИИ ПАО «ФСК ЕЭС»

СТО 56947007-29.240.10.302-2020

Типовые технические требования к организации и производительности технологических ЛВС в АСУ ТП ПС ЕНЭС

Стандарт организации

Дата введения: 26.02.2020

ПАО «ФСК ЕЭС»
2020

gost.e-ecolog.ru

Предисловие

Цели и принципы стандартизации в Российской Федерации установлены Федеральным законом от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации»; общие положения при разработке и применении стандартов организации – в ГОСТ Р 1.4-2004 «Стандартизация в Российской Федерации. Стандарты организаций. Общие положения»; 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: ООО «Интеллектуальные Сети».
2. ВНЕСЁН: Департаментом релейной защиты, метрологии и автоматизированных систем управления технологическими процессами, Департаментом инновационного развития.
3. УТВЕРЖДЁН И ВВЕДЁН В ДЕЙСТВИЕ:

   Приказом ПАО «ФСК ЕЭС» от 26.02.2020 № 68.
4. СОГЛАСОВАН: письмом АО «СО ЕЭС» от 22.01.2020 № В31-I-2-19-714.
5. ВВЕДЁН: ВПЕРВЫЕ.

Замечания и предложения по стандарту организации следует направлять в Департамент инновационного развития ПАО «ФСК ЕЭС» по адресу: 117630, Москва, ул. Ак. Челомея, д. 5А, 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 «ФСК ЕЭС».

Содержание

1. Область применения 5
2. Нормативные ссылки 5
3. Термины, определения, обозначения и сокращения 6
3.1. Термины и определения 6
3.2. Обозначения и сокращения 8
4. Технические требования к техническому обеспечению ЛВС 11
4.1. Промышленный коммутатор 11
4.2. Промышленный коммутатор Redundancy Box 12
4.3. Межсетевой экран 12
4.4. Система обеспечения единого времени 13
4.5. Промышленные устройства обнаружения и предотвращения вторжения 14
4.6. Регистратор событий ЦПС 15
4.7. Структурированные кабельные системы 16
5. Общие технические требования 17
5.1. Требования к надежности 17
5.2. Требования к электромагнитной совместимости 18
5.3. Требования к организации электропитания ЛВС 18
5.4. Требования к климатическим условиям 18
6. Организационно-технические требования 20
6.1. Типовые требования к общей архитектуре сети. Варианты типовых структур построения сети и внутрисистемных коммуникаций для различных архитектур построения сетей АСУ ТП и РЗА 20
6.2. Организационно-технические требования к безопасности, в том числе информационной 22
6.3. Требования к системе мониторинга и управления сетью 28
6.4. Требования к программному обеспечению 30
6.5. Типовые требования к интеграции информации от смежных систем и подсистем. Типовые требования к протоколам обмена данными 30
6.6. Требования к организации удаленного доступа к сети 31
6.7. Требования к проектированию ЛВС 31

6.8. Требования к производительности и допустимым нагрузкам на сеть, при которых сохраняется стабильная работа АСУ ТП и РЗА и требуемый уровень надежности 37
6.9. Требования к условиям и организации эксплуатации ЛВС 41
6.10. Требования к стандартизации и унификации ЛВС 42
6.11. Требования к приемке ЛВС 43
6.12. Требования к квалификации обслуживающего персонала 44
Приложение А_Типовые структуры построения сети и внутрисистемных коммуникаций для различных архитектур построения сетей АСУ ТП и РЗА 45
Приложение Б_Методика расчета количества оборудования ЛВС и ШСК 50
Приложение В_Типовые карты обслуживания шкафов сетевой коммутации (ШСК) 59
Библиография 60

1 Область применения

Настоящий стандарт устанавливает нормы и требования к организации и производительности технологических локально-вычислительных сетей в автоматизированных системах управления технологическими процессами подстанций Единой национальной электрической сети (ЛВС в АСУ ТП ПС ЕНЭС). В настоящей редакции стандарта не устанавливаются требования к интеграции программно-аппаратных средств систем мониторинга качества электроэнергии, мониторинга переходных процессов, оборудования АИИС КУЭ.

СТО должен применяться проектными организациями, производителями оборудования АСУ ТП, организациями, занимающимися вопросами разработки и внедрения АСУ ТП, службами РЗА и АСУ ТП ПАО «ФСК ЕЭС» при создании и расширении программно-технических комплексов АСУ ТП подстанций ЕНЭС.

В настоящий СТО должны быть внесены изменения в случаях ввода в действие новых технических регламентов и национальных стандартов, содержащих требования, неучтенные в стандарте, а также при необходимости введения новых требований и рекомендаций, обусловленных развитием техники.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие документы:

ГОСТ 34.003-90 Информационная технология (ИТ). Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

ГОСТ Р 51317.6.5-06 (МЭК 61000-6-5:2001) Совместимость технических средств электромагнитная. Устойчивость к электромагнитным помехам технических средств, применяемых на электростанциях и подстанциях. Требования и методы испытаний.

ГОСТ Р 53114-08 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

ГОСТ Р 55438-13 Единая энергетическая система и изолированно работающие энергосистемы. Оперативно-диспетчерское управление. Релейная защита и автоматика. Взаимодействие субъектов электроэнергетики и потребителей электрической энергии при создании (модернизации) и эксплуатации. Общие требования (с Изменением № 1).

ГОСТ Р 56205-14 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели.

ГОСТ Р 56939-16 Защита информации. Разработка безопасного программного обеспечения. Общие требования.

ГОСТ Р 57114-16 Единая энергетическая система и изолированно работающие энергосистемы. Электроэнергетические системы. Оперативно-диспетчерское управление в электроэнергетике и оперативно-технологическое управление. Термины и определения.

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

ГОСТ Р МЭК 61850-5-11 Сети и системы связи на подстанциях. Часть 5. Требования к связи для функций и моделей устройств.

ГОСТ Р МЭК 61850-7-1-09 Сети и системы связи на подстанциях. Часть 7. Базовая структура связи для подстанций и линейного оборудования. Раздел 1. Принципы и модели.

ГОСТ Р МЭК 61850-7-2-09 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 61850-7-3-09 Сети и системы связи на подстанциях. Часть 7. Базовая структура связи для подстанций и линейного оборудования. Раздел 3. Классы общих данных.

ГОСТ Р МЭК 61850-7-4-11 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.

3 Термины, определения, обозначения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по ГОСТ 34.003, ГОСТ Р 53114, ГОСТ Р 55438, ГОСТ Р 56205, ГОСТ Р 57114, а также следующие термины с соответствующими определениями:

Автоматизированная система технологического управления (АСТУ) – Совокупность взаимосвязанных технических и программных средств, обеспечивающих решение задач оперативно-технологического управления.

Автоматизированная система управления технологическими процессами (АСУ ТП) – Совокупность взаимосвязанных технических и программных средств, включающая подсистемы сбора и передачи информации о параметрах работы оборудования и устройств объекта электроэнергетики, диагностики и мониторинга технологического оборудования и устройств, инженерных систем, управления оборудованием и устройствами с целью реализации задач управления технологическими процессами объекта электроэнергетики.

Интерфейс – логический вход или выход, которые обеспечивают передачу потоков логической информации к модулю или из модуля.

Информационная безопасность (ИБ) – состояние защищенности в условиях угроз в информационной сфере.

Коммутатор – активный сетевой компонент, который соединяет две или несколько подсетей, которые, в свою очередь, могут состоять из сегментов, соединенных повторителями.

Локальная вычислительная сеть (ЛВС) – коммуникационная сеть, предназначенная для связывания между собой компьютеров и других интеллектуальных устройств в ограниченной географической области.

Маршрутизатор – шлюз между двумя сетями, функционирующими на уровне 3 взаимодействия открытых систем (OSI), который перенаправляет и посылает пакеты данных во внутреннюю сеть.

Межсетевой экран – устройство межсетевого взаимодействия, осуществляющее фильтрацию трафика между двумя связанными друг с другом сетями.

Промышленное исполнение – исполнение изделия, которое должно сохранять свои параметры в пределах норм, установленных техническими требованиями в течение сроков службы и сроков сохраняемости, указанных в техническом стандарте, после и (или) в процессе воздействия климатических факторов, значения которых установлены настоящим стандартом.

Противоаварийная автоматика (ПА) – совокупность устройств, обеспечивающих измерение и обработку параметров электроэнергетического режима энергосистемы, передачу информации и команд управления и реализацию управляющих воздействий в соответствии с заданными алгоритмами и настройкой для выявления, предотвращения развития и ликвидации аварийного режима энергосистемы.

Релейная защита и автоматика (РЗА) – Релейная защита, сетевая автоматика, противоаварийная автоматика, режимная автоматика, регистраторы аварийных событий и процессов, технологическая автоматика объектов электроэнергетики.

Удаленный доступ – использование систем, которые находятся в пределах периметра зоны безопасности, предусмотренное из другой географической точки, причем указанное использование осуществляется на тех же правах, как если бы системы физически находились в этой точке.

3.2 Обозначения и сокращения

АРМ	Автоматизированное рабочее место
АСУ ТП	Автоматизированная система управления технологическими процессами
АУВ	Автоматика управления выключателем
ДМЗ	Демилитаризованная зона
ЕНЭС	Единая национальная электрическая сеть
ЕЭС	Единая энергетическая система
ИБ	Информационная безопасность
ИЭУ	Интеллектуальное электронное устройство
КИИ	Критическая информационная инфраструктура
КП	Контроллер присоединения
ЛВС	Локальная вычислительная сеть
МЭК	Международная электротехническая комиссия
ОПУ	Общеподстанционный пункт управления
ОРУ	Открытое распределительное устройство
ПА	Противоаварийная автоматика
ПАС	Преобразователь аналоговых сигналов
ПДС	Преобразователь дискретных сигналов
ПО	Программное обеспечение
ПС	Подстанция
ПТК	Программно-технический комплекс (средство)
РАС	Регистратор аварийных событий
РДУ	Региональное диспетчерское управление, филиал АО «Системный оператор единой энергетической системы»
РЗА	Релейная защита, сетевая автоматика, противоаварийная автоматика, режимная автоматика, регистраторы аварийных событий и процессов, технологическая автоматика объектов электроэнергетики
РС ЦПС	Регистратор событий цифровой подстанции
СКС	Структурированные кабельные системы
СКСУ	Станционный контроллер связи и управления
СМиУКЭ	Система мониторинга и управления качеством электроэнергии

СОВ	Система обнаружения вторжения
СОЕВ	Система обеспечения единого времени
СТО	Стандарт организации
ТН	Трансформатор напряжения
ТТ	Трансформатор тока
УПАСК	Устройство передачи аварийных сигналов и команд
УСВИ	Устройство синхронизированных векторных измерений
УСО	Устройство связи с объектом
ЦПС	Цифровая подстанция
ЦТН	Цифровой трансформатор напряжения
ЦТТ	Цифровой трансформатор тока
ЦУС	Центр управления сетями
ШПАС	Шкаф преобразователей аналоговых сигналов
ШПДС	Шкаф преобразователей дискретных сигналов
ШСК	Шкаф сетевых коммутаторов
ШСО	Шкаф серверного оборудования
ШШП	Шкаф шины процесса
ЭТН	Электронный трансформатор напряжения
ЭТТ	Электронный трансформатор тока
DANP	Double Attached Node for PRP (англ.) – устройство с двумя независимыми интерфейсами, может напрямую подключаться к двум параллельным сетям, работающим в системе PRP
ERSPAN	Encapsulated Remote Switch Port Analyzer (англ.) – дублирование пакетов в L3 сетях с применением механизма GRE инкапсуляции
GOOSE	Generic Object Oriented Substation Event (англ.) – общие объектно-ориентированные события на подстанции
GPS	Global Positioning System (англ.) – система глобального позиционирования
IP	Internet Protocol (англ.) – межсетевой протокол
MMS	Manufacturing Message Specification (англ.) – протокол МЭК 61850-8-1 для передачи данных от интеллектуальных устройств в систему управления
MRP	Multiple Registration Protocol (англ.)

OSI	Open systems interconnection basic reference model (англ.) – базовая эталонная модель взаимодействия открытых систем
PRP	Parallel Redundancy Protocol model (англ.) – протокол бесшовного параллельного резервирования
PTP	Precision Time Protocol (англ.) – протокол точного времени, используемый для синхронизации часов по компьютерной сети
QoS	Quality of Service (англ.) – качество обслуживания
RSPAN	Remote Switch Port Analyzer (англ.) – дублирование пакетов одного порта сетевого коммутатора на порту другого сетевого коммутатора
RSTP	Rapid spanning tree protocol (англ.) – протокол резервирования, создающий древовидную структуру
SCD	Substation Configuration Description (англ.) – файл описания конфигурации подстанции
SIEM	Security information and event management (англ.) – система управления событиями безопасности
SPAN	Switched Port Analyzer (англ.) – дублирование пакетов одного порта сетевого коммутатора на другом
SV	Sampled Values (англ.) – протокол МЭК 61850-9-2 для передачи мгновенных значений тока и напряжения от измерительных трансформаторов
VLAN	Virtual Local Area Network (англ.) – логическая локальная вычислительная сеть
VRRP	Virtual Router Redundancy Protocol (англ.) – сетевой протокол для создания виртуального роутера на базе участвующих в этом процессе физических роутеров или L3-интерфейсов коммутаторов

4 Технические требования к техническому обеспечению ЛВС

4.1 Промышленный коммутатор

4.1.1 Сетевые коммутаторы (далее коммутаторы) относятся к активному сетевому оборудованию, обеспечивающему информационные связи устройств полевого уровня и уровня присоединения, устройств уровня присоединения и станционного уровня, и вместе с структурированными кабельными сетями составляют инфраструктуру передачи информации, являющуюся неотъемлемым архитектурным элементом подстанции.

4.1.2 Коммутатор функционирует на канальном (втором) уровне модели взаимодействия открытых систем (OSI) и обеспечивает выполнение следующих функций:

– непрерывность связи между устройствами ЛВС для возможности передачи трафика иному сетевому сегменту;

– построение единственного маршрута передачи данных по ЛВС без петель коммутации, приводящих к широковещательным штормам на данном участке ЛВС;

– установку приоритетов в доступе к ресурсам сети определенным видам трафика.

Коммутаторы должны обеспечивать надежную передачу данных между источником и приемником с заданными параметрами (время доставки, приоритезация и др.).

Коммутатор может обеспечивать функции маршрутизатора при наличии соответствующих технических возможностей и соответствии требованиям к маршрутизаторам.

4.1.3 Коммутаторы шины процесса и станционной шины должны поддерживать протокол синхронизации времени PTP (поддержка режимов master, slave, transparent clock) для станционной шины – программно, для шины процесса – аппаратно.

4.1.4 Коммутаторы обязательно должны поддерживать механизмы QoS (IEEE 802.1D) и VLAN (IEEE 802.1Q).

4.1.5 Коммутаторы обязательно должны поддерживать технологию зеркалирования трафика (например, SPAN) и удаленного зеркалирования (например, RSPAN или ERSPAN) от источников типа «порт» и «VLAN».

4.1.6 Коммутаторы шины процесса должны иметь коммуникационные интерфейсы с разъемами LC, выполненные на базе волоконно-оптических каналов связи. Коммутаторы должны иметь коммуникационные интерфейсы, соответствующие требованиям не хуже IEEE 802.3 в части интерфейса 100BASE-FX, и коммуникационные интерфейсы, соответствующие требованиям не хуже IEEE 802.3 в части интерфейса 1000BASE-LX.

4.1.7 Конкретный состав (тип разъемов, скорость передачи) коммуникационных интерфейсов должен определяться при проектировании. Количество коммуникационных интерфейсов сетевого коммутатора должно выбираться при проектировании инфраструктуры передачи информации

подстанции в соответствии с расчетами, выполненными в соответствии с данным СТО.

4.1.8 Промышленные коммутаторы должны соответствовать требованиям, утвержденным ПАО «Россети» и ПАО «ФСК ЕЭС» [1], [2].

4.2 Промышленный коммутатор Redundancy Box

4.2.1 Промышленный коммутатор Redundancy Box (далее RedBox) – коммутатор, реализующий в сети ЛВС технологию резервирования PRP (Parallel Redundancy Protocol) [3]. PRP использует две параллельных сети передачи данных (Сеть «А» и Сеть «В») с произвольной топологией, не исключая ЛВС с отсутствием резервирования (MRP и RSTP).

Сеть «А» и Сеть «В» работают независимо друг от друга и могут не содержать никакой специальной аппаратной или программной поддержки PRP. Сам протокол PRP реализуется на конечных устройствах типа DANP (Double Attached Node for PRP), имеющих два сетевых интерфейса и подключенных к двум независимым сетям.

В основе PRP резервирования – существование минимум двух одновременно активных соединений между двумя узлами сети таким образом, что отправитель данных посылает кадры синхронно по двум независимым Ethernet каналам. Учитывая разную топологию, пропускную способность и загруженность обоих сетей, два кадра доходят до адресата с разной задержкой. Первый пришедший получателю кадр принимается и передается на верхний уровень, второй – удаляется. Сетевое приложение (SAN устройство), принимающее поток данных от RedBox, не ощущает разницы между резервированным с PRP и обычным Ethernet-интерфейсом.

RedBox идентифицирует дублирование кадров благодаря специальному контрольному маркеру RCT (Redundancy Control Trailer) в составе кадров протокола. В дополнение к идентификатору подсети и пользовательским данным в кадр помещается 32-битовое поле, включающее номер последовательности PRP, который служит идентификатором для RedBox для передачи его на верхний уровень или удаления.

4.2.2 RedBox в ЛВС АСУ ТП ПС ЕНЭС предназначены для подключения серверов удаленного доступа и осциллограмм к станционной шине.

4.3 Межсетевой экран

4.3.1 Межсетевой экран (далее МЭ) – оборудование контроля и фильтрации пакетов информации сети передачи данных, осуществляющее контроль и фильтрацию проходящих через него пакетов информации сети передачи данных в соответствии с заданными правилами. Оборудование состоит из комплекса аппаратных и/или программных средств.

4.3.2 Фильтрация пакетов выполняется в целях:

– предотвращения передачи определенного вида трафика, как в локальный сегмент сети передачи данных, так и из него;

– замены адресов, используемых в локальной сети, на адреса, транслируемые вовне, и наоборот.

4.3.3 МЭ, применяемый в АСУ ТП, может иметь программное или программно-техническое исполнение и должен обеспечивать контроль и фильтрацию промышленных протоколов передачи данных (IEC, Modbus, Profibus и (или) иные протоколы).

4.3.4 МЭ располагаются на границах демилитаризованной зоны и АСУ ТП (шина управления и шина станции) и на границе демилитаризованной зоны и оборудования связи с вышестоящими системами управления.

На границах демилитаризованной зоны и АСУ ТП применяются МЭ типа «Б» или типа «Д», на физической границе (периметре) информационной системы применяются МЭ типа «А» или типа «Д» в соответствии с методическими документами ФСТЭК России.

4.3.5 Для обеспечения надежности межсетевые экраны должны поддерживать технологию VRRP, которая позволяет формировать отказоустойчивую, прозрачную систему из группы роутеров, работающих как один отказоустойчивый шлюз по умолчанию (первый узел маршрута).

4.4 Система обеспечения единого времени

4.4.1 Система обеспечения единого времени (СОЕВ) обеспечивает синхронизацию времени на подстанции с помощью первичных и вторичных часов. Время задается на первичных часах, которые синхронизируются по внешним каналам связи (спутники GPS/ГЛОНАСС), информация о времени передается по ЛВС подстанции.

СОЕВ состоит из:

– приемника (активной антенны) спутникового сигнала точного времени;

– сервера точного времени (ведущих часов);

– коммуникационной сети с аппаратной поддержкой протокола PTP;

– устройств подстанции с синхронизируемыми часами точного времени.

4.4.2 Устройства и каналы СОЕВ должны резервироваться. В системе синхронизации должно иметься не менее 2 серверов точного времени. СОЕВ на подстанции должна обеспечивать календарную синхронизацию времени и инструментальную синхронизацию времени.

4.4.3 Сервер точного времени должен обеспечивать поддержку стандартных сетевых протоколов SNTP, PTP. Протоколы SNTP и PTP должны обрабатываться независимо и не влиять друг на друга в процессе одновременной работы.

4.4.4 Рекомендуемое число независимых сетевых портов на сервере времени – 4.

4.4.5 Для III архитектуры с шиной процесса:

– сервер точного времени, установленный в ШСК №1, подключается к шине управления, шине станции и шине процесса (PRP сеть А);

– сервер точного времени, установленный в ШСК №2, подключается к шине управления, шине станции и шине процесса (PRP сеть Б).

4.4.6 Для I, II архитектуры и III архитектуры с мультишиной:

– сервер точного времени, установленный в ШСК №1, подключается к шине управления и шине станции (PRP сеть А);

– сервер точного времени, установленный в ШСК №2, подключается к шине управления и шине станции (PRP сеть Б).

4.4.7 Основным сервером синхронизации для комплектов основных защит, основных КП, ЭОБ основных каналов, основных устройств шины управления и т.д. является сервер СОЕВ, установленный в ШСК № 1, резервным – сервер СОЕВ, установленный в ШСК № 2.

4.4.8 Основным сервером синхронизации для комплектов резервных защит, резервных КП, ЭОБ резервных каналов, резервных устройств шины управления и т.д. является сервер СОЕВ, установленный в ШСК № 2, резервным – сервер СОЕВ, установленный в ШСК № 1.

4.4.9 Требования к системе обеспечения единого времени на подстанции установлены в соответствующем нормативном документе [4].

4.4.10 Технические характеристики устройств СОЕВ, допустимые габариты, количество интерфейсов должны соответствовать утвержденному стандарту ПАО «ФСК ЕЭС» [2].

4.5 Промышленные устройства обнаружения и предотвращения вторжения

4.5.1 Система обнаружения вторжения (далее СОВ) – специализированный программно-аппаратный комплекс мониторинга сетевого обмена между узлами в промышленной сети систем защиты и управления, который позволяет определять и регистрировать аномальные и важные, с точки зрения обеспечения безопасности эксплуатации оборудования, информационные события.

Об обнаруженных отклонениях технологического процесса от нормы, а также об угрожающих ИБ событиях, СОВ оповещает обслуживающий персонал (в том числе, специалистов ИБ).

4.5.2 Список основных функциональных возможностей СОВ:

– обнаружение и регистрация подключения новых сетевых устройств к контролируемым сегментам технологической сети;

– обнаружение и регистрация новых сетевых коммуникаций между узлами по признакам: адрес узла-отправителя, адрес узла-получателя, протокол обмена, порт, количество допустимых соединений и т.д.;

– обнаружение и регистрация сетевых подключений к ИЭУ с использованием прикладных технологических протоколов, используемых для конфигурирования;

– визуализация цепочек атак: СОВ должна связывать между собой в

цепочку отдельные события, сравнивая их с векторами типичных атак; по мере развития атаки цепочка должна позволить специалистам распознать и оперативно отреагировать на угрозы ИБ;

– СОВ должна иметь возможность быть интегрированной в систему управления событиями безопасности (Security information and event management - SIEM) вышестоящего уровня.

4.5.3 Применение СОВ должно позволять определять большинство возможных событий в технологической сети, являющихся частью сценариев нарушения информационной безопасности, тем самым обеспечивая своевременное информирование персонала о возможном инциденте, а также качественное расследование случаев технологических нарушений.

Наличие СОВ должно позволить точно установить причину технологического нарушения и, соответственно, принять адекватные и эффективные меры недопущения или защиты от подобных инцидентов в будущем.

4.5.4 Сервер СОВ устанавливается в демилитаризованной зоне. СОВ должна иметь копию информационного трафика как шины станции, так и шины управления.

4.5.5 Применение аппаратно-программного комплекса InfoDiode, предназначенного для однонаправленной передачи данных, определяется требованиями проекта и не является обязательным.

4.5.6 Применение СОВ обязательно для подстанций с АСУ ТП категории К2 и К1, рекомендовано для подстанций с АСУ ТП категории К3 в соответствии с приказом ФСТЭК России от 14.03.2014 № 31.

4.5.7 Применение СОВ обязательно для подстанций, на которых размещены объекты КИИ 1 и 2 категории значимости в соответствии с приказом ФСТЭК России от 25.12.2017 № 239; рекомендовано для подстанций, на которых размещены объекты КИИ 3 категории значимости или значимые объекты КИИ отсутствуют.

4.6 Регистратор событий ЦПС

4.6.1 Регистратор событий ЦПС (РС ЦПС) – программно-аппаратный комплекс, выполняющий функцию анализа сетевого трафика шины станции и шины процесса.

4.6.2 Основные функции РС ЦПС:

– анализ данных стандарта МЭК 61850 GOOSE, МЭК 61850-9-2 и корпоративного профиля МЭК 61850 ПАО «ФСК ЕЭС» на предмет соответствия электронному проекту (SCD-файлу);

– контроль параметров передачи SV-потоков и GOOSE-сообщений;

– анализ конфигурации информационной сети на соответствие SCD-файлу;

– мониторинг ошибок на предмет потери или искажения пакетов;

– анализ загруженности ЛВС;

– отображение всех SV-потоков и GOOSE-сообщений в ЛВС;

– регистрация и хранение собранной информации;
– выдача обобщенной сигнализации в АСУ ТП.

4.6.3 Объем дискового хранилища РС ЦПС должен определяться при проектировании и обеспечивать хранение собранной информации в течение не менее трех месяцев.

4.7 Структурированные кабельные системы

4.7.1 Структурированные кабельные системы (СКС) относятся к пассивному оборудованию, обеспечивающему информационные связи устройств полевого уровня и уровня присоединения, устройств уровня присоединения и станционного уровня, и вместе с сетевыми коммутаторами и другим оборудованием составляют инфраструктуру передачи информации, являющуюся неотъемлемым архитектурным элементом АСУ ТП ПС.

4.7.2 В состав инфраструктуры передачи информации подстанции должны входить следующие структурированные кабельные системы:

– шина процесса, технологическая СКС передачи данных основная;
– шина процесса, технологическая СКС передачи данных резервная;
– шина станции, СКС передачи данных основная;
– шина станции, СКС передачи данных резервная;
– шина управления;
– демилитаризованная зона.

4.7.3 Все соединения СКС на подстанции должны выполняться волоконно-оптическим кабелем.

4.7.4 Оптические коммутационные панели служат для распределения оптического сигнала, подведенного к ней по магистральному кабелю, по портам, оборудованным разъемами, к которым подключаются коммутационные шнуры, передающие сигнал на Ethernet-порты активного сетевого оборудования подстанции.

4.7.5 Для соединения устройств полевого уровня, расположенных вблизи основного электротехнического (первичного) оборудования или встроенных в него, с коммутаторами шины процесса должен применяться бронированный волоконно-оптический кабель, конструктивно предназначенный для прокладки вне помещений в кабельной канализации (линейные).

4.7.6 Для соединения устройств уровня присоединения с коммутаторами шины процесса и коммутаторами шины станции, устройств станционного уровня с коммутаторами шины станции должен применяться волоконно-оптический кабель, конструктивно предназначенный для прокладки внутри помещений.

4.7.7 Оптические коммутационные панели, волоконно-оптические кабели и коммутационные шнуры должны соответствовать утвержденному стандарту ПАО «ФСК ЕЭС» [2].

5 Общие технические требования

5.1 Требования к надежности

5.1.1 Одной из важнейших задач ЛВС АСУ ТП является сохранение целостности и доступности технологической информации и управляющих команд. На сегодняшний день использование в АСУ ТП широкого спектра разнообразных технологических устройств, часто принадлежащих к разным поколениям, не позволяют гарантировать доставку информации посредством реализации на этих устройствах семейства функций безопасности «неотказуемость отправления», включающего в себя функции избирательного и принудительного доказательства отправления, избирательного и принудительного доказательства получения.

В связи с этим, обеспечение гарантированной доставки информации организуется путём резервирования и дублирования каналов связи.

5.1.2 Для обеспечения надёжности передачи данных в технологической сети передачи данных и снижения времени восстановления связи после сбоя необходимо применять кольцевую топологию сети с использованием RSTP и MRP [5], [6]. Протокол подразумевает объединение в кольцо группы коммутаторов, один из которых берёт на себя роль ведущего (MRM – Media Redundancy Manager). Ведущий коммутатор осуществляет контроль целостности кольца.

5.1.3 Для передачи наиболее критически важных и чувствительных данных в шине станции и шине процесса, таких как управляющие воздействия и данные измерений от технологического оборудования, необходимо применять протокол «параллельного резервирования» PRP [3]. В пределах каждой сети (PRP сеть А и PRP сеть Б) для коммуникационного оборудования должен использоваться протокол RSTP или иной проприетарный (фирменный) протокол резервирования, созданный на основе семейства протоколов STP, с временем конвергенции (реконфигурации) информационной сети не хуже RSTP.

5.1.4 Надежность функционирования ЛВС АСУ ТП ПС ЕНЭС должна обеспечиваться следующими дополнительными функциями:

- диагностикой коммуникационной инфраструктуры подстанции;
- автоматическим восстановлением после сбоев (перезапуском);
- применением восстанавливаемых устройств (путем использования типовых элементов замены);
- применением типовых проектных решений для проектирования и конфигурирования оборудования системы защиты и управления подстанции;
- применением оборудования, имеющего сертификат соответствия стандарту МЭК 61850;
- проведением испытаний и проверки качества оборудования, предназначенного для применения на подстанции, на соответствие техническим требованиям ПАО «ФСК ЕЭС».

5.1.5 Устройства подстанции должны быть предназначены для функционирования в непрерывном длительном режиме с учетом периодического технического обслуживания. Регламент и периодичность технического обслуживания должны быть указаны производителем в комплекте эксплуатационной документации на устройство.

5.2 Требования к электромагнитной совместимости

5.2.1 Электромагнитная совместимость устройств, обеспечивающих информационные связи на подстанции, должна соответствовать требованиям ГОСТ Р 51317.6.5 и [2], [7].

5.2.2 Электромагнитная совместимость промышленных коммутаторов должна соответствовать утвержденному стандарту ПАО «Россети» [1].

5.3 Требования к организации электропитания ЛВС

5.3.1 Электропитание устройств, обеспечивающих информационные связи на подстанции, должно осуществляться от СОПТ.

5.3.2 Требования к электропитанию устройств постоянным оперативным током приведены в Таблице 5.1 в соответствии с [2].

Таблица 5.1 – Требования к электропитанию

№	**Наименование показателя**	**Значение**
1	Номинальное напряжение, В	220
2	Допустимые длительные отклонения напряжения, %	–20 … +10
3	Допустимый размах пульсаций напряжения по ГОСТ Р 51317.4.17, %	10
4	Провалы напряжения электропитания: в течение 0,1 с, % от номинального; в течение 1,0 с, % от номинального;	 60 30
5	Допустимый перерыв питания без перезапуска, с	0,5

Устройства должны иметь защиту от подачи напряжения питания обратной полярности.

5.3.3 Электропитание промышленных коммутаторов должно соответствовать требованиям утвержденного стандарта ПАО «ФСК ЕЭС» [1].

5.4 Требования к климатическим условиям

5.4.1 Оборудование, обеспечивающее информационные связи на подстанции, должно соответствовать требованиям, предъявляемым к местам расположения.

5.4.1.1 Для оборудования, обеспечивающего информационные связи на подстанции и размещенного в шкафах наружного исполнения (ШПАС, ШПДС, ЭТТ, ЭТН), требования устойчивости к климатическим воздействиям приведены в разделе 6, Таблица 6.1 [2].

5.4.1.2 Для устройств, расположенных в отапливаемом помещении, требования устойчивости к климатическим воздействиям приведены в разделе 6, Таблица 6.2 [2].

5.4.2 Для устройств, встраиваемых в основное электротехническое оборудование (ПАС, ПДС), требования устойчивости к климатическим воздействиям приведены в разделе 6, Таблица 6.3 [2].

5.4.3 Требованиям устойчивости оборудования, обеспечивающего информационные связи на подстанции, к климатическим воздействиям в процессе хранения и транспортирования приведены в разделе 6, Таблица 6.4 [2].

6 Организационно-технические требования

6.1 Типовые требования к общей архитектуре сети. Варианты типовых структур построения сети и внутрисистемных коммуникаций для различных архитектур построения сетей АСУ ТП и РЗА

6.1.1 ПТК АСУ ТП подстанции представляет собой единую, интегрированную, иерархическую распределенную человеко-машинную систему, оснащенную средствами управления, сбора, обработки, отображения, регистрации, хранения и передачи информации.

ПТК состоит из четырех основных уровней программно-технических средств:

- полевой уровень;
- уровень присоединения;
- станционный уровень;
- демилитаризованная зона.

6.1.1.1 К устройствам полевого уровня относятся:

- преобразователи аналоговых сигналов (ПАС);
- преобразователи дискретных сигналов (ПДС);
- волоконно-оптические электронные ТТ и ТН;
- ИЭУ РЗА с функцией АУВ, выполняющие функции контроллера присоединений 6-35 кВ;
- коммутаторы, сетевое оборудование **шины процесса**.

Оборудование полевого уровня устанавливается в непосредственной близости к первичному оборудованию.

6.1.1.2 Устройства уровня присоединения:

- контроллеры присоединений (КП) и УСО;
- интегрируемые устройства смежных систем (РЗ и СА, ПА, ОМП, РС ЦПС, УПАСК и другие устройства - информационно интегрируются, но не входят в состав АСУ ТП);
- станционные контроллеры связи и управления (СКСУ);
- измерительные преобразователи (ИП);
- оборудование СОЕВ;
- коммутаторы, RedBox, сетевое оборудование **шины станции**;
- преобразователи интерфейсов и среды передачи данных;
- конвертеры протоколов.

6.1.1.3 Устройства станционного уровня:

- сервера АСУ ТП;
- АРМ ОП (резервированное) и АРМ РЗА/АСУ;
- система гарантированного питания (СГП);
- коммутаторы, сетевое оборудование **шины управления и шины ДМЗ**;
- сервера удаленного доступа и сбора осциллограмм;
- серверы телемеханики;

– сервер ИБ;
– система обнаружения вторжений.

6.1.2 ИЭУ РЗА имеют двойное назначение: как устройства автономной системы РЗА, так и как компоненты уровня присоединения ПТК АСУ ТП, которые используются в качестве источников значительного объема цифровой информации для решения различных задач контроля и управления объектом в нормальных и аварийных режимах на ПС, а также на верхних уровнях диспетчерско-технологического управления электрическими сетями.

6.1.3 Устройства полевого уровня иерархии управления подстанции осуществляют информационный обмен с устройствами уровня присоединения посредством шины процесса и шины станции.

Устройства уровня присоединения осуществляют информационный обмен с устройствами полевого уровня посредством шины процесса и с устройствами станционного уровня посредством шины станции и шины управления напрямую. Информационный обмен с удаленными центрами управления осуществляется посредством серверов удаленного доступа и осциллограмм, расположенных в ДМЗ.

Устройства станционного уровня осуществляют информационный обмен посредством шины управления и шины станции с устройствами уровня присоединения напрямую и с удаленными центрами управления посредством серверов ТМ, расположенных в ДМЗ.

Демилитаризованная зона предназначена для организации передачи информации из шины управления и шины станции на вышестоящие уровни управления: ЦУС, РДУ, ОДУ и т.д.

Обмен технологической информацией между серверами удаленного доступа и сбора осциллограмм и вышестоящими ДЦ осуществляется по протоколу SFTP. Их удаленный просмотр при необходимости осуществляется с помощью протокола RDP.

6.1.4 В перспективных применениях в условиях повышения пропускной способности оборудования и ресурсов оконечных устройств по обработке целесообразно использовать единую шину данных, объединяющую шину станции и шину процесса, – мультишину.

6.1.5 Сетевое оборудование шины управления, шины ДМЗ, шины станции и шины процесса должно быть резервировано для исключения деградации системы связи при единичном отказе сетевого оборудования.

6.1.6 В зависимости от объемов внедрения цифровых технологий передачи данных на подстанции выделяют три архитектуры подстанций.

I архитектура предполагает применение протокола MMS для интеграции устройств РЗА и КП в единую систему АСУ ТП без использования протоколов GOOSE и SV.

Таким образом, данная архитектура не предполагает использование ШПДС, ШПАС. При проектировании построения сети и внутрисистемных

коммуникаций по I архитектуре следует руководствоваться Приложением А, структурными схемами 1 и 2.

Дополнительные требования в части построения сети и внутрисистемных коммуникаций предъявляются только в части информационной безопасности.

II архитектура предполагает применение протокола MMS для интеграции устройств РЗА и КП в единую систему АСУ ТП, а также использование протокола GOOSE для быстрой передачи информации между устройствами уровня присоединения (РЗА и КП), а также для передачи сигналов между устройствами РЗА и преобразователями дискретных сигналов, установленными в ШПДС.

Применение протокола Sampled Values в данной архитектуре не предусматривается. Вторая архитектура предполагает применение ШПДС.

При проектировании построения сети и внутрисистемных коммуникаций по II архитектуре следует руководствоваться Приложением А, структурной схемой 3.

III архитектура предполагает применение протокола MMS для интеграции устройства РЗА и КП в единую систему АСУ ТП, применение протокола GOOSE для быстрой передачи информации между устройствами уровня присоединений (РЗА и КП) и передачи информации между устройствами РЗА и ШПДС, а также применение протокола Sampled Values для передачи данных измерений токов и напряжений от ЦТТ и ЦТН, и, на переходном этапе, от ШПАС.

При проектировании построения сети и внутрисистемных коммуникаций по III архитектуре следует руководствоваться Приложением А, структурными схемами 4 и 5.

6.1.7 Для II и III архитектуры характерно применение резервированного контроллера присоединений, который устанавливается на каждое распределительное устройство (ОРУ 500 кВ, ОРУ 220 кВ и т.д.). Количество присоединений на КП определяет производитель ПТК.

6.1.8 Одной из функций контроллеров присоединений является диагностика устройств шины процесса, которая выполняется посредством GOOSE-сообщений II класса в соответствии с профилем МЭК 61850 ПАО «ФСК ЕЭС».

6.2 Организационно-технические требования к безопасности, в том числе информационной

6.2.1 Программно-аппаратные средства подстанции должны разрабатываться в соответствии с требованиями ГОСТ Р 56939 для предотвращения появления (или устранения) уязвимостей встроенного и пользовательского ПО.

6.2.2 Формирование требований, разработка и внедрение подсистемы безопасности подстанции должно производиться в соответствии с порядком, установленным приказом ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

6.2.3 Неиспользуемые порты на коммутационном оборудовании должны быть отключены на логическом и физическом уровне.

6.2.4 Решения по сегментации ЛВС

6.2.4.1 ЛВС АСУ ТП ПС должна быть сегментирована на логические сегменты – уровни/шины, определяемые по функциональному назначению с целью построения многоуровневой (эшелонированной) системы защиты.

Должна быть обеспечена защита периметров сегментов. На границах сегментов должно быть реализовано межсетевое экранирование с помощью МЭ, имеющих программное или программно-техническое исполнение (рисунок 6.1).

В ЛВС АСУ ТП ПС, в общем случае, выделяют четыре шины:

- шина процесса – должна быть отделена физически от шины станции;
- шина станции – обеспечивает связь между вторичными устройствами на уровне присоединений и отделена от шины управления при помощи МЭ;
- шина управления – обеспечивает связь между собой АРМ ОП, АРМ РЗА/АСУ, серверов АСУ ТП и отделена от ДМЗ при помощи МЭ типа «Б» или типа «Д»;
- ДМЗ отделена от шины управления и от шины станции при помощи МЭ типа «Д» (возможно применение программного МЭ), а от оборудования связи с вышестоящими уровнями управления при помощи МЭ типа «А» или типа «Д».

6.2.4.2 Для размещения объектов КИИ с разной категорией значимости должны выделяться логические сегменты ЛВС, разделенные средствами межсетевого экранирования.

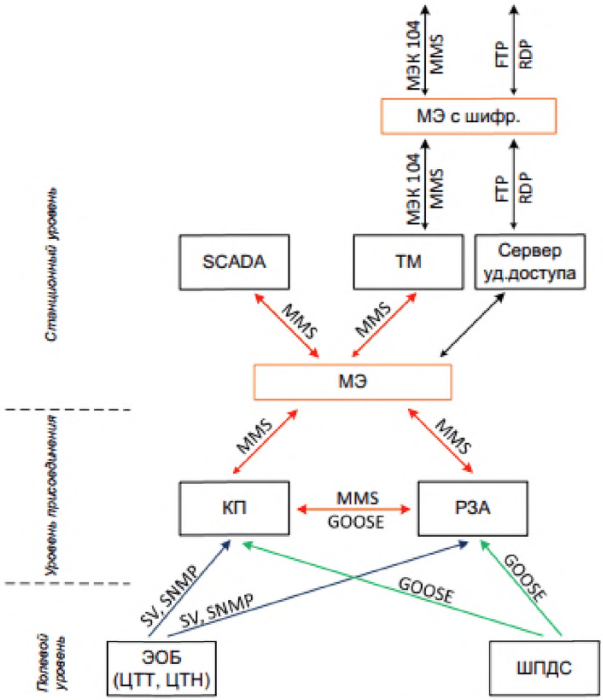


Рисунок 6.1 – Схема информационных потоков и сегментирования ЛВС АСУ ТП ЦПС для III архитектуры

6.2.5 Решения по организации демилитаризованной зоны

6.2.5.1 Для обеспечения информационного обмена с вышестоящими уровнями управления необходима организация демилитаризованной зоны.

На границах ДМЗ должно быть реализовано межсетевое экранирование с помощью МЭ, имеющих программное или программно-техническое исполнение.

6.2.5.2 Устройства АСУ ТП ПС ЕНЭС, расположенные в ДМЗ, перечислены в п. 6.1.1.3.

6.2.5.3 Для организации связи между устройствами, расположенными в ДМЗ, необходимо применять коммутаторы, аналогичные применяемым в шине управления.

6.2.6 Система информационной безопасности

Общеподстанционная система информационной безопасности должна состоять из следующих компонентов:

– объектовая система обнаружения вторжений;
– антивирусное обеспечение (защита АРМ и серверов, сетевого

трафика, защита от шпионского ПО, обнаружение запрещенных сетевых приложений);

- система обновления программного обеспечения;
- центр управления информационной безопасностью.

6.2.6.1 Решения по объектовой системе обнаружения вторжений

Система обнаружения вторжений (СОВ) на сетевом уровне должна контролировать трафик в следующих ключевых точках:

- шина станции RSTP (для I архитектуры);
- шина станции PRP сеть «А»;
- шина станции PRP сеть «Б»;
- шина управления;
- шина ДМЗ.

Для этого с коммутаторов через SPAN-порты трафик направляется на сервер СОВ. Интерфейс сервера СОВ настроен на работу только в режиме приема и неспособен оказать какое-либо влияние на работу АСУ ТП.

SPAN-порты настраиваются на коммутаторах шины управления – по одному на основном и резервном коммутаторе. На SPAN-порт зеркалируется трафик с портов коммутатора, к которым подключены сервера АСУ ТП, и с портов коммутатора, организующих кольцо.

Также SPAN-порты настраиваются на коммутаторах шины станции PRP сети А и Б – по одному из каждой сети. На SPAN-порт зеркалируется трафик с портов коммутатора, организующих кольцо.

Для III архитектуры с отдельной шиной процесса SPAN-порты также настраиваются на коммутаторах шины процесса PRP сети А и Б – по одному из каждой сети. На SPAN-порт зеркалируется трафик с портов коммутатора, организующих кольцо.

СОВ должна обеспечивать возможности, описанные в п. 4.5.2 данного СТО.

СОВ должна иметь документированные процедуры, регламентирующие действия при выявлении инцидентов информационной безопасности с целью оперативного реагирования, устранения причин, последствий и минимизации ущерба от вредоносных внутренних и внешних сетевых вторжений.

6.2.6.2 Решения по антивирусному обеспечению

Для обеспечения безопасности данных от инфицирования вредоносными программами и бесперебойной работы АРМ персонала (включая ноутбуки) и серверов/шлюзов, входящих в состав АСУ ТП, необходимо предусмотреть установку на них антивирусных программ, решающих следующие задачи:

- проверка информации в режиме реального времени (постоянная проверка);
- проверка по требованию – пользователь лично указывает файлы, каталоги или области диска для проверки и время проверки;
- проверка всех внешних носителей информации, flash накопители

каждый раз перед чтением информации с них (если такой доступ предусмотрен).

Для решения указанных задач антивирусная защита должна обладать следующим функциональным составом:

– сигнатурный анализ (однозначная идентификация наличия вируса в файле);

– эвристический анализ (поиск вирусов, похожих на известные, возможность обнаружить новые вирусы еще до того, как для них будут выделены сигнатуры; поиск вирусов, выполняющих подозрительные действия, выделение основных вредоносных действий (удаление файла, запись в файл т.д.);

– модуль обновления, обеспечивающий возможность обновления антивирусных баз, сигнатур и версий антивирусного программного обеспечения без прямого доступа к сети Интернет (для эффективной работы антивирусной защиты необходимо обеспечить регулярное обновление антивирусных баз);

– модуль планирования (позволяет настроить время для проверки всего компьютера на наличие вирусов и обновлять антивирусную базу);

– модуль управления настройками антивируса;

– карантин (позволяет защитить информацию и оборудование от возможной потери данных в результате действий антивируса).

АСУ ТП должна обеспечивать выполнение ряда организационных действий, направленных на усиление защиты по предотвращению проникновения в систему вредоносных программ:

– своевременную установку последних обновлений для используемого программного обеспечения (в первую очередь для операционной системы);

– проверку отключенного состояния всех отключенных USB-портов и дисководов;

– проверку отключенного состояния функции автозапуска;

– проверку включенного состояния постоянной проверки антивируса;

– постоянную проверку актуальности текущих используемых антивирусных баз.

Используемое программное обеспечение системы антивирусной защиты должно обеспечивать следующие функции:

– обнаружение фактов вирусного заражения компонентов АСУ ТП по запросам пользователей и/или администраторов при выполнении периодических проверок оперативной памяти, локальных носителей информации, томов, каталогов, файлов, файлов, получаемых по каналам связи;

– обнаружение фактов вирусного заражения, вызванного всеми известными вирусами;

– реализация процедуры, позволяющей выявлять факты заражения неизвестными вирусами;

– сигнализация в случае обнаружения фактов вирусного заражения;

– обнаружение вирусов в таких объектах, как архивы, компрессированные исполняемые модули, динамические библиотеки и др.;

– возможность восстановления исходного состояния компонентов АСУ ТП, подвергшихся вирусному заражению;

– блокирование доступа к отчуждаемым носителям информации в случае обнаружения фактов вирусного заражения и (или) активизации вируса;

– проведение периодического обновления антивирусных средств (механизмов обнаружения и удаления, расширение списка известных вирусов и алгоритмов поиска и удаления неизвестных вирусов).

Обновление средств защиты от вредоносного программного кода должно осуществляться централизовано. Перед обновлением программного обеспечения системы антивирусной защиты осуществляется тестирование и оценивается воздействие обновлений на функционирование АСУ ТП. Тестирование обновлений системы антивирусной защиты должно осуществляться на отдельном стенде в изолированной среде.

Случаи проникновения и внедрения вредоносного программного кода должны расследоваться в рамках мероприятий по управлению инцидентами ИБ. Восстановление АСУ ТП после воздействия вредоносного программного кода должно осуществляться в рамках регламентированных мероприятий.

6.2.6.3 Решения по системе обновления программного обеспечения

В АСУ ТП должна быть организована система обновления программного обеспечения элементов АСУ ТП.

Обновление программного обеспечения элементов АСУ ТП запрещается производить в автоматическом режиме.

Выполнение любых работ на действующем объекте допускается только после оформления разрешения на проведение работ в установленном на предприятии порядке.

Обновление программного обеспечения элементов АСУ ТП должно осуществляться поэтапно, то есть последовательно для различных элементов АСУ ТП.

Руководитель службы по обслуживанию АСУ ТП должен принимать решение об обновлении программного обеспечения элементов АСУ ТП и определять очередность элементов АСУ ТП.

Должен быть разработан, согласован и поддерживаться в актуальном состоянии план обновлений программного обеспечения.

Перед использованием обновлений программного обеспечения АСУ ТП необходимо проводить проверку функционирования обновлений и их программной совместимости с уже эксплуатируемыми приложениями.

Для проведения проверок функционирования обновлений и их программной совместимости необходимо использовать тестовый стенд, составленный из элементов АСУ ТП, не участвующих в технологическом процессе.

Перед осуществлением проверок на АРМ и серверах АСУ ТП, а также перед установкой обновлений на компоненты АСУ ТП необходимо сохранить

текущую конфигурацию программного обеспечения всех используемых компонентов.

При возникновении неполадок в работе компонентов АСУ ТП после обновлений программного обеспечения необходимо инициировать инцидент информационной безопасности и восстановить программное обеспечение в устойчивое состояние, предшествовавшее инциденту.

6.2.6.4 Центр управления информационной безопасностью

Для защиты всех компьютеров, входящих в состав ЛВС, необходимо применять систему удаленного централизованного управления защитой. Указанная структура должна позволять удаленно обслуживать с заранее выбранного компьютера (например, сервер ИБ) антивирусные программы, установленные на всех рабочих станциях и серверах, входящих в состав ЛВС АСУ ТП, производить их настройку, запускать проверку, обновлять антивирусные базы, и, кроме этого, должна предоставлять возможность тотального контроля за вирусной активностью и состоянием текущей антивирусной защиты всей сети.

Система удаленного централизованного управления должна состоять из отдельных программных компонентов:

– клиентской антивирусной программы - антивирусный комплекс для рабочих станций или сетевых серверов;

– сервера администрирования - программы, которая собирает, обрабатывает и хранит все настройки, информацию обо всех событиях и инцидентах, имевших место в сети, рассылает уведомления и отчеты;

– агента администрирования, который устанавливается на все компьютеры, входящие в логическую сеть системы антивирусной защиты. Этот программный компонент должен обеспечить связь клиентской программы с сервером администрирования и оперативно передавать ему информацию о состоянии антивирусной защиты на этой машине. Также агент администрирования должен получать новые антивирусные базы или другие указания и команды.

6.3 Требования к системе мониторинга и управления сетью

6.3.1 Для мониторинга ЛВС должны использоваться следующие сетевые протоколы и сервисы:

– ICMP – для проверки доступности устройств;

– SNMPv.3 – для проверки доступности и получения параметров устройств;

– SYSLOG – для отправки событий, происходящих в сети.

6.3.2 Диагностика сети должна проводиться стандартными утилитами ОС (ping, tracert, ipconfig / ifconfig, netstat) или специализированным ПО.

6.3.3 Информация о диагностике сети должна отображаться на мнемокадрах АРМ АСУ ТП «Диагностика АСУ ТП», «Диагностика РЗА». При нажатии на изображение сетевого устройства (коммутаторы, межсетевые

экраны, устройства RedBox) должно открываться окно диагностики данного устройства, в котором приведены следующие параметры:

– краткая информация об устройстве – наименование и обозначение оборудования, нумерация интерфейсов;

– информация о состоянии устройства – исправность устройства, исправность блоков питания, температура процессора, загрузка ЦПУ;

– настройки устройства – IP-адрес, подключенное оборудование для каждого порта);

– информация о состоянии портов – цветовая индикация для каждого порта в соответствии с его состоянием (зеленый цвет – есть связь, красный цвет – нет связи, серый цвет – не используется).

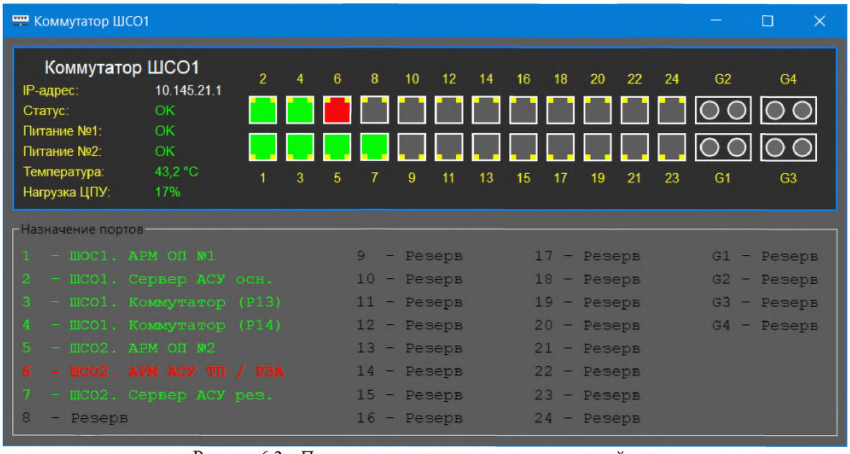


Рисунок 6.2 – Пример окна диагностики сетевого устройства

6.3.4 Управление ЛВС заключается в настройке сетевых параметров коммутаторов, межсетевых экранов, серверов и пр. Управление сетевыми устройствами и их параметрами должно быть доступно с АРМ АСУ ТП только авторизованным пользователям SCADA, которые имеют права для выполнения этих операций. Удаленное управление ЛВС из диспетчерских центров запрещено.

Управление ЛВС должно проводиться через шифрованные протоколы (например, SNMPv3, SSH или HTTPS).

Требуется отключение устаревших и небезопасных протоколов управления (SNMP: v1, v2c; HTTP, FTP, TELNET и пр.).

Управление портами коммутатора доступно только оперативному персоналу и инженерам РЗА/АСУ, авторизованным пользователям SCADA.

6.4 Требования к программному обеспечению

6.4.1 Программное обеспечение оборудования ЛВС должно соответствовать следующим требованиям:

- создание и сохранение резервной конфигурации устройства на самом устройстве;
- возможность обновления программного обеспечения, в том числе удаленное, при обеспечении идентификации обновления и последующего функционального тестирования (методика тестирования должна быть описана в документации на устройство);
- встроенные механизмы проверки на целостность прошивок;
- должно быть русифицировано.

6.5 Типовые требования к интеграции информации от смежных систем и подсистем. Типовые требования к протоколам обмена данными

6.5.1 Устройства смежных систем (РЗ и СА, ПА и др.) должны подключаться к станционной шине ПТК по резервированным каналам передачи данных Ethernet. В качестве основного протокола интеграции должен применяться МЭК 61850-8-1 (MMS).

6.5.2 Для устройств, не поддерживающих сетевое резервирование, подключение к станционной шине ПТК должно быть выполнено через RedBox. Применение протокола МЭК 60870-5-104 должно согласовываться отдельно.

6.5.3 Применение интерфейсов, отличных от Ethernet, и дополнительных устройств (шлюзов) для интеграции смежных систем нежелательно и требует отдельного обоснования. При использовании интерфейсов, отличных от Ethernet, интеграция устройств должна осуществляться по стандартным протоколам МЭК 60870-5-101/103 через СКСУ, располагаемый в отдельном шкафу.

6.5.4 Смежные подсистемы, не входящие в зону обслуживания АСУ, имеющие в составе сегменты ЛВС с возможностью подключения в них внешнего оборудования, должны подключаться к ПТК с помощью сетевых экранов (маршрутизаторов), предотвращающих проникновение в ЛВС ПТК АСУ ТП со стороны этих подсистем, сетевые экраны не резервируются.

К таким подсистемам относятся:

- Система мониторинга и управления качеством электроэнергии (СМиУКЭ);
- Система мониторинга переходных режимов (СМПР);
- Мониторинг трансформаторного оборудования;
- Мониторинг частичных разрядов КРУЭ;
- Мониторинг кабельных линий;
- Регистрация событий ЦПС (РС ЦПС);
- Комплекс систем технических средств безопасности (КСТСБ).

6.6 Требования к организации удаленного доступа к сети

6.6.1 Для организации защищённого доступа к ЛВС АСУ ТП необходимо использовать технологию виртуальных частных сетей Virtual Private Network (VPN).

6.6.2 Для организации защищенного и контролируемого удаленного подключения к АСУ ТП необходима реализация следующих процедур:

- подача заявки на удаленное подключение;
- прохождение согласования;
- выпуск сертификата для удаленной станции удостоверяющим центром;
- контроль действий подключаемого пользователя.

6.6.3 Организационно-распорядительные меры по организации удалённого доступа к ЛВС АСУ ТП должны включать в себя описания следующего набора мероприятий:

- непосредственно подключения;
- подтверждение сертификата;
- контроля и фиксации действий пользователей;
- управления режимами подключений;
- экстренной остановки сеанса подключения.

6.7 Требования к проектированию ЛВС

6.7.1 В проектной документации для подстанций должны быть предусмотрены следующие разделы, описывающие организацию и производительность ЛВС в АСУ ТП ПС ЕНЭС:

- обоснование и выбор топологии ЛВС из числа типовых структурных схем данного СТО;
- расчет числа, типов и мест установки ШСК (п. 6.7.2);
- таблица IP-адресов оборудования АСУ ТП (п. 6.7.3);
- карта распределения по VLAN (п. 6.7.3);
- задание приоритета для каждого типа трафика в соответствии с рекомендациями МЭК 61850 (п. 6.7.4);
- настройка приоритетов и управление информационной нагрузко (п. 6.7.4);
- настройки коммуникационного оборудования (промышленных коммутаторов, межсетевых экранов, коммутаторов RedBox) (п. 6.7.5);
- настройки протокола RSTP при использовании (расчет параметров настройки протокола резервирования сетевых коммутаторов, определение предельно возможного значения радиуса сети Ethernet, расчет предельного времени реконфигурации сети Ethernet) (п. 6.7.6);
- настройки сетевых интерфейсов серверов ТМ;
- карты маршрутизации серверов удаленного доступа и осциллограмм;
- расчет информационной нагрузки (п. 6.8.4);
- схема ЛВС АСУ ТП (п. 6.7.7).

Данные разделы разрабатываются с учетом СТО 56947007-29.240.10.299-2020 «Цифровая подстанция. Методические указания по проектированию ЦПС».

6.7.2 Методика расчета количества оборудования ЛВС и ШСК

Исходные данные: однолинейная схема ПС и количество интеллектуальных устройств, определенных в соответствии со стандартом СТО 56947007-29.240.10.299-2020 «Цифровая подстанция. Методические указания по проектированию ЦПС».

Правила для расчета количества оборудования ЛВС, основанные на технических решениях в рамках типизации НКУ для нужд ПАО «ФСК ЕЭС»:

Правило 1: в один коммутатор можно подключить не более 24 ИЭУ, остальные порты коммутаторов предназначены для внутришкафных соединений (например, устройств СОЕВ) и для соединений коммутаторов между собой при организации оптического кольца.

Правило 2: резерв свободных портов – не менее 10 %.

Правило 3: коммутаторы шины процесса (PRP сети А и Б) следует устанавливать в разных ШСК шины процесса. Если количество подключений оборудования КРУ/ЗРУ 6-35 кВ к шине процесса не велико, то можно выполнить подключение к ШСК шины процесса в помещении ОПУ.

Правило 4: коммутаторы шины станции PRP сети А и PRP сети Б должны устанавливаться в разных шкафах.

Правило 5: основные и резервные коммутаторы шины управления и шины ДМЗ устанавливаются в ШСО № 1 и ШСО № 2 соответственно, к ним подключается оборудование серверных шкафов и шкафа ИБ. Возможна установка коммутаторов шины ДМЗ в шкаф ИБ.

Правило 6: ШСК должны устанавливаться в помещении ОПУ. Для подключения устройств 6-35 кВ, если таких устройств более 10, ШСК можно установить в КРУ/ЗРУ 6-35 кВ.

Правило 7: в один ШСК можно установить не более 5 коммутаторов PRP сети А или PRP сети Б. Если в ШСК устанавливается 2 устройства СОЕВ, то максимальное количество коммутаторов в шкафу – 4.

Правило 8: количество и состав ШСК для устройств, расположенных в одном помещении, должны выбираться с учетом равномерного распределения подключенных устройств по шкафам.

Правило 9: устройства в пределах помещения подключаются к коммутаторам бронированными оптическими патч-кордами, минуя оптический кросс.

Правило 10: Устройства, расположенные на ОРУ (например, ПАС, ПДС) или в других зданиях, подключаются магистральным оптическим кабелем к оптическому кроссу, а далее оптическими патч-кордами к коммутатору. Максимальное количество подключаемых удаленных устройств – 36 (со 100% резервированием жил) или 48 (с 50 % резервированием жил).

Методика расчета:

1. Определить количество терминалов РЗ, СА, ПА, РАС, РС ЦПС, ОМП, УПАСК, КП, ИП, ПАС, ПДС в зависимости от однолинейной схемы ПС.
2. Выбрать топологию ЛВС из числа типовых структурных схем данного СТО.
3. Для архитектуры I, II типа и III типа с мультишиной:
   - 3.1. Определить количество устройств, подключаемых к шине управления и к шине ДМЗ.
   - 3.2. Определить количество основных и резервных коммутаторов шины управления и шины ДМЗ с учетом резерва свободных портов (10-15 %) на основании п. 3.1.
   - 3.3. Если требуется больше одного основного и резервного коммутаторов шины управления, то коммутаторы шины ДМЗ устанавливаются в шкаф ИБ, а на свободное место в ШСО устанавливаются дополнительные коммутаторы.
   - 3.4. Определить количество устройств, подключаемых к АСУ ТП через межсетевые экраны для обеспечения информационной безопасности.
   - 3.5. Определить количество устройств, подключаемых к шине станции, для каждого уровня напряжения отдельно. При этом выделить из их числа устройства, подключаемые магистральным оптическим кабелем (например, ПДС, ПАС).
   - 3.6. Определить количество коммутаторов PRP сети А / сети Б для шины станции для каждого уровня напряжения отдельно с учетом резерва свободных портов (10-15 %) на основании п. 3.7.
   - 3.7. Определить количество ШСК PRP сети А / сети Б для шины станции на основании п. 3.3 и п. 3.8.
   - 3.8. Определить количество портов в оптическом кроссе для ШСК шины станции. Для этого количество устройств, подключаемых магистральным оптическим кабелем из п. 3.7, умножить на 4 (каждое устройство подключается двумя жилами, две жилы резервные).
   - 3.9. Определить количество 16-портовых кассет оптического кросса для ШСК шины станции на основании п. 3.8.
4. Для архитектуры III типа с отдельной шиной процесса дополнительно рассчитать оборудование ЛВС для шины процесса:
   - 4.1. Определить количество устройств, подключаемых к шине процесса, для каждого уровня напряжения отдельно. При этом выделить из их числа устройства, подключаемые магистральным оптическим кабелем.
   - 4.2. Определить количество коммутаторов PRP сети А / сети Б для шины процесса для каждого уровня напряжения отдельно с

учетом резерва свободных портов (10-15 %) на основании п. 4.1.

4.3. Определить количество ШСК PRP сети А / сети Б для шины процесса на основании п. 4.2.

4.4. Определить количество портов в оптическом кроссе для ШСК шины станции. Для этого количество устройств, подключаемых магистральным оптическим кабелем из п. 4.1, умножить на 4 (каждое устройство подключается двумя жилами, две жилы резервные).

4.5. Определить количество 16-портовых кассет оптического кросса для ШСК шины станции на основании п. 4.4.

5. На основании полученных данных сформировать код заказа всех ШСК.

Пример расчета оборудования ЛВС для шины станции и шины процесса приведен в Приложении Б.

6.7.3 Требования к присвоению IP-адресов и присвоению VLAN

В составе рабочей документации должна быть приведена таблица IP-адресов оборудования АСУ ТП, должны быть назначены VLAN в соответствии с рекомендациями данного стандарта (Приложение Г[1]). Пример таблицы IP-адресов и присвоения VLAN для оборудования ПС, рассматриваемой в Приложении Б, приведен в Приложении Д[1].

6.7.4 Требования к организации управления информационной нагрузкой и задания приоритета

Качество обслуживания на втором уровне модели OSI (канальном) в пределах одного сетевого элемента обеспечивается за счет использования модели дифференцированного обслуживания (Differentiated Service – DiffServ).

Спецификация IEEE 802.1p, создаваемая в рамках процесса стандартизации IEEE 802.1Q, определяет метод передачи информации о приоритете сетевого трафика.

Стандарт 802.1p специфицирует алгоритм изменения порядка расположения пакетов в очередях, с помощью которого обеспечивается своевременная доставка чувствительного к временным задержкам трафика.

Для протоколов передачи данных цифровой подстанции рекомендуется применять следующие приоритеты, приведенные в Таблице 6.1.

[1] Примечание. Приложение предоставляется по запросу в Департамент релейной защиты, метрологии и автоматизированных систем управления технологическими процессами ПАО «ФСК ЕЭС» после предоставления подтверждающих документов (договора на проектирование, наладку и т.п.).

Таблица 6.1 – Рекомендуемые приоритеты VLAN

Наименование протокола	**Биты приоритета**	**Обозначение**	**Класс приоритета трафика**
	111 (7)	NC (Network Controlled)	Критически важный для сети
Протокол SV 96(80)	110 (6)	VO (Voice)	
Протокол SV 288(256)	101 (5)	VI (Video)	
Протокол GOOSE тип 1	100 (4)	CL (Controlled Effort)	
Протокол GOOSE тип 2	011 (3)	CA (Critical Applications)	
	010 (2)	EE (Excellent Effort)	Стандартный
	001 (1)	BE (Best Effort)	Фоновый
Остальные протоколы	000 (0)	BK (Background)	Низший

6.7.5 Требования к настройкам коммуникационного оборудования

В составе рабочей документации должны быть приведены настройки сетевых коммутаторов, межсетевых экранов, коммутаторов RedBox. Описание и пример настройки межсетевых экранов приведен в Приложении Е[2].

Пример управления портами коммутатора, к которым подключены терминалы РЗА, для реализации управляемой деградации сети в случае обнаружения в ней нарушителя приведен в Приложении Ж[2].

6.7.6 Требования к архитектуре и настройке коммуникационного оборудования, использующего протокол резервирования RSTP

Данные требования распространяются на шину станции (PRP сеть А и PRP сеть Б), шину управления и шину ДМЗ в случае применения больше двух коммутаторов.

Для обеспечения надежности сетей используют избыточные связи между оборудованием для предотвращения потери данных при обрыве соединений. Такие топологии подвержены возникновению широковещательного шторма из-за образовавшихся петель. Чтобы подобные отказоустойчивые системы имели возможность корректно функционировать, необходимо применять протокол RSTP или аналогичный.

Требования по параметрированию RSTP (на всех коммутаторах кольца):

- Активировать глобально протокол RSTP на устройстве.
- Назначить параметр Bridge Priority в соответствии с Таблицей 6.2.
- Параметр Hello Time выставить равным 1 с для уменьшения времени перестроения дерева.
- На портах, не участвующих в кольце, отключить протоколы резервирования (обязательно).

[2] Приложение. Предоставляется по запросу в Департамент релейной защиты, метрологии и автоматизированных систем управления технологическими процессами ПАО «ФСК ЕЭС» после предоставления подтверждающих документов (договора на проектирование, наладку и т.п.).

Таблица 6.2 – Таблица параметров Bridge Priority

Коммутатор	Значение параметра Bridge Priority
Коммутатор 1	0
Коммутатор 2	4096
Коммутатор 3	8192
Коммутатор 4	12288
Коммутатор 5	16384
Коммутатор 6	20480
Коммутатор 7	24576
Коммутатор 8	28672
Коммутатор 9	32768
Коммутатор 10	36864
Коммутатор 11	40960
Коммутатор 12	45056
Коммутатор 13	49152
Коммутатор 14	53248
Коммутатор 15	57344

Параметрирование портов, участвующих в кольце:

– На портах, участвующих в кольце, активировать протокол резервирования.

– Назначить параметр RSTP Port Cost в соответствии с Таблицей 6.3.

– Параметр Edge Port выставить равным False.

Таблица 6.3 – Параметры RSTP Port Cost

Скорость кольцевого порта	Значение параметра RSTP Port Cost
40 Гбит/с	500
10 Гбит/с	2 000
1 Гбит/с	20 000
100 Мбит/с	200 000

Коммутатор 1 в таком случае будет корневым (root).

Минимальные значения Bridge Priority назначаются коммутаторам, наиболее близким к устройствам RedBox и межсетевым экранам.

Стандарт протокола RSTP рекомендует использовать диаметр сети не более 7 (не более 15 коммутаторов в кольце).

Следует учитывать, что производители коммутаторов вносят проприетарные изменения в протоколы резервирования. Кольца, построенные на базе продуктовой линейки одного производителя, могут переконфигурироваться значительно быстрее стандартного протокола RSTP и иметь дополнительные параметры настройки.

6.7.7 Требования к схеме ЛВС АСУ ТП

На схеме ЛВС АСУ ТП должно быть показано сетевое оборудование АСУ ТП и устройства, подключенные к нему. Для каждого подключенного устройства должна указываться следующая информация:

- IP-адрес устройства в формате aaa.bbb.ccc.ddd;
- номер устройства в формате IEDccddd;
- количество MMS- и GOOSE-сообщений и SV-потоков.

Пример схемы ЛВС АСУ ТП ПС с отдельной шиной процесса приведен в Приложении И[3].

Пример схемы ЛВС АСУ ТП ПС с мультишиной приведен в Приложении К[3].

6.8 Требования к производительности и допустимым нагрузкам на сеть, при которых сохраняется стабильная работа АСУ ТП и РЗА и требуемый уровень надежности

6.8.1 Оценку информационной нагрузки на ЛВС при проектировании необходимо проводить в первую очередь для сегмента сети, где осуществляется передача данных по протоколу SV в связи с высокой нагрузкой указанного протокола.

6.8.2 Пропускная способность сети

Пропускная способность V_{max} это максимально возможная для данной сети скорость передачи данных, которая определяется битовой скоростью и некоторыми другими ограничивающими факторами (длительность интервалов между передаваемыми блоками данных, объем передаваемой по сети служебной информации и др.). Значения пропускной способности для сетевых технологий известны и приводится в документации на устройства. В большинстве случаев можно принять пропускную способность равной битовой скорости.

Для расчетов V_{max} для стандарта 100BASE-TX (Fast Ethernet) принимаем 12Мб/с, для стандарта 1000BASE-TX (Gigabit Ethernet) – 120Мб/с.

6.8.3 В проектах цифровых подстанций применяются форматы кадров SV (ASDU — количество выборок для одной фазы, передаваемых в одном кадре) и частоты дискретизации в соответствии с данными, приведенными в Таблице 6.4.

Таблица 6.4 – Спецификация форматов кадра SV, частоты дискретизации и набора данных для различных профилей

Профиль	РЗА	АСКУЭ	Структура набора данных
МЭК 61850-9-2LE	4000 Гц, 1 ASDU	12 800 Гц, 8 ASDU	Фиксированный набор данных для всех видов присоединений: 4 тока, 4 напряжения
Профиль ПАО «ФСК ЕЭС» на базе МЭК 61869-9	4800 Гц, 2 ASDU	14 400 Гц, 6 ASDU	Форматы набора данных: 3 тока, 3 напряжения, 1 ток, 1 напряжение

[3] Примечание. Приложение предоставляется по запросу в Департамент релейной защиты, метрологии и автоматизированных систем управления технологическими процессами ПАО «ФСК ЕЭС» после предоставления подтверждающих документов (договора на проектирование, наладку и т.п.).

В Таблице 6.5 приведены расчётные значения нагрузки, формируемые потоками SV для профиля МЭК 61850-9-2 LE и для Профиля ПАО «ФСК ЕЭС» на базе МЭК 61869-9.

Таблица 6.5 – Эмпирические значения нагрузки от разных видов информационных потоков

Количество потоков	**Загрузка канала Ethernet, Мб/с**	
	МЭК 61850-9-2LE	**Профиль ПАО «ФСК ЕЭС» на базе МЭК 61869-9**
1 поток РЗА (1 аналоговый сигнал)	5,12	2,82
1 поток РЗА (3 аналоговых сигнала)	5,12	3,44
8 потоков РЗА (3 аналоговых сигнала)	40,96	27,49
1 поток АИИСКУЭ (1 аналоговый сигнал)	11,10	6,12
1 поток АИИСКУЭ (3 аналоговых сигнала)	11,10	7,97
8 потоков АИИСКУЭ (3 аналоговых сигнала)	88,20	63,74

В Таблице 6.6 приведены расчётные значения нагрузки, формируемые потоками SV для типовых шкафов РЗА для профиля МЭК 61850-9-2 LE и для Профиля ПАО «ФСК ЕЭС» на базе МЭК 61869-9.

Таблица 6.6 – Эмпирические значения нагрузки от потоков SV для типовых шкафов РЗА (справочно)

Наименование схемы	**Количество потоков**	**Загрузка канала Ethernet, Мб/с**	
		МЭК 61850-9-2LE	**Профиль ПАО «ФСК ЕЭС» на базе МЭК 61869-9**
Шкаф комплекса дифференциальных защит сборных шин 110 – 220 кВ ШЭТ 240.01-2	40 потоков (3тока) + 2 потока (3 напряжения)	215,04	144,48
Шкаф защиты сборных шин 330 – 750 кВ ШЭТ 340.01-2	12 потоков (3тока) + 2 потока (3 напряжения)	71,68	48,16
Шкаф защиты ошиновки 110 – 750 кВ ШЭТ 441.01-2	6 потоков (3тока) + 5 потоков (3 напряжения)	56,32	37,84

Наименование схемы	Количество потоков	Загрузка канала Ethernet, Мб/с	
		МЭК 61850-9-2LE	Профиль ПАО «ФСК ЕЭС» на базе МЭК 61869-9
Шкаф защит ОВ 110 – 220 кВ ШЭТ 251.01-2	4 потока (3 тока) + 2 потока (3 напряжения) + 1 поток (1 напряжение)	35,84	24,08
Шкаф защит ШСВ/СВ 110 – 750 кВ ШЭТ 451.01-2	2 потока (3 тока) + 4 потока (3 напряжения)	30,72	20,64
Шкаф защит ЛЭП 110 – 220 кВ ШЭТ 221.01-2, ШЭТ 221.02-2, ШЭТ 221.03-2, ШЭТ 221.04-2, ШЭТ 221.05-2, ШЭТ 221.06-2	8 потоков (3 тока) + 3 потока (3 напряжения)	56,32	37,84
Шкаф защит ЛЭП 330 – 750 кВ ШЭТ 321.01-2, ШЭТ 321.02-2, ШЭТ 321.03-2, ШЭТ 321.04-2, ШЭТ 321.05-2	14 потоков (3 тока) + 6 потоков (3 напряжения)	102,4	68,8
Шкаф защит батареи статических конденсаторов ШЭТ 431.01-2	8 потоков (3 тока) + 1 поток (1 ток) + 2 потока (3 напряжения)	56,32	37,22
Шкаф защит шунтирующего реактора 110-750 кВ ШЭТ 431.02-2	15 потоков (3 тока) + 3 потока (3 напряжения)	92,16	61,92
Шкаф защит компенсационного реактора ШЭТ 431.03-2	4 потока (3 тока) + 3 потока (1 ток) + 1 поток (1 напряжение)	40,96	25,04
Шкаф защит трансформатора 110-220 кВ и ошиновки 6-35 кВ ШЭТ 211.01-2	16 потоков (3 тока) + 4 потока (1 ток) + 4 потока (3 напряжения)	122,88	80,08
Шкаф основных защит автотрансформатора 220 кВ и ошиновки 6-35 кВ ШЭТ 211.02-2	14 потоков (3 тока) + 5 потоков (3 напряжения)	97,28	65,36
Шкаф основных защит автотрансформатора 330-750 кВ и ошиновки 6-35 кВ ШЭТ 311.01-2	14 потоков (3 тока) + 3 потока (3 напряжения)	87,04	58,48

Наименование схемы	Количество потоков	Загрузка канала Ethernet, Мб/с	
		МЭК 61850-9-2LE	Профиль ПАО «ФСК ЕЭС» на базе МЭК 61869-9
Шкаф резервных защит автотрансформатора 220-750 кВ ШЭТ 410.01-2	4 потока (3 тока) + 5 потоков (3 напряжения)	46,08	30,96
Шкаф автоматики пуска пожаротушения ШЭТ 400.01-2	24 потока (3 тока) + 6 потоков (3 напряжения)	153,6	103,2
Для канала 1 ГБ	195 потоков РЗА	998,4	670,8
	290 потоков РЗА	-	997,6

6.8.4 Методика расчета нагрузки сети

6.8.4.1 Для шины процесса определяется количество SV-потоков, GOOSE-сообщений и производится суммирование в соответствии с Таблицей 6.5 и Таблицей 6.6 для запроектированного количества сообщений/потоков в сегменте сети.

6.8.4.2 Нагрузка сети от GOOSE-, MMS-сообщений принимается равной 0,8 Мб/с для типового шкафа РЗА.

Указанное значение было определено экспериментальным путем на полигонах производителей / поставщиков АСУ ТП при построении сети в соответствии с данным стандартом.

6.8.4.3 Для шины управления и шины ДМЗ расчет загрузки сети не производится.

6.8.4.4 Для мультишины определяется количество SV-потоков, GOOSE-сообщений, количество типовых шкафов и производится суммирование нагрузок.

6.8.4.5 В соответствии с полученными значениями нагрузки сети определяется тип интерфейсов сетевых коммутаторов для подключения устройств полевого уровня и уровня присоединения: 100BASE или 1000BASE.

6.8.5 Коэффициент использования сети

Коэффициент использования сети равен отношению нагрузки на сеть к пропускной способности. Коэффициент использования сети рассчитывается по формуле:

$$\eta = \frac{V}{V_{max}}.$$

Несмотря на то, что скорость передачи данных в сети определенной технологии всегда одна и та же, производительность сети уменьшается с увеличением объема передаваемых данных. Во-первых, объем передаваемых данных (трафик) делится между всеми компьютерами сети. Во-вторых, даже та доля пропускной способности разделяемого сегмента, которая должна

приходиться на один узел, очень часто ему не достается из-за особенностей работы механизма доступа к общей среде передачи данных.

После определенного предела увеличение коэффициента использования сети приводит к резкому уменьшению реальной скорости передачи данных. Потери времени, связанные с работой механизма доступа к разделяемой среде, зависят от характера обращений компьютеров к сети и не могут быть точно рассчитаны, поэтому для обеспечения достаточной производительности задается предельное значение коэффициента использования сети, при котором сеть будет быстро реагировать на обращения пользователей.

С учетом современного развития промышленных коммутаторов для ПС ЕНЭС определен **в размере 0,75.**

6.8.6 Гарантированное время доставки сообщения/потока, включая прием-передачу, между сетевыми коммутаторами не должно превышать 0,025 мс (при максимальной длине сообщения/потока 1536 байт).

Задержки переключения пакетов по одному каналу (между входным и выходным портами) коммутатора при номинальной загрузке другого канала не должны превышать гарантированного времени доставки сообщений/потоков.

6.8.7 При проектировании ЛВС выбранные решения должны обеспечивать соответствие времени доставки сообщений/потоков требованиям требования стандарта ГОСТ Р МЭК 61850-5 и корпоративного профиля МЭК 61850 ПАО «ФСК ЕЭС».

6.9 Требования к условиям и организации эксплуатации ЛВС

6.9.1 Все помещения, в которых размещаются шкафы с оборудованием ЛВС, должны быть оборудованы системой контроля и обеспечения санкционированного доступа.

6.9.2 Шкафы с оборудованием ЛВС, устанавливаемые в отапливаемых помещениях, должны соответствовать климатическому исполнению УХЛ4 или О4 (Таблица 6.7).

Для контроля температуры и влажности воздуха в помещениях должны предусматриваться соответствующие датчики температуры и влажности, сигналы от которых должны вводиться в АСУ ТП.

Таблица 6.7 – Климатическое исполнение

Наименование показателя	**Значение**
1. Климатическое исполнение по ГОСТ 15150	УХЛ; О
2. Верхнее предельное рабочее значение температуры воздуха, °С - исполнение УХЛ4 - исполнение О4	 +40 +55
3. Нижнее предельное рабочее значение температуры воздуха, °С	+1

Наименование показателя	Значение
4. Верхнее значение относительной влажности: - исполнение УХЛ4 - исполнение О4	 80% при 25 °С 98% при 35 °С

6.9.3 Оперативное обслуживание оборудования ЛВС в составе АСУ ТП выполняется оперативным персоналом ПС. Он дает оценку качества выполнения функций с регистрацией всех замечаний в оперативном журнале и журнале дефектов и неполадок АСУ ТП.

При плановых обходах оперативный персонал контролирует:

– целостность и отсутствие внешних повреждений кабелей связи, доступных для осмотра;

– целостность и отсутствие внешних повреждений оборудования ЛВС, доступных для осмотра;

– отсутствие предупредительной сигнализации в шкафах сетевой коммутации;

– отсутствие предупредительной световой индикации на лицевой панели оборудования ЛВС;

– температуру окружающего воздуха, влажность, вибрацию и запыленность в местах установки приборов и аппаратуры;

– закрытое состояние дверей шкафов и сборок.

6.9.4 Техническое обслуживание предусматривает надзор за работой оборудования ЛВС, уход за оборудованием ЛВС, поддержание оборудования ЛВС в исправном состоянии, проведение плановых технических осмотров, технических регулировок, промывок, чисток, продувок и т.д.

Техническое обслуживание осуществляется в процессе работы системы и оборудования ПТК в соответствии с руководствами по эксплуатации оборудования ЛВС.

Техническое обслуживание выполняется персоналом АСУ ТП.

Типовые карты обслуживания шкафов сетевой коммутации (ШСК) приведены в Приложении В.

6.10 Требования к стандартизации и унификации ЛВС

6.10.1 Оборудование ЛВС устанавливается в шкафы сетевой коммутации (ШСК).

Состав типового ШСК:

– сервер времени и оборудование СОЕВ;

– сетевой экран подключения смежных подсистем;

– коммутаторы PRP сети А/сети Б;

– оптические кроссы для подключения устройств полевого уровня.

6.10.2 Для полноценного резервирования и удобства технического обслуживания, сетевое оборудование и коммутаторы сети А и Б следует устанавливать в разных ШСК.

6.10.3 Максимальное количество подключаемых устройств в ШСК – 120. Достигается установкой пяти 24-портовых коммутаторов с LC-коннекторами для подключения устройств. Дополнительно в коммутаторах должны быть порты связи для связей между коммутаторами и внутришкафных связей.

6.10.4 В качестве основной среды передачи информации применяется многомодовое оптическое волокно с разъемами типа LC (для устройств, подключаемых в сеть PRP А и Б: терминалы РЗ и СА, ПА, ПДС, КП, УСО, ЩСН, ЩПТ, РС ЦПС и т.д.).

6.10.5 Допускается применение экранированной медной витой пары 5 или 6 категории для подключения в сеть в пределах одного помещения (связи между серверными шкафами, подключение смежных подсистем в станционную шину не по протоколу PRP).

6.10.6 В шкафах серверного оборудования (ШСО) устанавливается по два коммутатора: к комплекту сетевых коммутаторов шины управления подключается оборудование ШСО (стационарные/переносные АРМ, ПДС диагностики, сервера АСУ ТП); к комплекту сетевых коммутаторов шины ДМЗ подключается оборудование ШСО и ШИБ (сервера ТМ, сервера удаленного доступа и сбора осциллограмм, сервер ИБ). В зависимости от архитектуры построения сети коммутаторы включаются в кольца коммутаторов PRP сети А и Б, либо образуют собственное RSTP кольцо.

6.10.7 В шкафы ШСО устанавливаются RedBox станционного уровня и коммутатор для RedBox без поддержки PRP (в случае использования RedBox для связи не PRP сети с сетями PRP А и Б).

6.10.8 Сетевое оборудование должно иметь два источника питания и встроенную систему диагностики, контролирующую состояние портов коммутатора/межсетевого экрана/RedBox, температуру, исправность блоков питания с выдачей информации в SCADA-систему при помощи протокола SNMPv3.

6.11 Требования к приемке ЛВС

6.11.1 Приемка ЛВС выполняется перед комплексной проверкой АСУ ТП в соответствии с [8].

6.11.2 При приёмо-сдаточных испытаниях ЛВС обязательно проводятся следующие проверки:

– корректная настройка межсетевых экранов: проводится путем сканирования специальными утилитами (например, nmap) IP-адресов и портов на соответствие рабочей документации;

– корректная настройка VLAN: проверяется отсутствие multicast трафика в непрописанных в рабочей документации портах коммутаторов;

– корректная настройка коммутаторов: блокировка неиспользуемых портов;

6.11.3 Если в процессе сканирования обнаружатся открытые порты и сервисы интеллектуальных устройств, необходимо провести проверку

необходимости данных сервисов для корректной работы ПТК АСУ ТП. При отсутствии такой потребности неиспользуемые сервисы должны быть отключены.

6.12 Требования к квалификации обслуживающего персонала

6.12.1 Оборудование ЛВС входит в состав АСУ ТП и обслуживается персоналом АСУ ТП.

6.12.2 Квалификация персонала АСУ ТП должна соответствовать требованиям профессионального стандарта «Работник по обслуживанию и ремонту оборудования автоматизированных систем управления технологическими процессами в электрических сетях».

6.12.3 Требуется знание основных технологий, применяемых при построении ЛВС АСУ ТП:

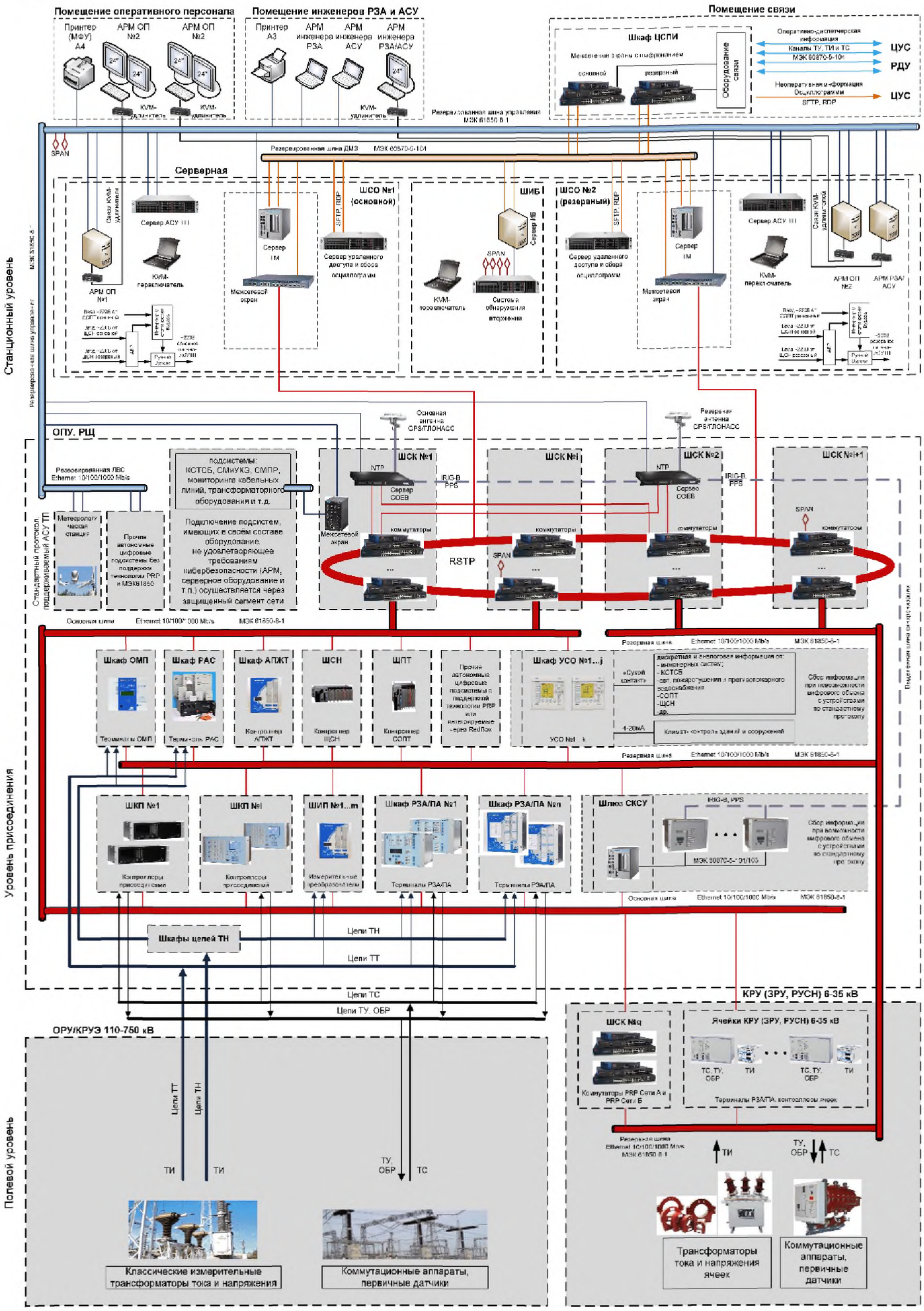
- знание принципов модели ISO OSI, используемых при построении сетей;
- знание стеков протоколов TCP/IP (version 4/version 6, unicast & multicast);
- знание протоколов и технологий уровня L2 (PPP, PPPoE, Ethernet коммутация, Spanning Tree);
- знание принципов и технологий доступа в Интернет, L3 VPN, VPLS, Multicast;
- знание основных принципов работы телематических сервисов (DNS, DHCP, NAT, FTP/HTTP и т.д.).

6.12.4 МЭС (ПМЭС) на плановой основе должен осуществлять непрерывное повышение квалификации персонала АСУ ТП путем проведения производственно-технической учебы и периодического обучения в соответствующих образовательных учреждениях.

6.12.5 Персонал АСУ ТП должен проходить краткосрочное и длительное обучение (не менее 72 часов), рекомендуемая периодичность обучения персонала АСУ ТП один раза в два года, но не реже чем один раз в 5 лет в соответствии с «Правилами работы с персоналом в организациях электроэнергетики Российской Федерации».

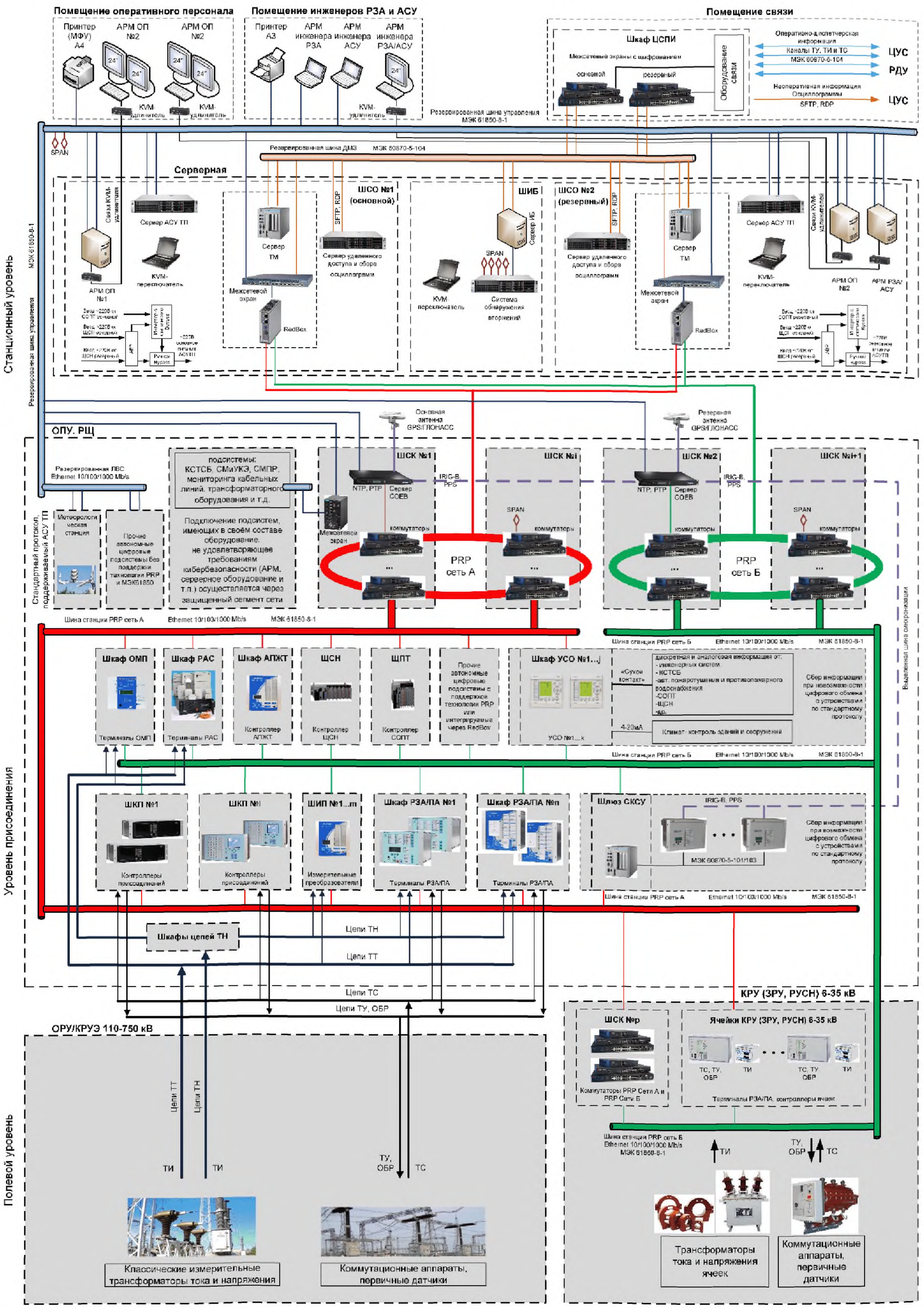
Персонал АСУ ТП должен проходить инструктажи и проверку знаний в соответствии с «Правилами работы с персоналом в организациях электроэнергетики Российской Федерации».

Приложение А
Типовые структуры построения сети и внутрисистемных коммуникаций для различных архитектур построения сетей АСУ ТП и РЗА



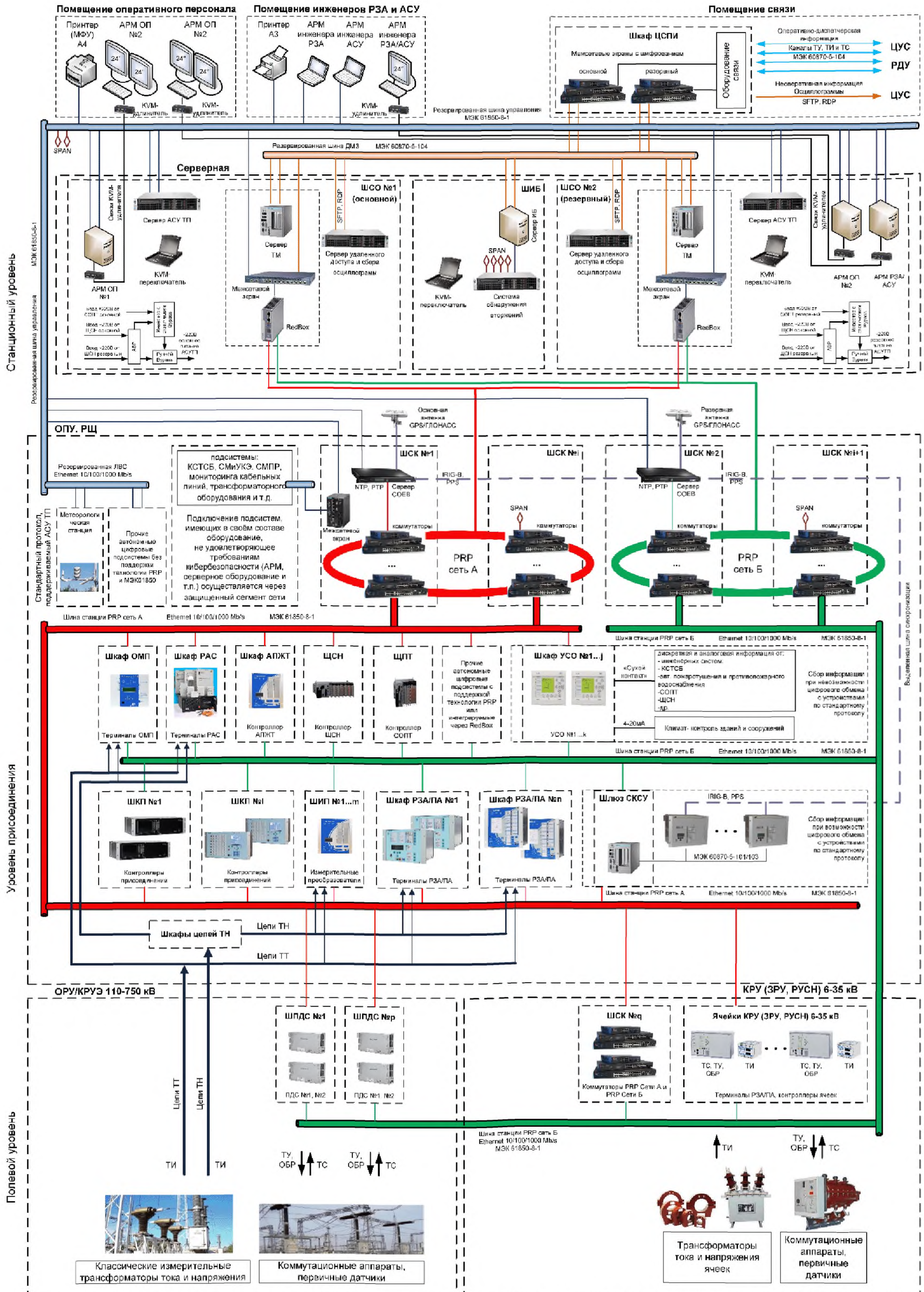
Структурная схема 1 – I архитектура (RSTP)

При реконструкции ПС подлежит модернизации только станционный уровень ПТК АСУ ТП.

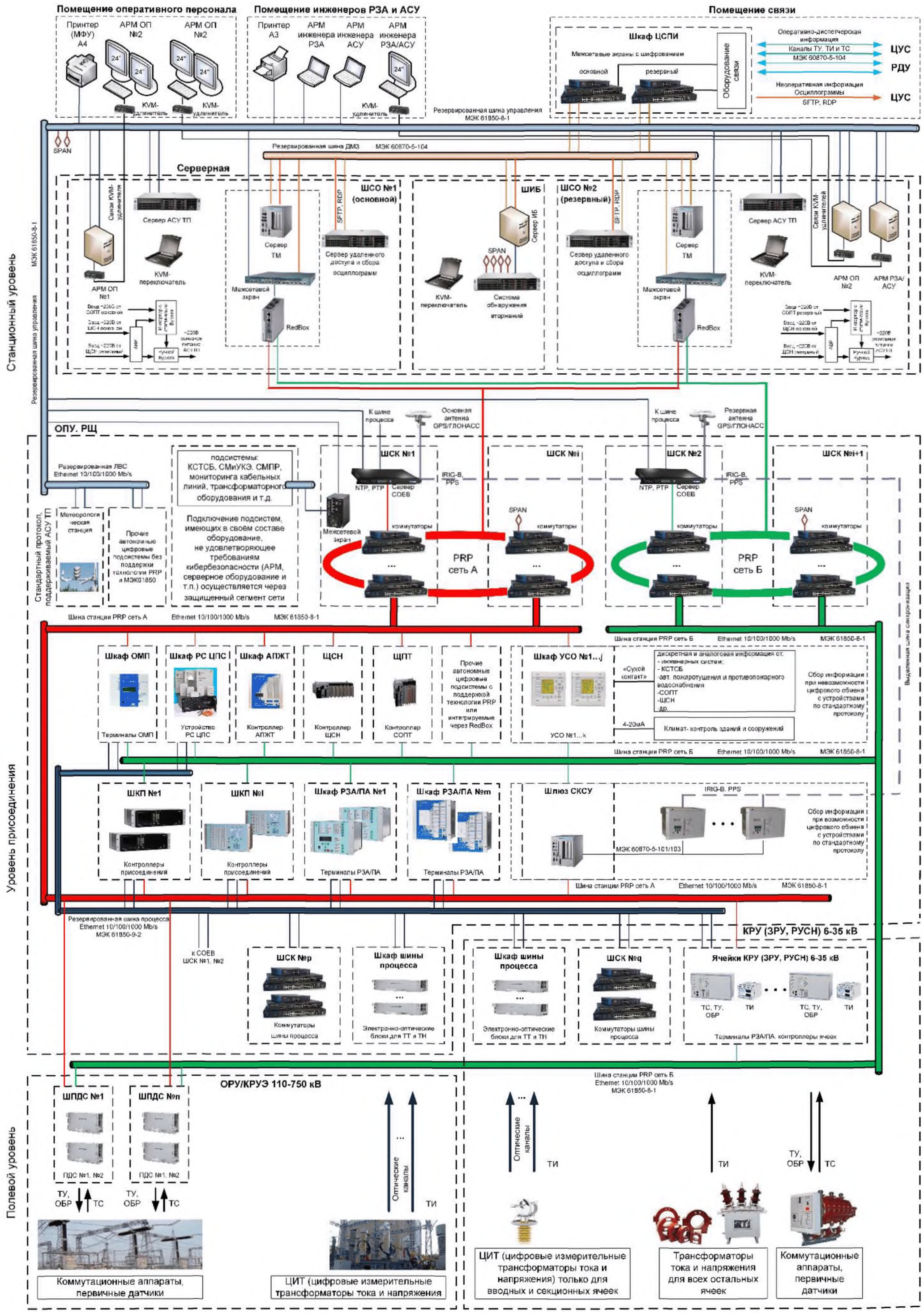


Структурная схема 2 – I архитектура (PRP)

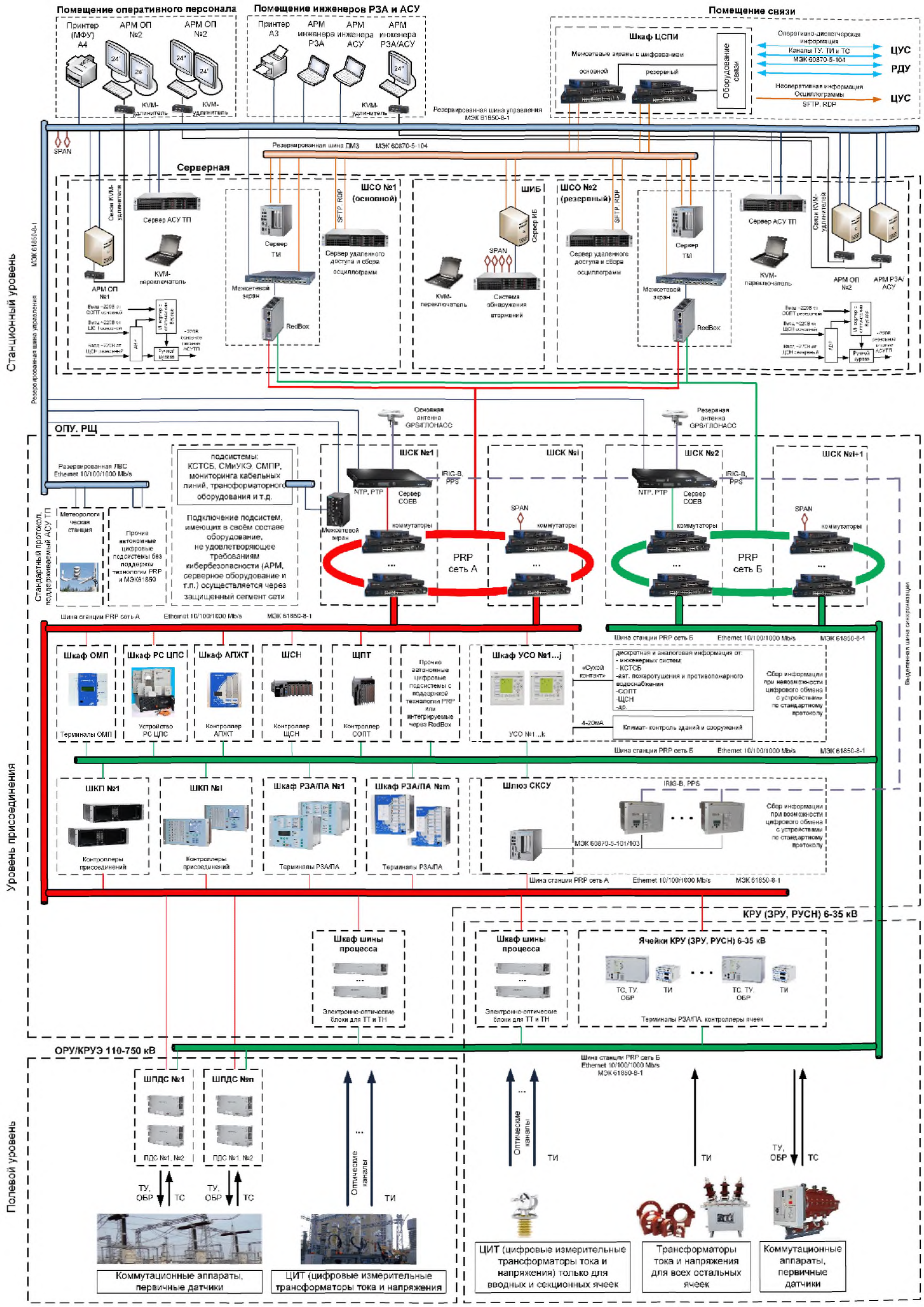
При реконструкции ПС подлежит модернизации только станционный уровень ПТК АСУ ТП.



Структурная схема 3 – II архитектура



Структурная схема 4 – III архитектура (отдельная шина процесса)



Структурная схема 5 – III архитектура (мультишина)

Приложение Б
Методика расчета количества оборудования ЛВС и ШСК

Однолинейная схема ПС, для которой приведен пример расчета оборудования ЛВС и ШСК, приведена в данном приложении.

На однолинейной схеме отмечены выбранные типовые шкафы РЗА, УПАСК, ШПДС, ШПАС (рисунки Б.1-Б.3).

Ниже приведен расчет количества оборудования ЛВС АСУ ТП для архитектуры III типа:

- с отдельной шиной процесса;
- с мультишиной.

Вариант 1 – с отдельной шиной процесса.

1. В таблице Б.1 указано количество оборудования ЛВС для АСУ ТП с отдельной шиной процесса.

Таблица Б.1 – Расчет оборудования ЛВС для АСУ ТП с отдельной шиной процесса

<table>
<tr><td rowspan="3">п. 3.1 Количество устройств, подключаемых</td><td colspan="2">к шине управления</td><td>к шине ДМЗ</td></tr>
<tr><td>резервированное подключение</td><td>нерезервированное подключение</td><td>резервированное подключение</td></tr>
<tr><td>АРМ – 3
Сервер – 2
ПДС ШСО – 1
Сервер СОВ – 1</td><td>АРМ – 2
Принтер – 2
Межсетевой экран - 2</td><td>Сервер ТМ – 2
Сервер удаленного доступа – 2
Сервер ИБ – 1
Сервер СОВ – 1
Межсетевой экран – 2 (нерезервированный)</td></tr>
<tr><td></td><td colspan="2">Итого: 10</td><td>Итого: 7</td></tr>
<tr><td>с учетом резерва</td><td colspan="2">12</td><td>8</td></tr>
<tr><td>п. 3.2 Количество коммутаторов шины управления и шины ДМЗ
- основной
- резервный</td><td colspan="2">

1
1</td><td>

1
1</td></tr>
<tr><td>п. 3.3 Место установки коммутаторов шины управления и шины ДМЗ</td><td colspan="3">основные коммутаторы шины управления и шины ДМЗ – в ШСО № 1;
резервный коммутаторы шины управления и шины ДМЗ – в ШСО № 2</td></tr>
<tr><td>п. 3.4 Количество устройств смежных подсистем, подключаемых через МЭ</td><td colspan="3">0</td></tr>
</table>

п. 3.5 Количество устройств, подключаемых к шине станции	500 кВ УПАСК - 2 РЗА – 18 КП – 2 ПДС – 26 Итого: 48	220 кВ УПАСК – 7 РЗА – 11 КП – 2 ПДС – 30 ПАС – 4 Итого: 54	10 кВ РЗА – 15 ИП – 13 Итого: 28
с учетом резерва	55	62	33
п. 3.6 Количество коммутаторов шины станции - PRP сети А - PRP сети Б	 3 3	 3 3	 2 2
п. 3.7 Количество ШСК шины станции - PRP сети А - PRP сети Б	 1 (3 коммутатора) 1 (3 коммутатора)	 1 (3 коммутатора) 1 (3 коммутатора)	 1 (2 коммутатора) 1 (2 коммутатора)
п. 3.8 Количество портов в оптическом кроссе	26*4 = 104	34*4 = 136	
п. 3.9 Количество 16-портовых кассет оптического кросса	7	9	
п. 4.1 Количество устройств, подключаемых к шине процесса	ЭОБ - 14 РЗА – 18 КП – 2 Итого: 34	ЭОБ – 11 РЗА – 11 КП – 2 ПАС – 4 Итого: 28	-
с учетом резерва	39	32	
п. 4.2 Количество коммутаторов шины процесса - PRP сети А - PRP сети Б	 2 2	 2 2	-
п. 4.3 Количество ШСК шины процесса - PRP сети А - PRP сети Б	 1 (4 коммутатора) 1 (4 коммутатора)		-
п. 4.4 Количество портов в оптическом кроссе	4*4 = 16		
п. 4.5 Количество 16-портовых кассет оптического кросса	1		

В итоге, для рассматриваемой ПС для архитектуры III типа **с отдельной шиной процесса** необходимо установить **8 ШСК (24 коммутатора)**:

– 2 ШСК по три коммутатора и 7 кассет оптического кросса для подключения устройств присоединений ОРУ 500 кВ к шине станции;

– 2 ШСК по три коммутатора и 9 кассет оптического кросса для подключения устройств присоединений ОРУ 220 кВ к шине станции;

– 2 ШСК по два коммутатора для подключения устройств присоединений 10 кВ к шине станции;

– 2 ШСК по четыре коммутатора и 1 кассете оптического кросса для подключения устройств присоединений ОРУ 500 кВ, ОРУ 220 кВ к шине процесса.

А также 2 коммутатора шины управления и 2 коммутатора шины ДМЗ в ШСО № 1 и ШСО № 2.

Вариант 2 – с мультишиной.

2. В таблице Б.2 приведен расчет оборудования ЛВС для АСУ ТП с мультишиной.

Таблица Б.2 – Расчет оборудования ЛВС для АСУ ТП с мультишиной

п. 3.1 Количество устройств, подключаемых	к шине управления		к шине ДМЗ
	резервированное подключение	нерезервированное подключение	резервированное подключение
	АРМ – 3 Сервер – 2 ПДС ШСО – 1 Сервер СОВ – 1	АРМ – 2 Принтер – 2 Межсетевой экран - 2	Сервер ТМ – 2 Сервер удаленного доступа – 2 Сервер ИБ – 1 Сервер СОВ – 1 Межсетевой экран – 2 (нерезервированный)
	Итого: 10		Итого: 7
с учетом резерва	12		8
п. 3.2 Количество коммутаторов шины управления и шины ДМЗ - основной - резервный	 1 1		 1 1
п. 3.3 Место установки коммутаторов шины управления и шины ДМЗ	основные коммутаторы шины управления и шины ДМЗ – в ШСО № 1; резервный коммутаторы шины управления и шины ДМЗ – в ШСО № 2		
п. 3.4 Количество устройств смежных подсистем, подключаемых через МЭ	0		
п. 3.5 Количество устройств, подключаемых к мультишине	500 кВ	220 кВ	10 кВ
	УПАСК - 2 РЗА – 18 КП – 2 ПДС – 26 ЭОБ - 14 Итого: 62	УПАСК – 7 РЗА – 11 КП – 2 ПДС – 30 ПАС – 4 ЭОБ - 11 Итого: 65	РЗА – 15 ИП – 13 Итого: 28
с учетом резерва	71	72	33
п. 3.6 Количество коммутаторов мультишины - PRP сети А - PRP сети Б	 3 3	 3 3	 2 2
п. 3.7 Количество ШСК мультишины - PRP сети А - PRP сети Б	 1 (3 коммутатора) 1 (3 коммутатора)	 1 (3 коммутатора) 1 (3 коммутатора)	 1 (2 коммутатора) 1 (2 коммутатора)

п. 3.8 Количество портов в оптическом кроссе	26*4 = 104	34*4 = 136	-
п. 3.9 Количество 16-портовых кассет оптического кросса	7	9	-

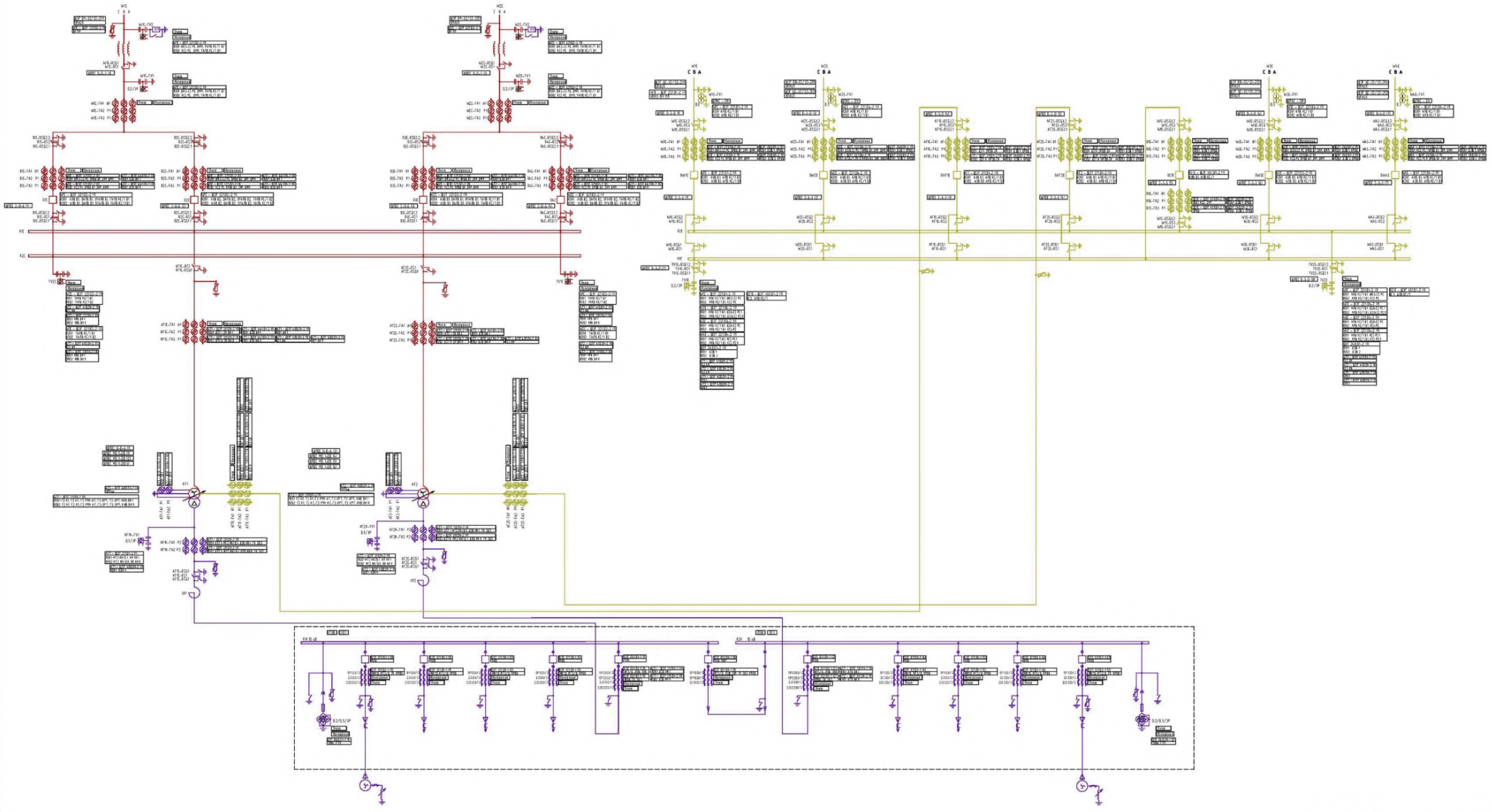
В итоге, для рассматриваемой ПС для архитектуры III типа **с мультишиной** необходимо установить **6 ШСК (16 коммутаторов)**:

– 2 ШСК по три коммутатора и 7 кассет оптического кросса для подключения устройств присоединений ОРУ 500 кВ к мультишине;

– 2 ШСК по три коммутатора и 9 кассет оптического кросса для подключения устройств присоединений ОРУ 220 кВ к мультишине;

– 2 ШСК по два коммутатора для подключения устройств присоединений 10 кВ к мультишине.

А также 2 коммутатора шины управления и 2 коммутатора шины ДМЗ в ШСО № 1 и ШСО № 2.



						ПС 500 кВ "Архипобская" и Архипектура
						Сервисная ПС 500 кВ "Архипобская" и Архипектура
Изм.	Кол.уч.	Лист	N Изм.	Подпись	Дата	
						Сервисная ПС 500 кВ "Архипобская" и Архипектура
Разработал					12.04.18	
Проверил					12.04.18	
Нач. отдела					12.04.18	
Н. контроль					12.04.18	

Стадия	Лист	Листов
8		

Схема расширения решений наблюдения мониторинга сигнала на ТТ и ТН Изм ПС 500 кВ "Архипобская"

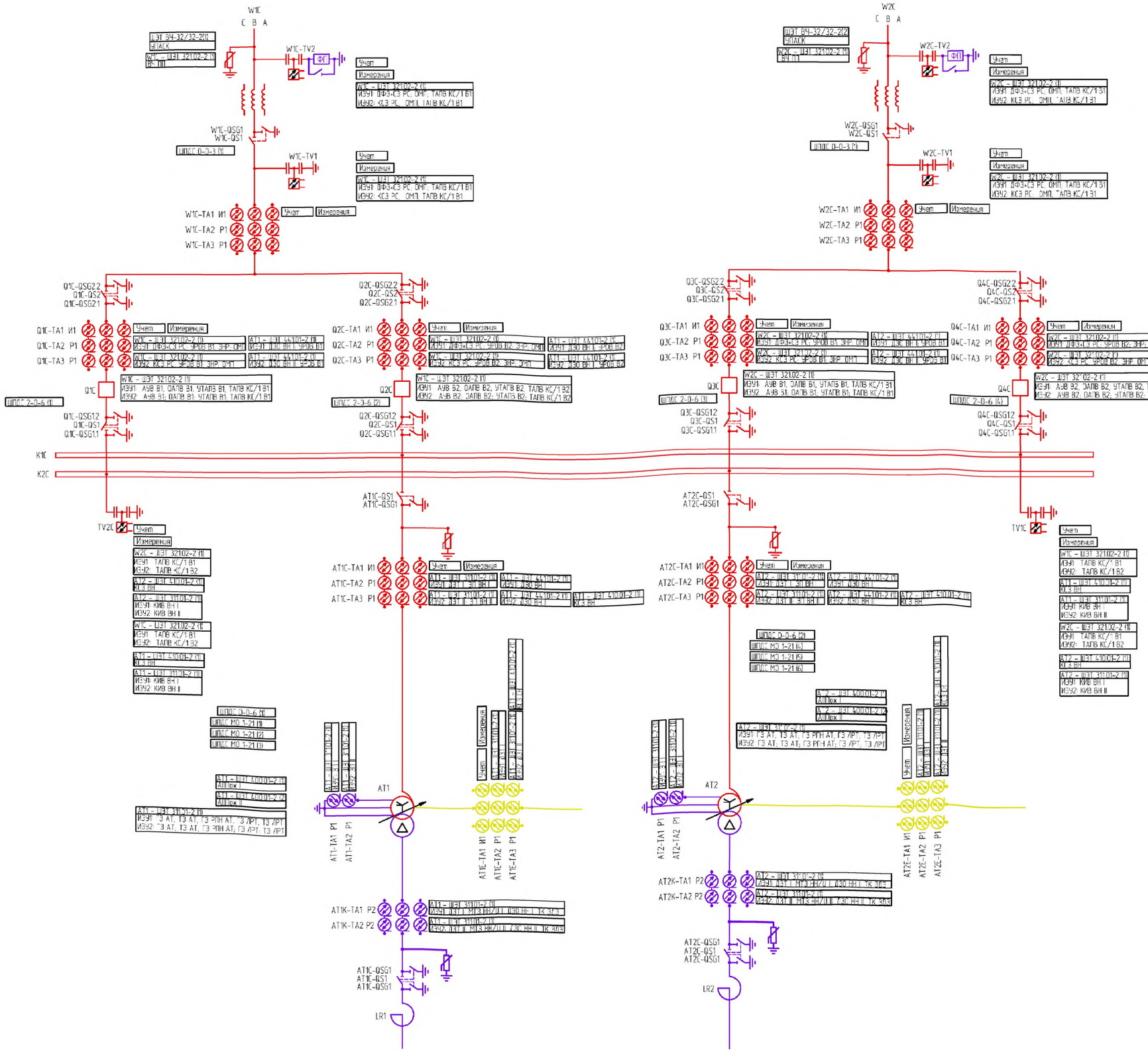


Рисунок Б.1 – Однолинейная схема ПС с указанием типовых шкафов. Фрагмент 1 (ОРУ 500 кВ)

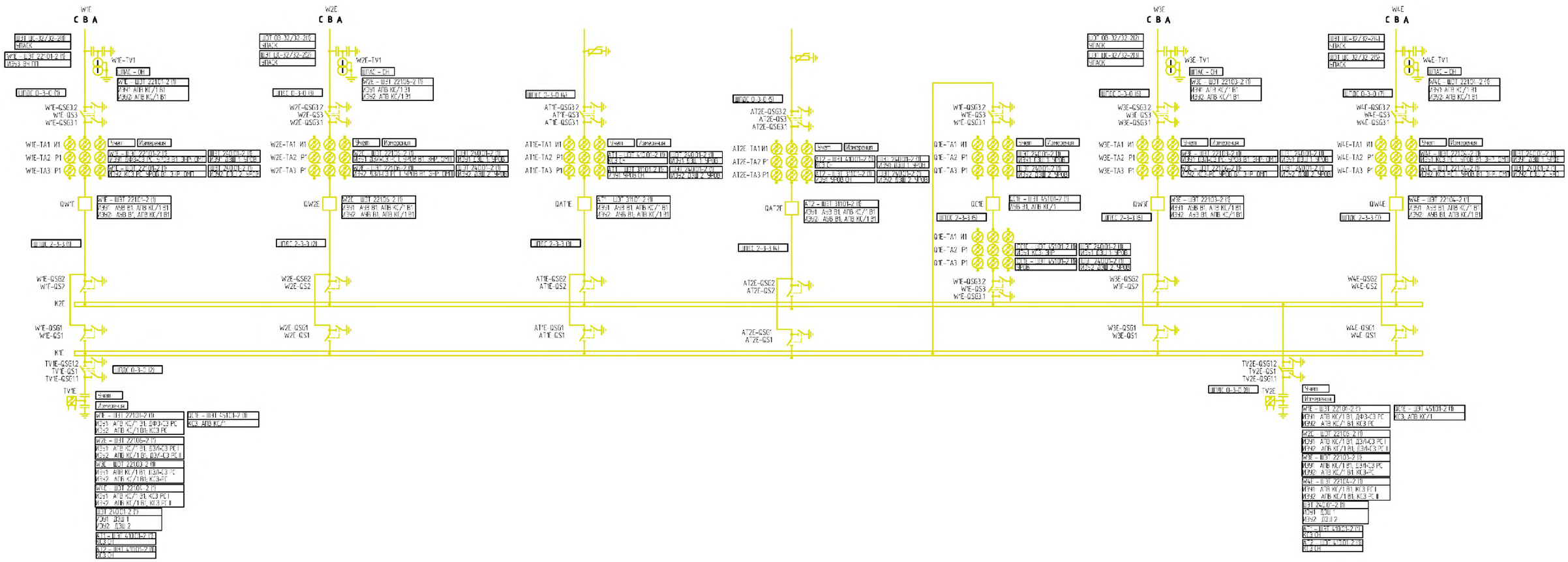


Рисунок Б.2 – Однолинейная схема ПС с указанием типовых шкафов. Фрагмент 2 (ОРУ 220 кВ)

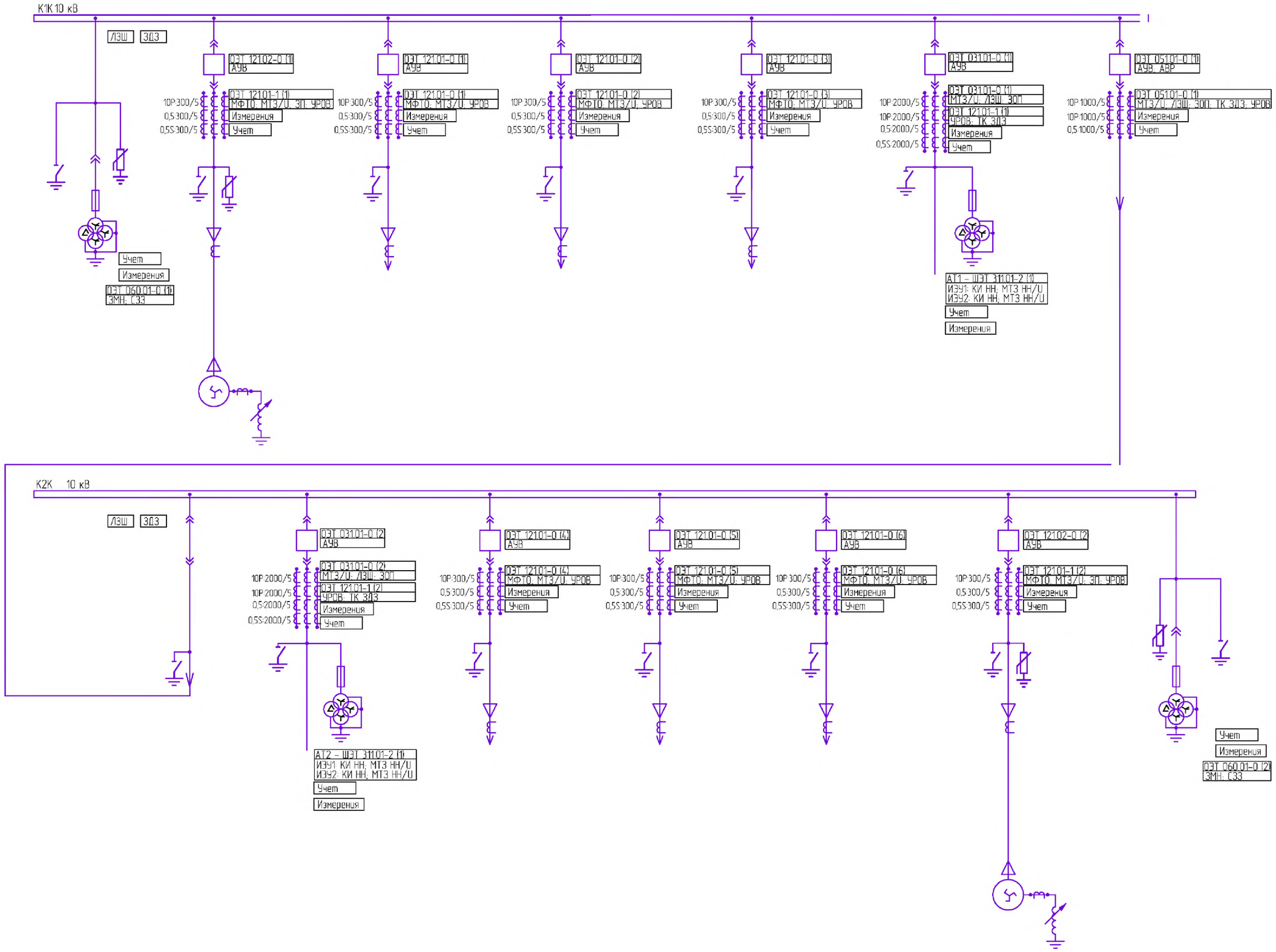


Рисунок Б.3 – Однолинейная схема ПС с указанием типовых шкафов. Фрагмент 3 (КРУ 10 кВ)

Приложение В
Типовые карты обслуживания шкафов сетевой коммутации (ШСК)

№ п/п	Наименование работ	Количество нормо-часов (чел/час)	Периодичность (раз/год)	Всего часов в год	Примечание
1	Очистка от пыли внутренней части шкафа (с использованием спец. промышленного пылесоса)	1	2	2	Производится без отключения оборудования шкафа
2	Диагностика состояния аппаратных средств сетевого оборудования, температурного режима работы	0,5*	4	2	Производится без отключения оборудования шкафа
3	Регулярный (обзорный, а при имевших место возмущениях в сети с работой или без работы систем РЗА, ПА, первичного оборудования и появлении сообщений о сетевых ошибках - детальный) анализ системных журналов и журналов событий операционной системы и базового программного обеспечения	0,5*	4	2	Производится без отключения оборудования шкафа
	Проверка работоспособности компонентов шкафа визуальным осмотром индикации	0,1	2	0,2	Производится без отключения оборудования шкафа
5	Проверка функционирования резервной сети	1	4	4	В соответствии с инструкцией по эксплуатации на ПТК

Примечание.
* Норма времени приведена в расчете на одно устройство.

Библиография

1. СТО 34.01-6-005-2019 Коммутаторы энергообъектов. Общие технические требования, ПАО «Россети».

2. СТО 56947007-29.240.10.256-2018 Технические требования к аппаратно-программным средствам и электротехническому оборудованию ЦПС, ПАО «ФСК ЕЭС».

3. МЭК 62439-3(2016) Промышленные сети связи. Сети с высокой готовностью к автоматической обработке. Часть 3. Протокол параллельного резервирования (PRP) и бесшовное резервирование среды высокой готовности (HSR) (IEC 62439-3(2016) Industrial communication networks - High availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR).

4. МЭК 61850-8-1 (2011) Сети связи и системы автоматизации энергосистем общего пользования. Часть 8-1. Схема распределения особой услуги связи (SCSM). Схема распределения для производственной системы модульной конструкции MMS (ISO 9506-1 и ISO 9506-2) и по ISO/IEC 8802-3 (IEC 61850-8-1 (2011) Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3).

5. IEEE 802.1D-2004 Стандарт Института инженеров по электротехнике и электронике (IEEE). Стандарт для локальных и городских сетей: мосты управления доступом к средствам массовой информации (MAC) (IEEE 802.1D-2004 Standard of the Institute of Electrical and Electronics Engineers (IEEE). IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges).

6. МЭК 62439-2(2016) Промышленные сети связи. Сети с высокой готовностью к автоматической обработке. Часть 2. Протокол резервирования среды передачи (MRP) (IEC 62439-2(2016) Industrial communication networks - High availability automation networks - Part 2: Media Redundancy Protocol (MRP).

7. СТО 56947007-29.240.044-2010 Методические указания по обеспечению электромагнитной совместимости на объектах электросетевого хозяйства, ПАО «ФСК ЕЭС».

8. СТО 56947007-25.040.40.012-2008 Типовая программа комплексных испытаний АСУ ТП при приемке из реконструкции и законченных строительством подстанций ПАО «ФСК ЕЭС» (с Изменениями от 26.07.2018), ПАО «ФСК ЕЭС».

9. МЭК 61850-9-2(2011) Системы автоматизации и сети связи на подстанциях. Часть 9-2. Схема особого коммуникационного сервиса (SCSM). Значения выборок по ISO/IEC 8802-3 (IEC 61850-9-2 (2011) Communication networks and systems for power utility automation - Part 9-2: Specific communication service mapping (SCSM) - Sampled values over ISO/IEC 8802-3).

10. МЭК 61850-5(2013) Коммуникационные сети и системы для автоматизации электростанций общего пользования. Часть 5. Коммуникационные требования для выполнения функций и к моделям приборов (IEC 61850-5(2013) Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models).

11. IEEE 802.1Q-2014 Стандарт Института инженеров по электротехнике и электронике (IEEE). Стандарт для локальных и городских сетей - Локальные и городские вычислительные сети. Межсегментные каналы связи и мостовые сети. (IEEE 802.1Q-2014 Standard of the Institute of Electrical and Electronics Engineers (IEEE). IEEE Standard for Local and metropolitan area networks - Bridges and Bridged Networks).

12. IEEE 802.3-2015 Стандарт Института инженеров по электротехнике и электронике (IEEE). Стандарт для информационных сетей (IEEE 802.3-2015 Standard of the Institute of Electrical and Electronics Engineers (IEEE). IEEE Standard for Ethernet).

13. МЭК 60870-5-101(2015) Аппаратура и системы телеуправления. Часть 5-101. Протоколы передачи данных. Сопроводительный стандарт для основных задач телеуправления (IEC 60870-5-101(2015) Telecontrol equipment and systems - Part 5-101: Transmission protocols - Companion standard for basic telecontrol tasks).

14. МЭК 60870-5-104(2016) Аппаратура и системы телеуправления. Часть 5-104. Протоколы передачи данных. Доступ к сетям, использующим стандартные профили по МЭК 60870-5-101 (IEC 60870-5-104(2016) Telecontrol equipment and systems - Part 5-104: Transmission protocols - Network access for IEC 60870-5-101 using standard transport profiles).

15. МЭК 61869-9(2016) Трансформаторы измерительные. Часть 9.

Цифровой интерфейс для измерительных трансформаторов (IEC 61869-9(2016) Instrument transformers - Part 9: Digital interface for instrument transformers).

16. СТО 56947007-29.240.10.299-2020 Цифровая подстанция. Методические указания по проектированию ЦПС, ПАО «ФСК ЕЭС».

17. Приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (с изменениями от 09.08.2018).

18. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (с изменениями от 26.03.2019) (редакция, действующая с 01.01.2020).

gost.e-ecolog.ru