
# Архитектура и управление в цифровой энергетике

Курск 2019

# 5. АРХИТЕКТУРА ЦИФРОВОЙ ПОДСТАНЦИИ

В пятой главе рассмотрена архитектура цифровой подстанции на основе: инфраструктуры передачи информации; программного, информационного и метрологического обеспечения; надежности, информационной и комплексной безопасности.

## 5.1. ИНФРАСТРУКТУРА ПЕРЕДАЧИ ИНФОРМАЦИИ

Рассмотрим требования к средствам коммуникации – инфраструктуре передачи информации (ИПИ) как неотъемлемому архитектурному элементу ЦПС. ИПИ является кибернетическим архитектурным элементом ЦСП (рис. 5.1) [2].

В отличие от инфраструктуры передачи мощности (ИПМ), представляющей собой исполнительный архитектурный элемент ЦПС, основное назначение ИПИ заключено в том, чтобы создать условия для эффективного управления ИПМ, в рамках чего обеспечить информационный обмен между техническими средствами в пределах и за пределами ЦПС. Необходимо также специально отметить, что непосредственно само управление ИПМ не является функцией ИПИ.

Физическая структура ИПИ включает различные компоненты: структурированные кабельные системы (передачи данных и инструментальной синхронизации); активное оборудование – коммутационный пул (коммутаторы и кросс-панели) и коммуникационные окончания (порты) технических средств, подключаемых к ИПИ; синхронизационный пул и синхронизационные окончания (порты) соответствующих технических средств; различные вспомогательные подсистемы (бесперебойного питания, мониторинга) и механические конструкции (стойки, шкафы, лотки, кабельные каналы и пр.).

Наряду с физической, существует и логическая структура ИПИ, пользоваться которой для описания информационных процессов, имеющих место быть в ЦПС, гораздо удобнее и включает в себя (рис. 5.1):

а) терминальные элементы: передатчики и приемники данных;

б) сетевые элементы:

- станционная шина,
- технологическая шина,
- инструментальная синхронизационная шина,
- прочие шины, такие как сетевая сервисная, диагностическая и др.;

в) шинообразуюшие элементы:

- мост.

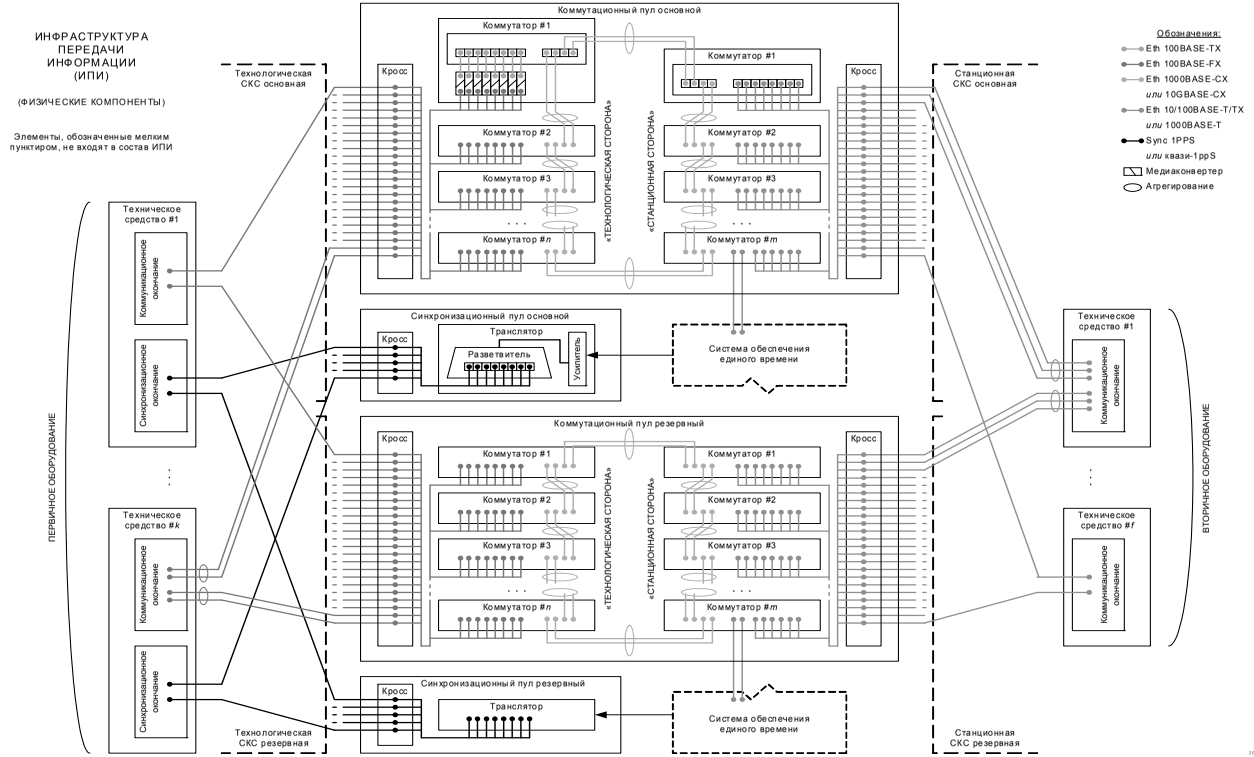


**Рис. 5.1. Физическая организация ИПИ ЦПС и ее структурные компоненты**

5.1. Станционная шина. Рассмотрим требования к станционной шине, как к элементу логической структуры ИПИ ЦПС.

5.1.1. Коммуникационный профиль. В станционной шине должны присутствовать сообщения, генерируемые протоколами, составляющими коммуникационный (прикладной и транспортный) профиль MMS поверх TCP/IP, IEC 61850-8.1.

Рекомендуется дополнить указанный профиль обязательной инкапсуляцией в сообщения с меткой виртуальной сети по IEEE 802.1Q.

Присутствие в станционной шине сообщений прочих протоколов, не входящих в указанный профиль, недопустимо.

5.1.2. Обмен сообщениями. Допускается организовать коммуникацию сообщений в станционной шине на основе динамических, статических и (или) смешанных правил фильтрации IEEE 802.1Q. Допускается организовать присвоение конечным техническим средствам сетевых адресов статически, т.е. предварительно, и (или) динамически, используя протокол DHCP, RFC 2131.

Рекомендуется проектировать серверную модель коммуникационного профиля MMS, чтобы она обеспечивала неблокирующее обслуживание не менее трех клиентов одновременно. Прочие способы организации коммуникации станционных сообщений следует исключать.

5.1.3. Топология. Станционная шина должна быть организована таким образом, чтобы коммуникационный профиль MMS, отвечающих за управление публикацией конечным техническим средством технологических сообщений, был доступен по тому же (физическому) соединению, по которому осуществляется публикация таких технологических сообщений.

Рекомендуется использовать для обмена станционными сообщениями одну единую (односегментную) виртуальную сеть, т.е. не сегментировать станционную шину.

Рекомендуется отделять через промежуточные маршрутизаторы участки коммуникационной сети, в которых присутствуют как станционные, так и технологические сообщения, от участков, в которых технологические сообщения полностью исключены.

В связи с тем, что станционная шина представляет собой типовую локальную TCP/IP-сеть, поведение которой хорошо изучено, прочие специфические требования к организации станционной шины не предъявляются.

5.1.4. Технологическая шина. В настоящем подразделе рассмотрим требования к технологической шине как к элементу логической структуры ИПИ ЦПС.

5.1.5. Коммуникационный профиль. В технологической шине должны присутствовать сообщения исключительно следующих типов:

– GOOSE, IEC 61850-8.1;
– SV, IEC 61850-9.2.

Каждый шаблон сообщений GOOSE должен иметь имя-идентификатор, уникальное в пределах подстанции.

Примечание: имя-идентификатор GOOSE = goID по IEC 61850-8.1.

Каждый поток сообщений SV должен иметь имя-идентификатор, уникальное в пределах подстанции.

Примечание: имя-идентификатор SV = svID по IEC 61850-9.2. Присутствие в технологической шине сообщений прочих типов, отличных от указанных выше, недопустимо.

5.1.6. Публикация сообщений и подписка на них. Рекомендуется организовать коммутацию сообщений в технологической шине на основе статических правил фильтрации IEEE 802.1Q.

Примечание: такие правила закладываются в каждый коммутатор, задействованный в коммутации технологических сообщений, при статическом подходе исключена необходимость организации множественных виртуальных сегментов – сетей – внутри коммуникационного пространства, кроме того, максимально возможно детерминировано поведение самой сети.

При статической коммутации публикуемые сообщения должны иметь индивидуальный адрес получателя, уникальный в пределах сети, выбранный из диапазона индивидуальных адресов IANA. Подписка на сообщения в этом случае, выполняется предварительно на уровне коммутатора.

Примечание: диапазон 00-00-5E-xx-xx-xx.

Допускается организовать коммутацию сообщений в технологической шине на основе динамических правил фильтрации IEEE 802.1Q.

Примечание: подобные правила формируются самим коммутатором во время работы, при динамическом подходе существует необходимость организации множественных виртуальных сегментов, кроме того, поведение сети становится менее предсказуемым.

При динамической коммутации для публикации сообщений и подписки на них конечные технические средства и коммутаторы должны исполнять протокол GMRP, IEEE 802.1Q, сообщения при этом должны иметь групповой адрес получателя, уникальный в пределах сети, выбранный из диапазона групповых адресов IANA [2].

Примечание: диапазон 01-00-5E-xx-xx-xx.

Прочие способы организации коммутации технологических сообщений рекомендуется исключать.

5.1.7. Топология. Рекомендуется организовать сегменты (при динамическом подходе) и (или) псевдосегменты (при статическом под-

ходе) технологической шины таким образом, чтобы минимизировать количество промежуточных коммутаторов между конечными техническими средствами, включенными в сегмент. Именно поэтому следует применять многопортовые стекируемые коммутаторы с преобразованием, при необходимости, электрических соединений в оптические посредством медиаконвертеров.

5.1.8. Подсистема мониторинга состояния коммуникационной сети ЦПС и механизм мониторинга. Рассмотрим требования к подсистеме мониторинга коммуникационной сети ЦПС. Коммутаторы и конечные технические средства должны выполнять мониторинг состояния соединений, подключенных к портам в их коммуникационных окончаниях, а также аспектов своего собственного состояния, влияющих на корректную работу их самих и (или) работу коммуникационной сети.

Коммутаторы и конечные технические средства, выполняя непрерывный мониторинг своего состояния и состояния своих соединений, должны также хранить и посылать информацию о нем на спорадической, периодической и (или) запросной основе.

5.1.9. Средства мониторинга. Хранение и предоставление на запросной основе информации о состоянии, как результате мониторинга, рекомендуется организовать как информационный объект SMNP MIB, RFC 3418 и доступ к нему.

Посылки информации на спорадической и (или) периодической основе рекомендуется организовать как сообщения SNMP Trap, RFC 1251.

5.1.10. Пропускная способность и гарантированное время доставки сообщений в коммуникационной сети ЦПС. В настоящем подразделе рассмотрим требования к пропускной способности и гарантированному времени доставки сообщений по ИПИ ЦПС.

5.1.11. Соединения с конечными техническими средствами. Конечные технические средства должны соединяться с коммутатором по методу «точка–точка» без каких-либо промежуточных «вставок», исключая медиаконвертеры, наличие которых в соединении допустимо.

Единичное соединение, связывающее техническое средство с коммутатором, должно обеспечивать пропускную способность не менее 100 Мбит/с.

Примечание: протокол 100BASE-X или 1000BASE-T, IEEE 802.3.

При необходимости увеличения пропускной способности техническое средство может быть связано с коммутатором при помощи нескольких единичных соединений, агрегированных по протоколу LACP, IEEE 802.3.

Гарантированное время доставки сообщения, включая прием-передачу, между коммутатором и подключенным к нему конечным

техническим средством не должно превышать 0,25 мс, максимальная длина сообщения 1536 байт.

Рекомендуется для связи с первичным оборудованием, а также оборудованием, находящимся на территории ОРУ, применять волоконно-оптические соединения, для связи с интеллектуальными устройствами – электрические.

5.1.12. Соединения между коммутаторами. Коммутаторы, организующие коммуникационную сеть, должны быть соединены в «кольцо», соединения в котором могут быть агрегированными.

Управление «кольцом» должно отслеживать «изменения», исключать «петли» и исполняться динамически по протоколу RSTP, IEEE 802.1D.

Соединения между коммутаторами должны обеспечить пропускную способность не менее 1 Гбит/с, а при необходимости 10 Гбит/с.

Примечание: протоколы 1000BASE-X и 10GBASE-X, IEEE 802.3.

Гарантированное время доставки сообщения, включая прием-передачу, между коммутаторами не должно превышать 0,025 мс.

Примечание: максимальная длина сообщения 1536 байт.

Рекомендуется установить коммутаторы в едином месте (стойке), отдавая предпочтение как можно более коротким (физическим) связям между коммутаторами против увеличения (физической) протяженности соединений с конечными техническими средствами.

5.1.13. Резервирование коммуникационной среды. Коммуникационная среда ИПИ ЦПС должна резервироваться путем полного физического дублирования, при этом основной и резервный комплекты компонент ИПИ не должны взаимодействовать между собой.

Конечные технические средства должны иметь удвоенное количество портов в своих коммуникационных окончаниях, первой половиной из которых они подключаются к соединениям основной, а второй – резервной коммуникационной среды.

Для корректного оперирования в дублированном окружении конечные технические средства должны исполнять протокол RPR, IEC 62439, в то время как коммутаторы не нуждаются в каких-либо дополнительных протоколах.

## 5.2. ПРОГРАММНОЕ, ИНФОРМАЦИОННОЕ И МЕТРОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

5.2.1. Общее и технологическое программное обеспечение. Для решения функциональных задач АСУ ТП ПС на всех уровнях системы должна быть реализована совокупность взаимосвязанных по информа-

ции и по дисциплине выполнения программных средств, образующих программное обеспечение АСУ ТП ПС, которое условно можно представить в виде двух основных составляющих:

– общего (системного) программного обеспечения (ОПО);

– технологического (или специального) программного обеспечения (ТПО).

ОПО предназначено для организации функционирования ПТК АСУ ТП в целом и является фундаментом для успешной реализации всех целевых функций системы. В общем случае ОПО должно включать средства организации внутрисистемных и внесистемных коммуникаций, а также операционные системы реального времени (функционирующие в контроллерах нижнего уровня и в вычислительных устройствах верхнего уровня), под управлением которых должны выполняться программные средства ТПО.

ТПО представляет собой совокупность отдельных программных компонентов (модулей или их комплексов), резидентных в устройствах разных уровней ПТК и реализующих алгоритмы решения специфических для АСУ ТП ПС задач обработки информации, контроля, анализа, диагностики и управления.

Характерной особенностью ПО АСУ ТП ПС должна быть ориентация на использование современной компьютерной технологии создания систем управления, базирующейся на следующих основных принципах:

– полнота ПО, т.е. его практическая достаточность для решения основных функциональных задач сбора и обработки информации, оперативных расчетов, контроля, анализа, диагностики и управления основным и вспомогательным оборудованием в нормальных и аварийных режимах работы электротехнического оборудования;

– типовой характер ПО, заключающийся в том, что для всех видов автоматизируемого электротехнического оборудования (систем шин, выключателей, разъединителей и т.д.) реализуемые алгоритмы применимы для всех существующих на ПС их типов и конструкций, а также схем соединений;

– высокая степень готовности всех элементов ПО к использованию при разработке АСУ ТП для данной ПС, заключающаяся в том, что привязка к объекту не требует «допрограммирования» и осуществляется только путем параметрической настройки и конфигурирования элементов ПО;

– функциональная открытость и гибкость структуры (возможность добавления и исключения программных средств без структурных конфликтов);

– наличие развитой системы средств человеко-машинного обмена информацией (MMI), обеспечивающей эффективность работы персонала подстанции;

– автоматизация процессов проектирования и внедрения АСУ ТП ПС за счет использования комплекса инструментальных программных средств (ИПС) для поддержки процедур создания программного и информационного обеспечения.

Эффективность создания, внедрения и эксплуатации ПО и тесно связанного с ним информационного обеспечения АСУ ТП ПС практически недостижима без использования развитого специализированного комплекса инструментальных программных средств (ИПС), осуществляющих компьютерную поддержку процедур разработки, проектирования, наладки и сопровождения в процессе функционирования системы.

5.2.2. Инструментальное программное обеспечение. ПО инструментальных средств разработки, отладки и документирования ПТК должно базироваться на действующих стандартах и обеспечить автоматизацию (поддержку) процедур создания программного и информационного обеспечения АСУ ТП, включая функции разработки (модификации) и тестирования. Как правило, результатом работы инструментального ПО должны быть компоненты системы контроля и управления, полностью готовые к запуску.

Инструментальное ПО должно включать следующие программные средства:

– компоновки и генерации программных средств ПТК;

– библиотеку программных модулей стандартных алгоритмов решения задач сбора и обработки технологической информации, контроля и управления;

– автоматизированного формирования исполняемых программных модулей;

– организации и обслуживания баз данных;

– самодиагностики и тестирования аппаратуры и программного обеспечения ПТК;

– включения в состав ПО программ, написанных на универсальных языках программирования;

– допустимой производителем ПТК модификации ПО.

Основу инструментального ПО должны составлять следующие программные системы (пакеты):

1. SCADA-система для организации человеко-машинного интерфейса оперативного персонала ПС и обеспечения функционирования в реальном времени программно-технических средств соответствующих АРМ всего комплекса в целом.

SCADA-система должна обеспечивать [2, 15]:

– коммуникацию с контроллерами среднего уровня для приема от них текущей информации о состоянии технологического объекта и передачи команд оператора для их последующей трансляции в устройства нижнего уровня;

– визуализацию на видеограмме мнемосхемы и других экранных образов (в том числе индикацию аналоговых параметров, изменение состояний и сообщений о событиях) с воссозданием клавиатуры управления на экране (электронные клавиши) и обеспечением возможности управления электронными клавишами.

SCADA-система должна обладать следующими основными свойствами:

– наглядность, простота и удобство конфигурирования (настройки) АРМ с обеспечением возможности внесения изменений в конфигурацию и настройку параметров АРМ в режиме on line и с обеспечением доступа к оперативной базе данных и архивам;

– доступность для прикладных задач наблюдения и управления процессами объектов, имеющих стандартные интерфейсы и аксессуары (кнопки, окна, раскрываемые объекты);

– широкий набор стандартных функций визуализации процесса и управления процессом в сочетании с возможностью программирования и отладки нестандартных функций пользователя с помощью встроенного языка;

– возможности использования полнографического редактора изображений, редактора отчетов и протоколов, редактора аварийных сообщений; базы данных для архивирования информации, широкого набора вспомогательных программ;

– многопользовательский режим на базе локальной сети и технологии «клиент – сервер».

2. ПО для конфигурирования контроллеров среднего и нижнего уровней должно обеспечить:

– параметрирование контроллеров с помощью средств специального технологического языка;

– генерацию загрузочного модуля контроллеров с помощью средств, предусмотренных производителем ПО;

– получение данных, необходимых для функционирования АРМ, автоматизированной обработки информации и организации работы с архивами;

– выпуск комплекта документации по информационному обеспечению ПТК в текстовом и/или графическом виде;

– оперативное внесение изменений в технологическое программное обеспечение ПТК.

3. ПО доступа к МП терминалам РЗА, ПА для их параметрической настройки, дистанционного контроля в процессе эксплуатации, а также анализа аварийных событий и процессов. ПО должно в полном объеме реализовать функции АРМ РЗА, а также функции по обслуживанию терминалов (например, проверку функционирования устройства защиты при подаче на его вход аварийных параметров режима).

Кроме того, появляется возможность дистанционного тестирования устройств РЗА и ПА, которое предполагается выполнять следующим образом:

– устройство РЗА (ПА) переводится в режим тестирования;

– на устройство подается тестовый набор входных сигналов и контролируется работа логики терминала и появление соответствующих команд на выходе терминала, при этом всем выходным сигналам устройства придается статус «TEST», в результате чего дальнейшее действие (отключение выключателей, запуск других комплектов РЗА и т.п.) блокируется; в протокол информация попадает с меткой TEST.

4. ПО для контроля и конфигурирования устройств на шине IEC 61850-9.2 и 61850-8.1 (цифровые ТТ и ТН, модули связи электрооборудования с шиной процесса) должно обеспечить:

– параметрирование устройств;

– блокирование устройства и его дистанционную диагностику.

5.2.3. Информационное обеспечение. (Информационные модели на базе стандартов МЭК 61968/61970). Рассмотрим регламент создания общего информационного пространства ЦПС и организацию информационного взаимодействия ЦПС с центрами управления на основе общей информационной модели (Common Information Model – CIM) [2].

Согласно [2] CIM описывает объектно-ориентированное представление данных, которое включает такие общие абстрактные элементы, как *классы*, *объекты*, *свойства*, *методы и ассоциации*. Формальным определением информационной модели объекта является схема. В схему входят классы, свойства и методы, а также отношения между классами, которые также являются классами.

В случае использования CIM-представления создается единая информационная модель физического объекта и все приложения обмениваются данными, используя их единое описание. CIM-представление является единым языком описания данных и, соответственно, интерфейса только в общей интегрированной среде. Иначе говоря, CIM представляет собой общий язык для приложений при работе в единой большой системе, какой, например, является АСТУ ОАО «ФСК ЕЭС».

Исходными данными для построения информационной модели ЦПС являются:

– главная электрическая схема ЦПС;

– типы, паспортные и иные данные об оборудовании;

– состав и типы измерений, определяющих режим и состояние оборудования;

– методика идентификации объектов и данных ЦПС;

– профиль модели электрических сетей ЕНЭС, в части ПС, определяющий:

- классы, атрибуты и отношения между ними в схеме информационной модели;
- стандарты в области информационных технологий (с точностью до версий), следование которым является обязательным в процессе проектирования, внедрения и эксплуатации системы управления.

Стандартами МЭК 61968/61970 определено описание следующих групп оборудования подстанций:

– коммутационные аппараты (силовые выключатели, разъединители, заземляющие разъединители и т.п.);

– трансформаторное оборудование, включая РПН и систему охлаждения);

– компенсирующее оборудование;

– ограничители напряжения и тока;

– измерительные трансформаторы напряжения и тока.

Информацию об оборудовании можно разделить на следующие категории:

– о текущем состоянии режима (токи, напряжения, мощности) и данные об отклонении эксплуатационных параметров за предельно допустимые значения:

– о работе устройств защит и автоматики;

– данные о текущем состоянии первичного и вторичного оборудования, характеризующие его готовность выполнять свои функции;

– паспортные данные и технические характеристики;

– данные об испытаниях и проведенных ремонтных работах;

– документарная (руководства, инструкции).

Следует отметить, что при проектировании и реализации систем управления технологическими процессами на подстанциях ЕНЭС в качестве базового используется стандарт МЭК 61850, который определяет собственную информационную модель оборудования ПС. При этом информационные модели на базе стандартов МЭК 61968/61970 –

CIM и МЭК 61850 нередко пересекаются в части первичного оборудования и сигналов. Поэтому актуальным является проведение исследований проблем взаимоувязки соответствующих указанным стандартам моделей в процессах информационного обмена между компонентами ПАК ЦПС, а также между подстанциями и центрами управления (ДЦ, ЦУС).

5.2.4. Создание единой системы классификации, кодирования и идентификации оборудования и информации (ЕСКК). Стандарты МЭК 61968/61970 требуют, чтобы описываемое оборудование и информация были поименованы, т.е. им должны быть присвоены уникальные имена.

Уникальные имена должны быть присвоены в соответствии с отраслевой системой, под которой будем понимать единую систему классификации и кодирования – ЕСКК ОАО «ФСК ЕЭС», основанную на общих для всех объектов ЕНЭС принципах идентификации контролируемого и управляемого оборудования ЦПС, компонентов информационно-технологических и управляющих систем и информационных потоков и предназначенную для применения как в пределах подстанции, так и отрасли в целом.

Такая система обозначений, согласно требованию стандарта МЭК 61970, должна удовлетворять требованиям стандарта МЭК 61346 (Промышленные системы, установки и оборудование и промышленные продукты. Принципы структурирования и кодовые обозначения).

5.2.5. Общие положения по построению ЕСКК ЦПС. Единая система классификации, кодирования и идентификации объектов ЕНЭС (класс «Подстанции») – ЕСКК должна удовлетворять следующим основным требованиям:

– единство системы обозначений для всех видов электросетевых объектов;

– достаточная емкость и возможность детализации внутри объектных систем и агрегатов;

– однозначность идентификации любого объекта в пределах системы и связанных с ним данных;

– устойчивость используемых идентификаторов – единство обозначения объектов классификации и маркировки на всех фазах жизненного цикла технического продукта: при проектировании, внедрении (сооружении), эксплуатации, сопровождении, модернизации (реконструкции) энергообъектов, выводе их из эксплуатации;

– возможность встраивания подсистем и технических продуктов в системы, разработанные другими организациями, без изменения этих подсистем и документации;

– поддержка представления системы в разных аспектах, независимо от ее сложности;

– однозначность и корректность выполнения запросов для получения различных данных и документов при машинной обработке (на этапе проектирования и в процессе эксплуатации);

– обеспечение возможности сохранения действующих локальных обозначений.

В соответствии со стандартом МЭК 61346 для однозначной идентификации объекта должна применяться буквенно-цифровая система кодирования. Буквенный код основан на системе классификации, которая должна обеспечить функционально-технологическую иерархию объектов ПС. Буквенные коды являются классификационными кодами типа объекта и независимы от реального положения в системе экземпляров данного типа объекта. Буквенный код должен обозначать технологическое назначение объекта, а не один из аспектов этого объекта (например, «выключатель силовой», но не «выключатель силовой элегазовый»). Система классификации должна отражать практику применения буквенных кодов, а определение классов некоторого уровня системы желательно строить на общей основе.

Цифровые коды (счетные коды), как правило, определяют конкретные экземпляры данного типа объекта определенным классификационным кодом. Для счетных кодов должны быть установлены, по возможности, правила их присвоения.

ЕСКК должна устанавливать правила присвоения идентификаторов с использованием классификационных кодов и принятых в ней методик их использования для всех объектов, относящихся к классу «Подстанция».

Отдельно должны быть разработаны правила применения ЕСКК в части идентификации объектов системы управления, построенной на базе стандарта МЭК 61850.

5.2.5. Описание оборудования и информации в терминах стандарта МЭК 61850. Следует отметить, что стандарт IEC 61850, используемый при проектировании и реализации системы управления технологическими процессами на ПС в качестве базового, определяет собственную информационную модель ПС. При этом информационные модели на базе стандартов МЭК 61968/61970 – CIM и МЭК 61850 нередко пересекаются в части первичного оборудования и сигналов. Так, сказанное выше относительно идентификации объектов ПС на основе стандартов МЭК 61968/61970 применимо и для информационной модели системы управления в стандарте МЭК 61850, с той лишь разницей, что в последнем часть информации жестко проидентифицирована.

Важно подчеркнуть, что в настоящее время не существует технического решения для обеспечения обмена данными между этими двумя видами информационных моделей. Поэтому в числе первоочередных задач должны быть предусмотрены работы по реализации настоящей Методологии с включением НИР по исследованию проблем согласования моделей ЦПС, соответствующих стандартам МЭК 61850 и МЭК 61968/61970 (CIM), в процессах информационного обмена между ЦПС и центрами управления (ДЦ, ЦУС). А также разработка технических решений и инструментальных программных средств поддержки проектирования и функционирования соответствующих ПТК.

5.2.6. Инструментальные программные средства для работы с информационным обеспечением ПАК ЦПС. Обладают основным свойством поддержки полного жизненного цикла ПАК ЦПС и обеспечивают поддержку работ с информационным обеспечением ПАК ЦПС на всех стадиях жизненного цикла комплекса, т.е.:

– при проектировании ПАК;

– при выполнении работ по внедрению ПАК, прежде всего в процессе пуско-наладки, ввода в действие и опытной эксплуатации;

– в процессе промышленной эксплуатации – в случае необходимости внесения допустимых изменений в компоненты информационного обеспечения;

– при возможной реконструкции и расширении подстанции.

На каждой фазе жизненного цикла инструментальные программные средства должны использовать (импортировать) и производить (экспортировать) информацию в виде документации и конфигурационных файлов в заданных специфицированных форматах, принятых в «ОАО ФСК». Каждая фаза должна сопровождаться специфицированным перечнем документов / файлов, полностью описывающих результаты данной фазы жизни ПАК ЦПС. При этом должна обеспечиваться преемственность информационного обеспечения, т.е. возможность передачи информации в электронном виде между фазами жизненного цикла ЦПС.

5.2.7. Поддержка единого информационного пространства ПАК ЦПС. Инструментальные программные средства должны поддерживать единое информационное пространство ПАК ЦПС, для чего необходимо:

– строгое следование стандартам в области представления данных, методам доступа к данным и их корректной интерпретации (применение стандарта IEC 61850 в части обеспечения информационных обменов между компонентами интегрированной системы управления ЦПС, использование стандартов МЭК 61970/61968 в части построения функциональ-

ной координирующей подсистемы и представления ЦПС на высших уровнях иерархии управления – в ДЦ СО, ЦУС, МЭС (ПМЭС);

– использование единой системы классификации, кодирования и идентификации информации – ЕСКК (оборудования, компонентов информационно-технологических и управляющих систем, сигналов, документов и т.д.) в соответствии с принятым в ОАО «ФСК ЕЭС» профилем общей информационной модели ЕНЭС (CIM-профилем). Разработка ЕСКК и принятие соответствующего стандарта является одной из актуальнейших задач создания автоматизированной системы технологического управления (АСТУ) ОАО «ФСК ЕЭС».

5.2.8. Поддержка использования стандартов МЭК. В целях автоматизации процессов проектирования и функционирования ПАК ЦПС должны быть созданы специальные инструментальные программные средства поддержки информационных моделей ЦПС, базирующихся на использовании стандартов МЭК, в том числе:

– средства описания по стандартам МЭК 61970/61968/61850 с использованием ЕСКК ФСК;

– средства взаимного согласования информационных моделей ЦПС, базирующихся на использовании стандартов МЭК 61970/61968 (CIM) и МЭК 61850;

– средства графического описания главной электрической и оперативной схем ПС, функциональных схем системы управления ПС. Графические описания должны быть связаны с данными модели ПС (по стандартам МЭК 61970/61968/61850) и образовывать с ними непротиворечивую информационную модель. Формат хранения графических данных должен соответствовать МЭК 61970 – 453.

5.2.9. Метрологическое обеспечение. Методология метрологического обеспечения – это набор базисных принципов, методов, способов, которыми достигаются единство и точность измерений в измерительной системе (ИС) ЦПС. Структура ИС ЦПС изображена ниже на рис. 5.2 [2].

К базовым принципам построения ИС ЦПС относятся:

– вертикальная дифференциация;

– горизонтальная интеграция.

Следствием применения принципа вертикальной дифференциации является четкое разделение средств измерений, применяемых в ИС ЦПС, на:

– преобразования первичных данных (трансформаторы тока, трансформаторы напряжения, датчики технологической информации);

– отображение данных первичных преобразований в унифицированный цифровой вид (устройства объединения);

– вычисления и обработку цифровых данных (устройства защиты, счетчики электроэнергии, устройства телемеханики и т.д.).


**Рис. 5.2. Структура измерительной системы (ИС) ЦПС**

Следствием применения принципа горизонтальной интеграции является применение в ИС ЦПС следующих связующих компонентов:

– система обеспечения единого времени (СОЕВ), обеспечивающая синхронность работы всех компонентов ИС;

– единая коммуникационная сеть, обеспечивающая доступность данных от любого первичного преобразователя любому конечному устройству.

Повышение точности измерений в пределах ИС ЦПС реализуется следующими способами:

– повышение качества первичных преобразований за счет использования более точных средств первичного преобразования;

– снижение метрологических потерь, связанное с передачей аналоговой информации;

– применение микропроцессорных средств вычислений.

Обеспечение единства измерений в пределах ИС ЦПС осуществляется следующими способами:

– синхронизация первичных измерителей;

– использование передачи данных в цифровом виде;

– возможность тиражирования данных.

5.2.10. Общие требования к методологии метрологического обеспечения ИС ЦПС. Согласно [2] ИС ЦПС является типовым измерительным объектом типа ИС-2.

*Измерительные компоненты*. В ИС ЦПС должны использоваться электронные трансформаторы (т.е. трансформаторы, снабженные цифровым выходом). Использование традиционных трансформаторов допустимо только совместно с использованием измерительного преобразователя.

*Вычислительные компоненты.* Вычислительный компонент должен иметь сопряжение с коммуникационной сетью ЦПС. В качестве основного потока входных данных вычислительный компонент должен использовать поток данных от устройств объединения и датчиков технологической информации в формате согласно стандартам [2]. В качестве входного сигнала для вычислительного компонента также выступает источник синхронизации.

*Связующие компоненты.* Сеть передачи измерительных данных должна быть выполнена в рамках коммуникационной сети ЦПС. Пропускная способность связевого и коммуникационного оборудования должна быть достаточна для передачи данных от устройств объединения к вычислительным компонентам в объеме и количестве, предусмотренном проектным решением.

5.2.11. Требования к нормам точности измерений. Нормы точности измерительных каналов ИС ЦПС определяются особенностями процесса измерения. В типовом измерительном канале процесс измерения можно разбить на следующие этапы:

– аналого-цифровое преобразование (измерительные компоненты);

– вычисление на основе преобразованных данных самой измеряемой величины (вычислительный компонент).

Исходя из того, что погрешность вычисления алгоритмов определяется через характеристики входных значений, и все множество алгоритмов ИС ЦПС использует одни и те же данные первичных преобразований, то требования к точности измерительных компонентов фор-

мируются на основе требования точности всех вычислительных компонентов. В этом состоит отличие ИС ЦПС от традиционных, в которых, как правило, использовался отдельный измерительный канал для каждой функциональной задачи.

Для того чтобы предъявить требования к вычислительным компонентам, необходимо классифицировать множество измеряемых ИС ЦПС величин. Результат классификации представлен в табл. 5.1 [2].

Требования к точности компонентов ИС ЦПС устанавливаются на основании анализа способов вычисления данных величин и требований к ним, установленным в нормативной документации.

5.2.12. Нормы точности измерительных компонентов. Для электронных трансформаторов тока и напряжения нормируют класс точности и определяют предел погрешности в соответствии с [2].

Для устройств объединения нормируют следующие метрологические характеристики цифрового потока данных:

- частоту дискретизации;
- эффективную разрядность данных;
- погрешность синхронизации;

Указанные метрологические характеристики нормируют для различных потоков, формируемых устройством объединения, в зависимости от целей, для которых они применяются. Следует различать цели для:

- защиты и управления;
- учета электроэнергии;
- измерений показателей качества электрической энергии.

На выбор частоты дискретизации влияет необходимость учета, не менее:

- 5 гармоник для целей защиты;
- 13 гармоник для целей учета электроэнергии;
- 50 гармоник для целей измерения ПКЭ.

Частоту дискретизации ($f_s$) следует нормировать в виде $f_s = N f_r$, где $N$ – количество выборок, приходящихся на период номинальной частоты ($f_r$).

Частота дискретизации должна быть как минимум вдвое выше частотного диапазона (теорема Котельникова–Найквиста), следовательно, необходимо выбирать $N = 2am$, где $m$ – необходимое число гармоник; $a$ – коэффициент запаса (не обязательно целый, но не менее 2 для целей измерений), необходимый для предварительной цифровой обработки сигнала вычислительными компонентами ИС ЦПС. Отсюда необходимо для частоты дискретизации выбирать значения, не менее:

- 500 Гц для защиты;
- 2600 Гц для целей учета электроэнергии;
- 10 000 Гц для целей анализа качества электроэнергии.

Эффективную разрядность данных нормируют исходя из потребностей типовых алгоритмов обработки данного потока, вычисления:

– действующих значений тока и напряжения простейшими способами, сравнение с уставками, в алгоритмах для целей защиты;

– действующих значений мощности, накопительных алгоритмов для целей учета электроэнергии;

– Фурье-преобразования для целей вычислений параметров качества электроэнергии.

На основе методики [2] можно установить, что минимальная:

– эффективная разрядность цифрового потока тока для целей защиты должна быть не менее 10 бит;

– эффективная разрядность цифрового потока напряжения для целей защиты должна быть не менее 13 бит.

Аналогично требования для цифровых потоков, применяемых для измерений, приведены в табл. 5.2 [2]. Требования к точности синхронизации предъявляют исходя из требований различных задач, для которых используются цифровые потоки. В ИС ЦПС применяется универсальная система синхронизации, поэтому она должна выдерживать самые жесткие предъявляемые требования. На основе [2] к системе следует предъявить требования синхронизации данных токов и напряжений в 1 мкс.

5.2.13. Нормы точности вычислительных компонентов. Нормами точности для вычислительного элемента является точность алгоритмов, на основе которых выполняется расчет величины. Вычисляемые характеристики можно условно разделить на следующие типы по характеру входных данных:

– канальные, вычисляются на основе данных одного канала (например, действующие значения тока);

– фазные, вычисляемые на основе данных одной фазы (например, действующее значение мощности);

– многофазные, вычисляемые на основе данных трехфазной системы (например, действующее значение обратной последовательности).

**5.2. Требования к минимальной разрядности**

| Класс точности | Канал тока | | | | | | Канал напряжения | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0.1 | 0.2 | 0.5 | 1 | 0.2S | 0.5S | 0.1 | 0.2 | 0.5 | 1 | 3 |
| Разрядность, бит | 16 | 15 | 14 | 13 | 17 | 16 | 14 | 13 | 12 | 11 | 9 |

Вычисляемые характеристики можно разделить на критичные к гармоникам и некритичные к ним.

Для алгоритмов, реализуемых на вычислительных компонентах, следует нормировать следующие характеристики:

– вычислительная погрешность на идеальных данных;

– зависимость погрешности алгоритма от погрешности входных данных;

– условия достоверности алгоритма.

При разработке алгоритмов необходимо стремиться к тому, чтобы вычислительная погрешность на идеальных данных стремилась к нулю, а зависимость погрешности алгоритма от погрешности входного потока была минимальной в метрологическом диапазоне параметров потока.

5.2.14. Нормы точности измерительных каналов. Основной метрологической характеристикой канала является вычислительная погрешность алгоритма, который вычисляет данную характеристику, определенная по нормированным характеристикам входных цифровых потоков.

Перечень основных характеристик, которые необходимо вычислять в пределах ИС ЦПС, указан ранее. Там же представлены основные нормативные документы, в которых определены нормы точности для измерения данных характеристик.

5.2.15. Требования к поверке измерительных каналов. ИС ЦПС имеет четкую структуру, которая отражена в структуре измерительных каналов. Типовой измерительный канал состоит из измерительного, вычислительного и прочих компонентов. Метрологические характеристики измерительных каналов определяются только измерительным и вычислительным компонентами. Благодаря глубокой коммуникационной и синхронизационной интеграции в такой системе возможно построение большого числа измерительных каналов. Независимая поверка каждого канала в отдельности становится нерациональной. Таким образом, для поверки измерительных каналов ИС ЦПС используется метод покомпонентного анализа.

Покомпонентная поверка подразумевает независимую поверку всех компонентов, входящих в измерительный канал. На основании удовлетворительной поверки всех компонентов делается вывод об удовлетворительной поверке измерительного канала.

Таким образом, в части поверки измерительных каналов ИС ЦПС возникают следующие разнородные задачи, поверка:

– измерительных компонентов (реальных физических приборов);

– поверка вычислительных компонентов (алгоритмов расчета);

– проверка работоспособности связевых компонентов.

Следует отметить, что архитектура ИС ЦПС реализует отделение функции первичного преобразования от функций вычисления, в связи с чем возникает нормативное обеспечение поверки и аттестации вычислительных средств измерений. В настоящий момент существуют требования WELMEC 7.2 и их российская адаптация [2].

Однако считать данные нормативные инициативы базовыми пока не представляется возможным в силу новизны проблемы.

5.2.16. Общие требования. Поверке подвергают измерительные каналы ИС ЦПС, на которые распространен сертификат утверждения типа средств измерений.

Поверку измерительного канала проводят:

– первично, при вводе системы в эксплуатацию;
– по истечению межповерочного интервала;
– при замене одного из компонентов системы, при этом допускается проводить поверку только заменяемого компонента.

5.2.17. Поверка измерительных компонентов. Поверку электронных трансформаторов тока и электронных трансформаторов напряжения проводят с помощью методов [2].

Система, состоящая из традиционного трансформатора и измерительного преобразователя, должна поверяться как электронный трансформатор (рис. 5.3) [2].

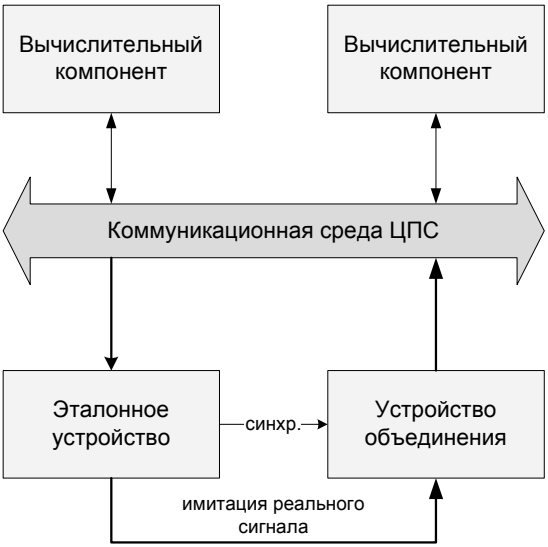


**Рис. 5.3. Схема поверки измерительных компонентов ИС ЦПС**

Определение амплитудно-частотных характеристик трансформаторов является на сегодняшний день открытой актуальной проблемой, рассмотрение которой выходит за рамки монографии. Если определить амплитудно-частотные характеристики невозможно, следует для трансформаторов использовать амплитудно-частотные характеристики, полученные в результате численного моделирования или экстраполяции.

Модуль объединения должен поверяться методом сравнения с эталоном. Эталонное устройство должно:

– формировать цифровой поток либо на основе заданных характеристик, либо на основе записанного цифрового файла;

– формировать сигнал синхронизации либо иметь синхронизационное окончание, такое же, как и на модуле объединения;

– иметь интерфейс Ethernet, совместимый с устройством объединения.

Для проведения поверочных испытаний:

– к устройству объединения присоединяется в качестве входных выходные цепи эталонного устройства;

– эталонное устройство синхронизуется с устройством объединения;

– эталонное устройство и модуль объединения соединяются посредством сети Ethernet;

– с помощью типовых тестов определяют основные метрологические характеристики модулей объединения; поверка осуществляется на основе анализа по выборочной разнице между сформированными и выданными цифровыми данными;

– с помощью записанных файлов имитируют работу электронных трансформаторов, с которыми должно работать устройство объединения.

5.2.18. Поверка вычислительных компонентов. Вычислительные компоненты проходят первичную поверку при сертификации алгоритмов, на которых они основаны.

Поверка вычислительного компонента производится с помощью эталонных цифровых потоков двух типов. Первый тип является фиксированным и предназначен для определения вычислительной точности алгоритма в идеальных условиях. Второй предназначен для определения вычислительной погрешности в зависимости от погрешностей входных потоков и должен содержать случайную компоненту.

Поверочные сигналы не должны быть привязаны к алгоритму, который вычисляет заданную характеристику, но должны определяться самой характеристикой.

5.2.19. Поверка работоспособности связевых компонентов. Включает в себя проверку:

– целостности коммуникационной среды;
– пропускной способности коммуникационной среды;
– доступности коммуникационной среды;
– латентности коммуникационной среды;
– прочие проверки.

5.2.20. Оценка влияния коммуникационной среды на метрологические характеристики измерительных каналов. Коммуникационная среда представляет важную часть ИС ЦПС. Несмотря на то, что сама по себе она не является средством измерения, ее характеристики могут оказывать на процесс измерения существенное влияние. Коммуникационная среда ЦПС строится на базе сетей Ethernet, в основе которой лежит пакетный принцип передачи данных. Таким образом, в пределах коммуникационной среды ЦПС потеря информации сводится к потере пакетов. К ситуации потери пакета следует также отнести ситуацию, в которой пакет был доставлен с задержкой, превышающей нормативные значения, указанные в [2]. Влияние потери пакета на алгоритмы зависит от целей, для которых применяют алгоритм, для:

– алгоритмов, применяемых для целей защиты, потеря пакета неприемлема;

– алгоритмов, применяемых для вычислений действующих значений, которые в основном основаны на вычислении сверток, потеря пакетов приводит к снижению точности;

– алгоритмов, применяемых для вычисления показателей качества электрической энергии, потеря пакета может привести к значительному искажению результата, поэтому ПКЭ, вычисленные с потерей пакета, должны быть маркированы как недостоверные, согласно [2].

## 5.3. НАДЕЖНОСТЬ, ИНФОРМАЦИОННАЯ И КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ

В число основных целей создания ЦПС входит создание технических условий для перехода к подстанциям без постоянного присутствия дежурного персонала (с управлением из диспетчерских центров или ЦУС) и интеграции подстанций в активно-адаптивную электрическую сеть (ААС). В свете указанных целей к ЦПС предъявляются требования по обеспечению надежности выполнения основных технологических функций подстанции, которые, по меньшей мере, не ниже, а по отдельным показателям надежности – выше аналогичных требований к большинству существующих подстанций ЕНЭС РФ.

Надежность выполнения ЦПС своих основных технологических функций в значительной степени определяется надежностью компонентов программно-аппаратного комплекса (ПАК) ЦПС.

В связи с вышесказанным для обеспечения высоких требований по надежности, предъявляемых к оборудованию ПАК ЦПС, требуется разработка единой программы обеспечения надежности ПАК ЦПС, решающей задачи обеспечения надежности ПАК ЦПС в комплексе, регламентирующей, в том числе, требования:

– к применению самодиагностики и функциональной диагностики оборудования ПАК ЦПС;

– к резервированию компонентов ПАК ЦПС;

– к регламентам проведения работ по техническому обслуживанию и ремонтам оборудования ПАК ЦПС на основании данных самодиагностики и функциональной диагностики оборудования и т.п.

5.3.1. Состояние вопроса надежности в мировой практике построения ЦПС. Значимой тенденцией, сопутствующей переходу от традиционных подстанций к цифровым, является переход от периодического технического обслуживания и ремонтов оборудования подстанций к техническому обслуживанию и ремонтам оборудования подстанций по состоянию. Принятые в современной зарубежной электроэнергетике требования (к примеру, нормативный документ NERC (США) [2]) устанавливают необходимость в организации процессов аудита действующих программ технического обслуживания и ремонтов по состоянию в соответствии со стандартами управления качеством (ISO 9001) или надежностью (IEC 60300).

5.3.2. Анализ современных требований к надежности ЦПС**.** Базовые требования из области надежности к АСУ ТП и отдельным компонентам оборудования подстанций определены стандартами ГОСТ серии 27: ГОСТ 27.002, ГОСТ 27.003, ГОСТ 27.301, ГОСТ 27.310, ГОСТ 27.410.

Требования по надежности к компонентам первичного оборудования подстанций определяются требованиями государственных стандартов на отдельные виды оборудования (ГОСТ 11677, ГОСТ Р 52565 и т.п.).

Требования по надежности оборудования вторичных систем подстанций определяются, в основном, требованиями отраслевых документов, в том числе РД 34.35.120 и РД 34.35.310.

Требования к надежности коммуникационной среды подстанции определены в принятом стандарте ГОСТ Р МЭК 61850-3.

Международной электротехнической комиссией (МЭК) приняты стандарты, регламентирующие требования к системам управления надежностью в электроэнергетике. Основная часть данных стандартов принята в РФ. Организация процессов управления надежностью ЦПС в соответствии со стандартами ГОСТ Р 51901.2, ГОСТ Р 51901.3 и др. не только имеет целью обеспечение выполнения программ технического обслуживания и ремонтов оборудования ЦПС по состоянию и процессов аудита выполнения указанных программ, как это требуется за рубежом, но также обеспечивает упорядочивание процессов, направленных на поддержание необходимого уровня надежности ЦПС в целом, реализацию программ повышения надежности ЦПС на всех стадиях жизненного цикла ЦПС (проектирование, внедрение, эксплуатация). В связи с этим создание системы управления надежностью ЦПС является ключевым моментом программы обеспечения надежности (ПОН) ЦПС.

5.3.3. Общие требования к надежности ЦПС. В рамках данного подраздела применяются термины из области надежности в соответствии с ГОСТ 27.002. Дополнительные термины из области надежности, используемые и применяемые в текущем подразделе, приведены ниже в табл. 5.3 [2].

**5.3. Термины из области надежности**

| Термин | Определение термина |
|---|---|
| Единичный отказ компонента ПАК ЦПС | Событие отказа одного компонента ПАК ЦПС при сохранении работоспособности остальных компонентов ПАК ЦПС |
| Множественный отказ компонентов ПАК ЦПС | Одновременное возникновение нескольких единичных отказов компонентов ПАК ЦПС или единичный отказ компонента ПАК ЦПС при неработоспособности одного или нескольких других компонентов ПАК ЦПС |
| Единая точка отказа | Один или несколько компонентов ПАК ЦПС, одновременный отказ или неработоспособное состояние которых приводит к отказу какой-либо функциональной подсистемы АСУ ТП ЦПС |

В рамках данной Методологии рассматриваются следующие объекты надежности ЦПС:

– отдельные компоненты ПАК ЦПС, в том числе первичное оборудование (силовые трансформаторы и автотрансформаторы, высоковольтные коммутационные аппараты и др.) и оборудование вторичных систем (устройства IED, коммуникационное оборудование, серверы синхронизации времени, кабельные системы коммуникационной сети и сети синхронизации времени ЦПС и т.п.);

– отдельные функции системы АСУ ТП ЦПС (функции РЗА, ПА, РАС, ОМП, учета электроэнергии, контроля качества электроэнергии и т.п.).

Структура объектов надежности ЦПС показана ниже на рис. 5.4 [2].

5.3.4. Требования к надежности компонентов ПАК ЦПС. Компоненты ПАК ЦПС должны соответствовать следующим требованиям стандарта ГОСТ Р МЭК 61850-3 по надежности.

Любой единичный или множественный отказ компонентов ПАК ЦПС, относящихся к оборудованию вторичных систем подстанции, не должен приводить к отказу других компонентов ПАК ЦПС (работоспособных до возникновения указанного единичного или множественного отказа).

Любой единичный или множественный отказ компонентов ПАК ЦПС должен своевременно обнаруживаться.

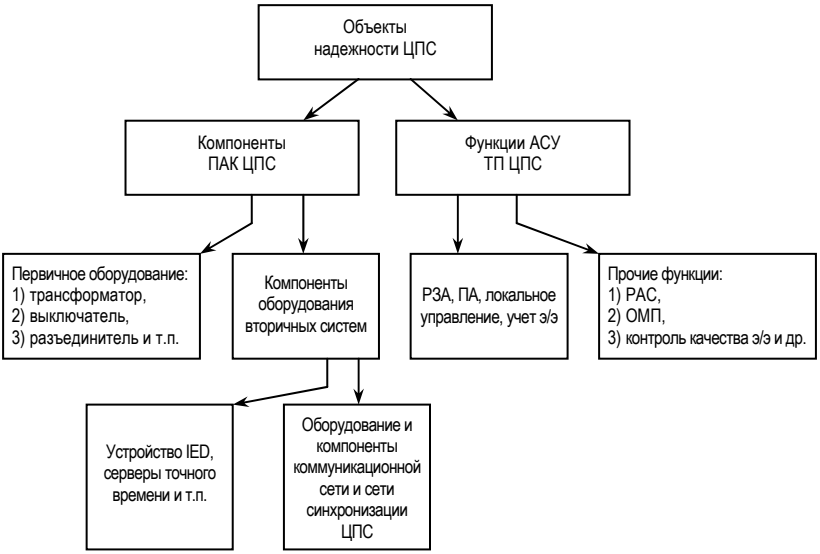


**Рис. 5.4. Структура объектов надежности ЦПС**

Коммуникационная сеть и сеть синхронизации времени ЦПС должны обеспечить поддержку резервирования компонентов ПАК ЦПС, в том числе, поддержку автоматического переключения с основного компонента на резервный при отказе основного компонента.

Время переключения с основного компонента на резервный при отказе основного компонента коммуникационной сети или сети синхронизации времени ЦПС не должно превышать предельного времени переключения, при котором обеспечивается сохранность показателей вероятности безотказной работы функций АСУ ТП ЦПС.

При использовании резервирования компонентов ПАК ЦПС, относящихся к оборудованию вторичных систем подстанции, должны быть исключены единые точки отказа, возникновение отказа в которых может привести одновременно к неработоспособности основного (резервируемого) и резервного компонента, или наличие указанных единых точек отказа должно быть сведено к минимуму.

Любой возможный единичный или множественный отказ компонентов ПАК ЦПС, относящихся к оборудованию вторичных систем подстанции, не должен приводить к запрещенным и/или нерегламентированным управляющим воздействиям на первичное оборудование.

Деградационные отказы компонентов ПАК ЦПС должны быть сведены к минимуму за счет замены компонентов достигших предельного состояния (определение терминов «деградационный отказ» и «предельное состояние» – в соответствии с ГОСТ 27.002).

В составе ПАК ЦПС должны применяться только такие компоненты оборудования, для которых производителем данного оборудования регламентирована вероятность отказа компонента в течение заявленного производителем срока службы компонента или среднее время наработки до отказа.

Применяемые в ПАК ЦПС устройства IED в части требований по надежности должны соответствовать РД 34.35.310.

5.3.5. Требования к надежности функций АСУ ТП ЦПС. В соответствии с требованиями РД 34.35.120 значение показателя вероятности безотказной работы для отдельных функций ЦПС в течение срока службы ЦПС должно составлять не менее [1,2]:

– 0,9997 – для функций РЗА;

– 0,999 – для прочих функций АСУ ТП ЦПС, в том числе функций ПА, автоматического и оперативного управления, учета электроэнергии, контроля качества электроэнергии, регистрации аварийных событий, ОМП и т.п.

При построении ЦПС (на этапе заказа работ по созданию ЦПС или этапе проектирования ЦПС) допускается для отдельных функций ЦПС устанавливать более высокие значения требуемого показателя вероятности безотказной работы в течение срока службы ЦПС.

В ЦПС должно обеспечиваться взаимное резервирование функций локального управления подстанцией (с АРМ ОП) и удаленного управления подстанцией (из диспетчерского пункта).

При отказе какой-либо функции АСУ ТП ЦПС среднее время восстановления работоспособности данной функции с обеспечением на период восстановления резервирования данной функции в соответствии с требованиями ГОСТ Р МЭК 61850-3 должно составлять не более 36 ч (соответственно классу ремонтопригодности М1 по ГОСТ Р МЭК 870-4). Указанный лимит времени восстановления включает в себя время ожидания восстановления (организационное и транспортное время в соответствии с ГОСТ Р МЭК 870-4) и время проведения непосредственно работ по восстановлению.

При отказе какой-либо функции АСУ ТП или смежной интегрируемой в АСУ ТП системы, не имеющей резерва, или одновременном отказе функции и ее резерва суммарное время восстановления работоспособности данной функции должно составлять:

– для функций РЗА, противоаварийной автоматики, автоматического и оперативного управления – не более допускаемого времени восстановления устройства РЗА в соответствии с РД 34.35.310, т.е. не более 0,5 ч;

– для прочих функций АСУ ТП ЦПС – не более 6 ч (в соответствии с классом ремонтопригодности М3 по ГОСТ Р МЭК 870-4).

При построении ЦПС (на этапе заказа работ по созданию ЦПС) допускается устанавливать меньшие требуемые лимиты времени восстановления работоспособности функций ЦПС, чем указано выше.

5.3.6. Методы обеспечения программно-аппаратной надежности ЦПС. Комплекс методов обеспечения программно-аппаратной надежности ПАК ЦПС включает в себя следующие методы:

– самодиагностика и внешняя автоматизированная диагностика компонентов ПАК ЦПС;

– применение в ПАК ЦПС оборудования со встроенными средствами автоматического восстановления после сбоев;

– функциональная диагностика ПАК ЦПС;

– резервирование компонентов ПАК ЦПС;

– применение в рамках ЦПС системы управления надежностью на базе стандартов ГОСТ Р 51901.2, ГОСТ Р 51901.3 и др.

Далее в отдельных пунктах приведено описание вышеперечисленных методов обеспечения программно-аппаратной надежности ЦПС.

5.3.7. Самодиагностика и внешняя автоматизированная диагностика компонентов ПАК ЦПС. В подразделе приведены требования к самодиагностике и внешней автоматизированной диагностике компонентов ПАК ЦПС, а также требования к применению средств автоматического восстановления после сбоев в компонентах ПАК ЦПС.

Общая схема самодиагностики и внешней автоматизированной диагностики показана ниже на рис. 5.5 [2].

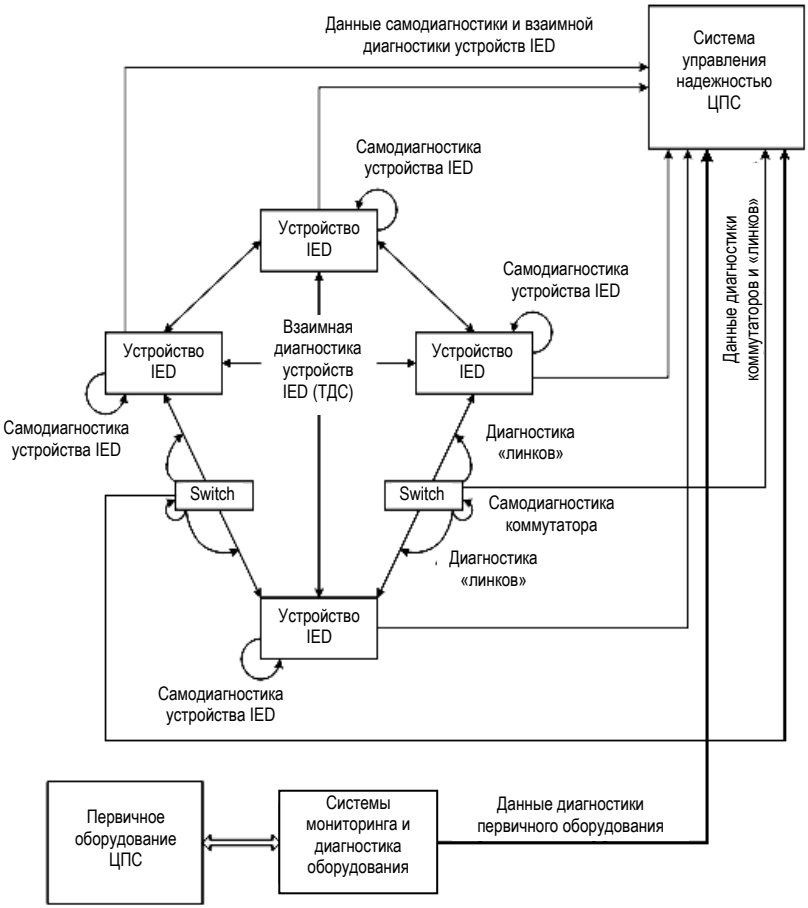


**Рис. 5.5. Структура общих требований к ЦПС в части надежности**

В рамках ЦПС должен выполняться непрерывный мониторинг состояния всего первичного оборудования подстанции, в том числе:

– силовых трансформаторов, автотрансформаторов, трансформаторов собственных нужд, устройств РПН трансформаторов, систем охлаждения силовых трансформаторов (автотрансформаторов, трансформаторов собственных нужд);

– высоковольтных выключателей и разъединителей;

– оборудования систем оперативного постоянного тока, в том числе аккумуляторных батарей.

Перечень параметров мониторинга для каждого вида первичного оборудования, временной регламент выполнения мониторинга должны определяться действующими регламентами ОАО «ФСК ЕЭС».

Каждое устройство IED в составе ПАК ЦПС, в том числе, устройства IED нижнего уровня АСУ ТП ЦПС и устройства IED связи АСУ ТП с первичным оборудованием должны выполнять функции самодиагностики.

Функции самодиагностики устройств IED должны обеспечить контроль зависания внутренней программы устройства. При обнаружении зависания внутренней программы устройство должно производить немедленную автоматическую перезагрузку внутренней программы.

Функции самодиагностики устройств IED должны обеспечить проверку работоспособности аппаратных элементов устройства IED.

Для каждого аппаратного элемента IED, проверяемого в ходе процедур самодиагностики IED (внешние информационные интерфейсы, микропроцессор, внутренние часы, оперативная память, блоки АЦП), устройство IED должно выполнять проверку работоспособности с периодичностью не менее одного раза в сутки.

Устройства IED с резервируемыми блоками электропитания дополнительно должны обеспечить диагностику работоспособности основного блока питания (блока питания, через который осуществляется питание устройства в данный момент времени). При диагностировании отказа основного блока питания устройство IED должно обеспечить переключение на резервный с фиксацией события в журнале событий.

Все применяемые в рамках ЦПС устройства IED должны производить непрерывный информационный обмен тестовыми диагностическими сообщениями (далее – ТДС) через коммуникационную сеть ЦПС с целью обеспечения быстрого выявления отказов отдельных устройств IED в ЦПС.

ТДС должны иметь формат GOOSE-сообщений в соответствии с IEC 61850-8.1.

Каждое устройство IED в ЦПС должно обеспечивать одновременно прием и отправку ТДС.

Количество устройств IED – получателей ТДС от данного устройства IED в рамках ЦПС должно быть не менее двух. Конкретные получатели ТДС от данного устройства IED определяются на стадии проектирования ЦПС.

Каждое устройство IED должно обеспечить прием ТДС одновременно не менее чем от двух устройств IED – отправителей ТДС. Конкретные отправители ТДС, для которых данное устройство IED является получателем, определяются на стадии проектирования ЦПС.

Устройство IED должно фиксировать и вести учет последних ТДС, полученных от других устройств IED – отправителей ТДС. В случае, если от одного из отправителей в течение длительного времени после последнего ТДС не было получено нового ТДС, данное устройство IED должно немедленно сигнализировать о возможном отказе устройства IED – отправителя ТДС.

5.3.8. Функциональная диагностика ПАК ЦПС. Функциональная диагностика – проверка корректной работы компонентов ПАК ЦПС в режиме штатного выполнения функций подстанции (в штатном режиме АСУ ТП ЦПС) или с использованием тестового режима выполнения функций АСУ ТП ЦПС. Различаются три основных метода функциональной диагностики ЦПС:

1. Проверка функциональных подсистем оперативного управления, а также интегрированных в АСУ ТП систем РЗА, противоаварийной автоматики, автоматического управления с использованием тестового режима выполнения функций АСУ ТП ЦПС.

2. Проверка функциональных подсистем оперативного управления, а также интегрированных в АСУ ТП систем РЗА, противоаварийной автоматики, автоматического управления в штатном режиме выполнения функций АСУ ТП ЦПС.

3. Проверка функциональных подсистем первичных измерений, измерений производных величин, а также интегрированной системы учета электроэнергии в процессе штатного функционирования АСУ ТП ЦПС методом сведения балансов по присоединениям. Далее в отдельных подпунктах приведено описание вышеуказанных методов функциональной диагностики ПАК ЦПС.

5.3.9. Проверка устройств в тестовом режиме работы. Цифровые вторичные цепи и информационные потоки позволяют производить функциональную самодиагностику в процессе штатного функционирования системы. Далее приведено описание метода на примере функциональной диагностики устройства РЗА (IED) (рис. 5.6) [2].

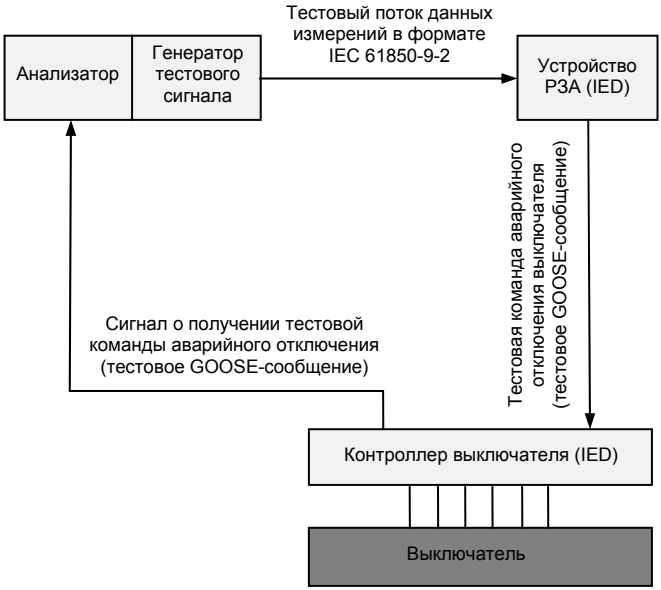


**Рис. 5.6. Функциональная диагностика релейной защиты в тестовом режиме работы АСУ ТП ЦПС**

В ЦПС имеется отдельный генератор тестового измерительного сигнала, который производит генерацию тестового потока данных измерений тока/напряжения в формате протокола IEC 61850-9.2. Получателем тестового потока IEC 61850-9.2 является тестируемое устройство РЗА (IED). Данные потока помечены как «test».

Генератор тестового сигнала формирует тестовый поток IEC 61850-9.2, соответствующий данным измерения тока / напряжения в нормальном (неаварийном) режиме. Периодически (с периодичностью, как правило, от нескольких секунд до нескольких минут) генератор вставляет в поток IEC 61850-9.2 запрограммированную серию срезов мгновенных значений тока / напряжения, соответствующих аварийному режиму (режиму, в котором должна срабатывать релейная защита). При получении серии срезов данных измерений потока IEC 61850-9.2, соответствующих аварийному режиму, устройство РЗА отдает команду на аварийное отключение выключателя, посылая GOOSE-сообщение (IEC 61850-8.1) контроллеру выключателя. Поскольку устройство РЗА «осведомлено» о том, что входной поток IEC 61850-9.2 является тестовым, GOOSE-сообщение, содержащее в себе команду аварийного отключения, также снабжается признаком «test».

Контроллер выключателя получает GOOSE-сообщение с командой аварийного отключения. Так как GOOSE-сообщение помечено флагом «test», контроллер выключателя не производит фактического отключения выключателя. Итоговое диагностическое GOOSE-сообщение также помечается флагом «test».

Анализатор по полученному итоговому диагностическому GOOSE-сообщению определяет временные характеристики срабатывания релейной защиты в ЦПС.

5.3.10. Проверка функциональных подсистем оперативного управления, а также интегрированных в АСУ ТП систем РЗА, ПА, автоматического управления при штатном выполнении функций. Описание метода приведено на примере функциональной диагностики функции интегрированного в АСУ ТП ЦПС устройства релейной защиты (рис. 5.7) [2].

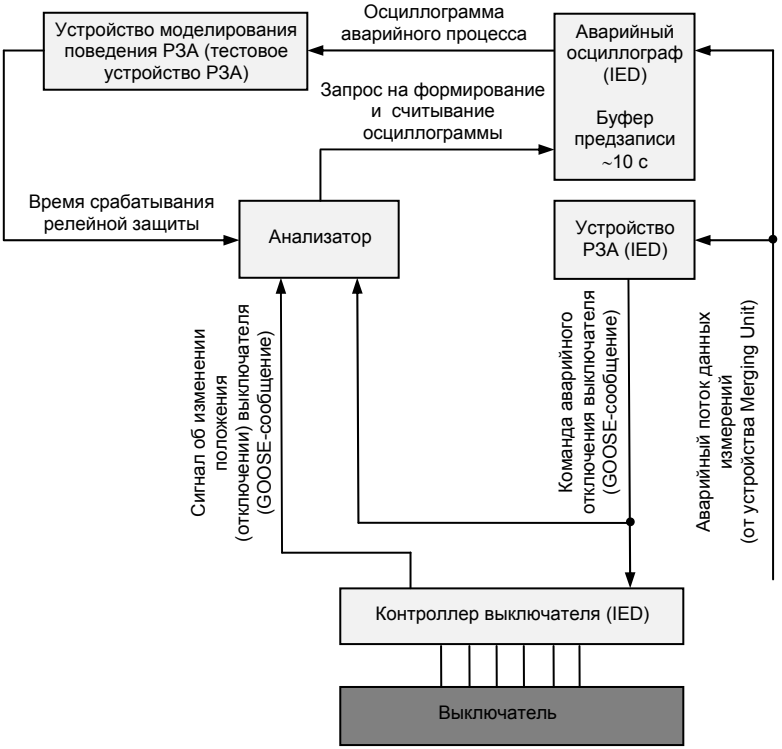


**Рис. 5.7. Функциональная диагностика релейной защиты в тестовом режиме работы АСУ ТП ЦПС**

Данный пример иллюстрирует один из возможных подходов к решению задачи. На последующих этапах работы необходимо разработать техническое решение, удовлетворяющее требованиям, предъявляемым к системам РЗА и ПА.

Функциональная диагностика релейной защиты в режиме штатного выполнения функций АСУ ТП ЦПС обеспечивает проверку всех компонентов ПАК ЦПС, на базе которых функционирует подсистема релейной защиты, в том числе устройства РЗА (IED), контроллера выключателя, каналов коммуникационной сети («линков») между устройством РЗА, контроллером выключателя и т.п. в штатном режиме, в том числе и в момент срабатывания устройства РЗА.

Устройство РЗА присоединения штатно получает поток данных измерений тока и/или напряжения в формате IEC 61850-9.2. Параллельно в коммуникационной сети ЦПС функционирует аварийный осциллограф, который также является получателем данного потока IEC 61850-9.2. Аварийный осциллограф производит непрерывное осциллографирование тока/напряжения на глубину порядка нескольких секунд (~ 10 с).

При получении аварийного сигнала IEC 61850-9.2 срабатывает устройство РЗА, формирующее при своем срабатывании GOOSE-сообщение с командой аварийного отключения, которое посылается контроллеру выключателя. Контроллер выключателя производит отключение выключателя. После выполнения отключения выключателя контроллер формирует GOOSE-сообщение об измененном (отключенном) положении выключателя.

Указанное GOOSE-сообщение улавливается анализатором. Анализатор также улавливает GOOSE-сообщения от устройства РЗА с командами аварийного отключения. GOOSE-сообщение от устройства РЗА с командой аварийного отключения выключателя должно содержать в себе отметку времени формирования (отправки) данного GOOSE-сообщения. Формируемое контроллером выключателя GOOSE-сообщение об измененном (отключенном) положении выключателя должно содержать в себе отметку времени момента отключения выключателя.

При получении GOOSE-сообщений о срабатывании РЗА и об отключенном положении выключателя после срабатывания РЗА анализатор формирует команду аварийному осциллографу (IED) о записи осциллограммы, накопленной в буфере предварительной записи. Указанная осциллограмма передается устройству моделирования, которое производит моделирование процесса срабатывания РЗА по исходным

данным в виде осциллограммы кривых тока/напряжения и на основании имеющихся у него текущих уставок устройства РЗА. При моделировании процесса срабатывания РЗА точно вычисляется требуемый момент времени срабатывания. Указанные данные о времени срабатывания передаются анализатору. На основании этих и ранее полученных данных анализатор определяет:

1. Время срабатывания устройства РЗА (от момента получения аварийной серии срезов мгновенных значений тока/напряжения в формате протокола IEC 61850-9.2 до момента отправки GOOSE-сообщения контроллеру выключателя с командой аварийного отключения).

2. Время передачи GOOSE-сообщения от РЗА контроллеру выключателя.

3. Время от момента получения контроллером выключателя команды аварийного отключения до момента отключения выключателя.

Замеры вышеуказанных временных параметров при штатном выполнении функции РЗА позволяют диагностировать соответствие указанных параметров требуемым временным характеристикам работы функций РЗА. При обнаружении несоответствия временных параметров требованиям производится автоматическое информирование локально на АРМ ОП или АРМ-релейщика, или информирование соответствующих служб эксплуатации подстанции по цифровым каналам связи.

В ЦПС функциональная диагностика должна применяться для каждой функциональной подсистемы, обеспечивающей выполнение функций РЗА.

Рекомендуется применять функциональную диагностику для следующих функциональных подсистем ЦПС:

– подсистемы ПА, автоматического и оперативного управления;

– подсистемы первичных измерений тока/напряжения для задач РЗА;

– подсистемы учета электроэнергии – для особо ответственных присоединений подстанции (например, отходящих высоковольтных линий с целью обеспечения более высокой надежности функций учета электроэнергии).

Допускается применение вышеописанной схемы диагностики функциональной подсистемы РЗА без аварийного осциллографа и устройства моделирования срабатывания РЗА. В этом случае анализатор в указанной схеме обеспечивает только замеры следующих временных характеристик срабатывания:

1. Время передачи GOOSE-сообщения от устройства РЗА контроллеру выключателя.

2. Время от момента получения контроллером выключателя команды аварийного отключения до момента отключения выключателя.

При этом контролируется, в основном, только способность контроллера выключателя и самого выключателя обеспечить быстрое аварийное отключение.

5.3.11. Программно-аппаратное резервирование компонентов ПАК ЦПС. Резервирование устройств IED является основным средством повышения надежности ПАК ЦПС. Под программно-аппаратным резервированием устройства IED понимается резервирование одного устройства IED (резервируемого) одним или более другими устройствами IED (резервными). При этом резервируемые и резервные устройства IED должны быть взаимозаменяемыми и выполнять идентичные функции.

В ЦПС для резервирования устройств IED применяются следующие способы резервирования в соответствии с ГОСТ 27.002:

1. Резервирование замещением.

2. Скользящее резервирование.

3. Постоянное резервирование.

Термины «резервирование замещением», «скользящее резервирование» и «постоянное резервирование» – в соответствии с ГОСТ 27.002.

Для устройств IED, обеспечивающих функции релейной защиты и резервируемых способом постоянного резервирования, возможны два варианта применения постоянного резервирования:

– параллельное резервирование;

– резервирование «с голосованием».

5.3.12. Резервирование коммуникационной сети ЦПС. В коммуникационной сети АСУ ТП ЦПС применяются следующие механизмы программно-аппаратного резервирования:

– дублирование отдельных сегментов коммуникационной сети ЦПС;

– обеспечение резервных «линков», коммутаторов, маршрутизаторов в коммуникационной сети (в рамках одного сегмента коммуникационной сети).

При этом в коммуникационной сети с дублированием отдельных сегментов и/или с обеспечением резервных «линков», коммутаторов и маршрутизаторов в рамках одного сегмента коммуникационной сети обеспечивается протокольная поддержка указанных резервных структур (протоколы RSTP (IEEE 802.1D), PRP и HSR (IEC 62439-3) и т.п.).

Способы и механизмы резервирования коммуникационной сети АСУ ТП ЦПС описаны в главе 1.

5.3.13. Резервирование сети и серверов синхронизации времени. Требования к резервированию сети и серверов синхронизации времени приведены выше в разделе требований к системе обеспечения единого времени и подсистеме инструментальной синхронизации.

5.3.14. Система управления надежностью ПАК ЦПС. Применение системы управления надежностью ПАК ЦПС в соответствии со стандартами серии ГОСТ Р 51901 имеет целью обеспечение своевременных операций по техническому обслуживанию и ремонтам оборудования ПАК ЦПС для поддержания требуемого уровня надежности ЦПС.

Система управления надежностью ПАК ЦПС выполняет следующие функции:

1. Сбор данных об отдельных повреждениях и отказах компонентов ПАК ЦПС и функциональных подсистем ЦПС из систем самодиагностики и внешней автоматизированной диагностики, функциональной диагностики ПАК ЦПС.

2. Анализ текущих показателей надежности ПАК ЦПС (в том числе отдельных программно-аппаратных компонентов и подсистем ПАК ЦПС, отдельных функциональных подсистем ЦПС).

3. Формирование очередей заявок на проведение восстановлений (ремонтов) компонентов ПАК ЦПС по данным о повреждениях и отказах программно-аппаратных компонентов/подсистем ПАК ЦПС.

5.3.15. Информационная безопасность. В рамках данного раздела освещены вопросы обеспечения информационной безопасности (ИБ) цифровой подстанции (ЦПС).

Необходимость в обеспечении ИБ ЦПС связана:

– с ростом общей информатизации энергообъекта;

– с переходом к подстанциям без постоянного присутствия персонала;

– с низким уровнем ИБ традиционных подстанций.

При построении информационной безопасности ЦПС особое внимание нужно уделять следующим потенциальным угрозам (см. IEC 62351-1): неосторожность персонала, отключение (обход) защиты, нарушение политики авторизации, компрометация канала связи («Man-in-the-middle»), атаки типа «Отказ в обслуживании» (DoS), действие вредоносного программного обеспечения («компьютерные вирусы», «черви» и т.д.).

Для обеспечения информационной безопасности должны использоваться как технические средства, так и организационные меры.

В рамках данного раздела применяются термины и определения, принятые IEC 62351-1, ГОСТ 34.10-2001 и Р 50.1.053–2005, если не указано иное.

5.3.16. Информационная модель информационной безопасности ЦПС. При построении системы ИБ группы ЦПС следует использовать иерархическую структуру обеспечения информационной безопасности, включающую в себя: удостоверяющий центр, головной сервер ИБ, серверы ИБ уровня ЦПС, объекты доступа (IED) (рис. 5.8) [2].

В задачи системы ИБ ЦПС включается обеспечение безопасности информационного обмена между устройствами (IED-ами) и пользователями системы. Безопасность должна быть обеспечена для всех видов информационного обмена (штатный информационный обмен, конфигурирование, администрирование и т.д.). Система ИБ ЦПС функционирует на основании предоставленного головным сервером ИБ МЭС объема достоверных данных.

Механизмами обеспечения ИБ в рамках ЦПС являются:

– использование цифровых сертификатов (далее сертификатов), включающих в себя открытый ключ проверки и закрытый ключ подписи;

– использование ЭЦП для обеспечения достоверности и подлинности;

– прочие аппаратные и программные решения по защите встраиваемого и автономного программного обеспечения, используемого в рамках ЦПС.

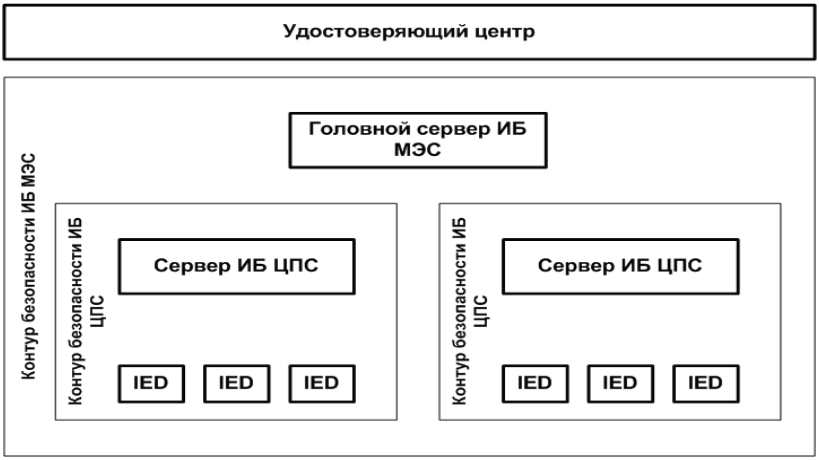


**Рис. 5.8. Общая структура ИБ**

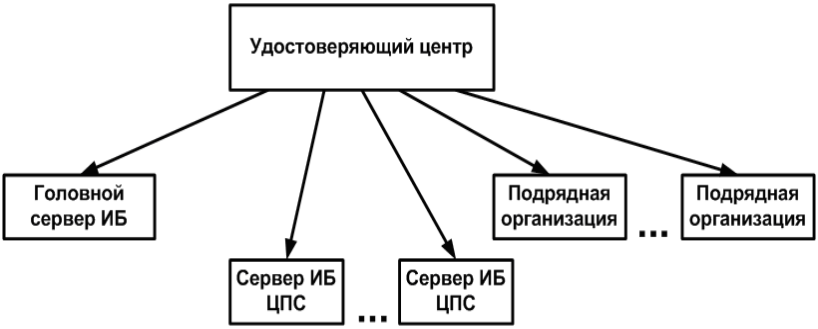


**Рис. 5.9. Схема распространения ключей подписи**

Задача удостоверяющего центра – формирование цифровых сертификатов для всех участников информационного обмена ЦПС (рис. 5.9) [2]. Структура цифрового сертификата приведена в RFC 3280.

Для установления безопасного канала каждая из сторон должна обладать:

– ключом подписи (конфиденциальные данные);

– достоверными данными о принадлежности ключа проверки другой стороне информационного обмена.

Удостоверяющий центр обладает достоверной информацией о ключах проверки других сторон, так как он осуществляет выдачу этих ключей. Другим участникам информационного обмена достоверная информация о принадлежности ключа проверки данного удостоверяющего центра передается совместно с их собственным ключом подписи.

Производителем должен быть предусмотрен защищенный механизм записи сертификата устройства, позволяющий эксплуатационной организации производить его замену.

Сертификат для оборудования формируется удостоверяющим центром. Ключ подписи в рамках каждого устройства должен быть уникальным, рекомендуется производить регулярные проверки сертификатов.

По скомпрометированным сертификатам должна быть проведена работа по замене сертификатов устройств со скомпрометированным сертификатом, а также проведено внесение скомпрометированного сертификата в списки отозванных сертификатов на каждом сервере ИБ ЦПС.

Головной сервер ИБ осуществляет распространение/тиражирование открытых данных сертификатов (рис. 5.10) [2].

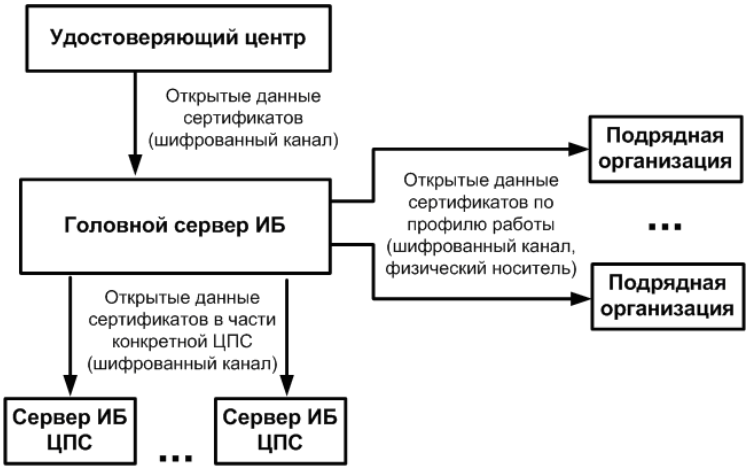


**Рис. 5.10. Схема распространения открытых данных**

Данные с головного сервера ИБ передаются на сервера ИБ ЦПС, в части объектов доступа ЦПС и в части субъектов доступа, допущенных к работе на данной ЦПС. В рамках защиты ИБ ЦПС должен быть обеспечен единый механизм защиты от несанкционированного подключения к коммуникационной среде. Следует использовать механизм, предусмотренный IEEE 802.1X. Поддержка IEEE 802.1X должна быть предусмотрена как в коммуникационном оборудовании, так и в конечных устройствах, подключаемых к сети ЦПС.

5.3.17. Сервер ИБ уровня ЦПС. В составе сервера ИБ ЦПС должны быть реализованы следующие сервисы:

– RADIUS/DIAMETER (RFC 2865/RFC 3588) сервер аутентификации подключения к коммуникационной сети ЦПС;

– Центр управления сертификатами.

Должна быть обеспечена надежность сервера ИБ ЦПС (бесперебойное питание, подключение к коммуникационной среде). Не допускается размещение сервера ИБ ЦПС за пределами ЦПС. Для корректного выполнения функции контроля сроков действия сертификатов сервер ИБ ЦПС подключать к серверу ведения единого времени по схеме с обязательной аутентификацией (обеспечить достоверность данных времени).

5.3.18. Модель потоков данных. В рамках ЦПС выделяются следующие типы защищаемых потоков данных:

– данные, передаваемые поверх TCP/IP: информационный обмен с использованием сервисов MMS (ISO 9506-1, ISO 9506-2), конфи-

гурирование IED с использованием SCL (IEC 61850-6) файлов, FTP (RFC 959) и т.д.

– данные, передаваемые поверх UDP: протоколы синхронизации времени SNTP (RFC 2030), NTP (RFC 5905), PTP (IEC 61588);

– данные, передаваемые непосредственно поверх кадров Ethernet: быстродействующие управляющие воздействия (GOOSE-сообщения), потоки мгновенных значений (SV 9.2).

Не допускается использование закрытых (фирменных) протоколов передачи данных без обеспечения аналогичного уровня информационной безопасности.

Защита данных, передаваемых поверх TCP/IP, обеспечивается средствами криптографического протокола TLS (Transport Layer Security) не ниже версии 1.0 (RFC 2246). Не допускается неограниченное использование выбранного симметричного ключа. Симметричные ключи должны пересматриваться по истечении определенного времени либо количества переданных/полученных байт. Инициатива по смене симметричного шифра должна исходить от устройства, получившего запрос на соединение, команды по смене шифра, получаемые от устройств, инициирующих соединения, должны быть проигнорированы.

В устройствах также должен быть предусмотрен конфигурируемый тайм-аут на операцию по смене шифра, по истечении тайм-аута должен производиться разрыв соединения. Поверх UDP допускается передача трафика протоколов SNTP, NTP либо PTP. В качестве источника точного времени допускается использовать сервер с поддержкой NTP версии не ниже 4. Для обеспечения достоверности сервера для клиента необходимо использовать механизм автоключей (RFC 5906) либо шифрование по MD5 (RFC 1321).

Защиту NTP сервера в части атак на отказ в доступе (DoS) следует реализовать средствами коммуникационной среды (ограничения на используемый канал) либо механизмом «Kiss-o-Dead» (NTPv4). В рамках сервера точного времени предусмотреть поддержку клиентов, не поддерживающих процесс аутентификации. В случае обнаружения сервером NTP атаки на отказ в доступе блокировать данных клиентов. Поверх Ethernet допускается только трафик протокола IEC 61850: GOOSE-сообщения, поток данных по стандарту IEC 61850-9.2 (SV). При передаче данных в виде потока данных по стандарту IEC 61850-9.2 и GOOSE-сообщений использовать пакеты расширенной структуры (Extended PDU согласно IEC 62351-6), содержащие контрольную сумму пакета и ЭЦП данных.

К защите ключа подписи источника данных предъявляются требования, аналогичные требованиям к защите ключа подписи устройства. В рамках приемников потока данных по стандарту IEC 61850-9.2 допускается проводить выборочную проверку пакетов, но не менее 1 проверки в секунду.

Для приемников GOOSE-сообщений требуется проверка всех получаемых сообщений. Для обеспечения защиты от воспроизведения записанного ранее сообщения (replaying) включить в передаваемые сообщения метки времени.

5.3.19. Модель прав пользователей. Модель прав пользователей должна быть построена на основании положений системы управления доступом на основе ролей (RBAC).

В базовую модель прав пользователей должны быть включены следующие роли и соответствующие им права (табл. 5.4) [2].

**5.4. Роли и права пользователей в базовой модели**

| Наименование роли | Права роли | Типовые пользователи роли |
|---|---|---|
| Пользователь | Чтение данных.<br>Управление оборудованием | Диспетчер, оперативный персонал подстанции, автоматизированные системы |
| Технический специалист | Все права пользователя (кроме управления оборудованием).<br>Изменение данных за исключением конфигурационных настроек, связанных с коммуникацией, авторизацией | Персонал, выполняющий монтажные, пуско-наладочные, ремонтные работы |
| Администратор | Все права технического специалиста, а также права на изменение конфигурационных настроек, связанных с коммуникацией, авторизацией | Администратор сети |

Назначение прав пользователям должно производиться с предоставлением минимума прав, необходимого для выполнения работ. Используемое в рамках ЦПС оборудование должно содержать минимальную базовую модель прав пользователей с указанными выше правами. Экземпляром роли называется профиль доступа, обладающий правами данной роли в части конкретного перечня оборудования.

Формирование экземпляров роли следует осуществлять в рамках выполнения конкретной функциональной задачи. Каждый экземпляр роли характеризуется перечнем оборудования, правами доступа к нему. Для каждого экземпляра роли формируется индивидуальный уникальный сертификат.

5.3.20. Модель обеспечения защиты от действия вредоносного программного обеспечения. Для устройств, функционирующих под управлением свободно распространяемых операционных систем (семейство Windows, Unix, Linux и т.д.), требуется обязательное применение антивирусного программного обеспечения. Поддержка актуальности антивирусных баз возлагается на сервер ИБ ЦПС.

Решение по антивирусной защите должно быть унифицированным в рамках ЦПС. Действия антивирусной защиты не должны оказывать влияние на выполнение технологических функций, предусмотренных для устройства.

Решение по защите устройств под управлением прикладных операционных систем определяется на основании анализа существующих угроз (наличие вредоносного ПО) и технических возможностей платформы.

Обновление антивирусных баз должно проводиться регулярно и с максимально возможной оперативностью. Передача антивирусных баз должна осуществляться по шифрованному каналу связи.

5.3.21. Требования к защите от несанкционированного доступа к информации. Для аутентификации пользователя используется инфраструктура открытых ключей (PKI, согласно X.509, RFC 1422). Применение системы паролей допускается только при локальном доступе (при ПНР и ремонтно-восстановительных работах).

Контроль сроков действия сертификатов осуществляется сервером ИБ ЦПС. Сервером ИБ контролируется не только срок окончания действия сертификата, но и время его начала.

Все операции, связанные с изменением данных авторизации, попытками несанкционированного доступа должны фиксироваться в журнале событий объекта.

В рамках информационного ресурса должна быть предусмотрена защита от кибератак типа «подбор пароля/сертификата путем перебо-

ра». Для этой цели производителем определены: максимальное количество неудачных попыток авторизации, время, в течение которого ведется учет неудачных попыток авторизации, время недоступности устройства при достижении данного количества неудачных попыток за указанное время.

На уровне сервера ИБ ЦПС должно производиться чтение системных журналов событий на предмет аномально большого количества неудачных авторизаций.

Оперативный контроль за кибератаками типа «подбор путем перебора» должен осуществляться с помощью анализа данных, полученных от логических узлов GSAL (generic security application), каждого из IED-ов (см. IEC 61850-7-4). Поддержка данного логического узла является обязательной для всех объектов доступа.

Схема компрометации сертификата должна подразумевать иерархическую систему, т.е. при компрометации сертификата высокого уровня компрометируются пароли, доступ/изменение которых возможно при использовании скомпрометированного сертификата.

Субъект доступа при установлении соединения с объектом доступа подтверждает свою подлинность по следующей схеме (рис. 5.11) [2]:

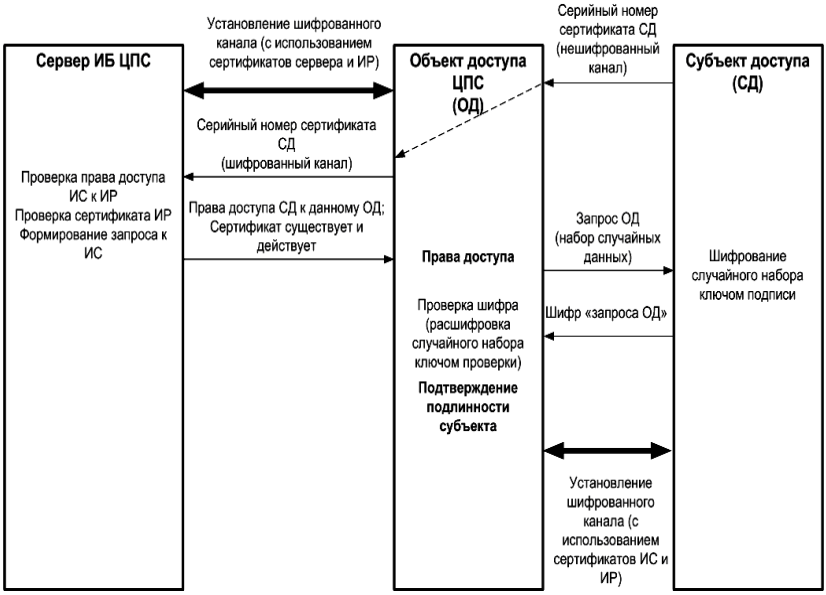


**Рис. 5.11. Схема использования сертификатов**

Субъект доступа осуществляет аналогичные операции для подтверждения подлинности объекта доступа. В рамках устройства рекомендуется производить кэширование сертификатов с целью снижения количества обращений к серверу ИБ ЦПС. Длительность хранения сертификатов не более 8 часов. Не допускается использование сертификатов с неограниченным сроком действия. В рамках системы ИБ следует предусмотреть механизм отзыва сертификатов, соответствующий требованиям RFC 3280.

Не допускается установление соединения с просроченным или отозванным сертификатом. В случае выхода срока сертификата при установленном соединении разрыв соединения по данной причине не допускается.

5.3.22. Требования к аппаратной и программной защите алгоритмов и настроек IED. В рамках обеспечения ИБ рекомендуется применять синтез аппаратных, программных и организационных средств защиты.

Аппаратная защита должна включать в себя несколько уровней:

– защиту конфигурационных параметров, допускающих изменение в процессе эксплуатации;

– защиту конфигурационных параметров и алгоритмов работы устройства, не допускающих изменение в процессе эксплуатации и определяемых на этапе производства устройства.

Производителем устройств не должны предусматриваться операции по обслуживанию IED, требующие нарушения пломбы производителя. Физическое пломбирование рекомендуется дополнять электронными пломбами, дублирующими и дополняющими аппаратные средства защиты. Состояние электронных пломб должно быть доступно через информационный интерфейс устройства.

Защита конфигурационных параметров, допускающих изменение в процессе эксплуатации, обеспечивается защитой от несанкционированного доступа. Перечень указанных конфигурационных параметров определяется производителем и должен быть приведен в эксплуатационной документации на устройство. Факты и время изменения конфигурационных параметров должны фиксироваться в системном журнале устройства, при наличии технической возможности рекомендуется дополнительно фиксировать содержание изменений.

Защита конфигурационных параметров, не допускающих изменение в процессе эксплуатации, должна обеспечиваться методами аппаратной защиты. К операциям, не допускающим выполнение в процессе эксплуатации, относятся операция калибровки измерительного устройства, изменение уникального идентификатора устройства (серийный номер, MAC адрес и т.д.) и аналогичные им операции, не предусмотренные штатным процессом эксплуатации устройств.

Защиту алгоритмов работы устройства (встроенного программного обеспечения) рекомендуется проводить синтезом аппаратных и программных средств.

Обновления программного обеспечения требуется разделять на два типа:

– информационные – затрагивают только информационную часть (реализацию протоколов передачи данных), исправление ошибок и расширение функций;

– технологические – принципиально изменяющие функциональное назначение устройства либо меняющие его метрологические или основные технические свойства.

Информационные обновления не должны требовать срыва аппаратной пломбы производителя. Решение о применении информационных обновлений должно приниматься на основании критичности устраненных в нем ошибок, актуальности новых функций, внесенных в обновление. При отсутствии потребности в обновлении рекомендуется ПО не обновлять.

Применение технологических обновлений должно выполняться с соблюдением принятых регламентов проверки данного типа оборудования.

Производитель должен иметь специализированный сертификат для обновления ПО. Ключ проверки данного сертификата записывается в каждое устройство производителя. Конфиденциальность ключа подписи обеспечивает производитель.

Обновления программного обеспечения, выпускаемые производителем, должны быть подписаны ключом подписи сертификата обновления. Файл обновления должен содержать тип оборудования, для которого он предназначен, версии ПО которого допускается заменять данным файлом.

Файл обновления, переданный на устройство, должен проходить этап верификации (проверка целостности файла обновления, подлинности назначения файла обновления, допустимости обновления). Файл обновления, не прошедший указанные проверки, не должен применяться устройством.

В составе обновления может содержаться новый ключ проверки сертификата обновлений производителя.

Обновление программного обеспечения осуществляется по шифрованному каналу. Коммуникационный доступ осуществляется с помощью сертификата с уровнем не ниже администратора системы ИБ.

5.3.23. Требования к защите метрологического ядра IED. В рамках данного раздела применяются термины и определения в соответствии с МИ 2891-2004.

Выделяется два типа метрологически аттестуемых устройств:

– устройства, выполняющие аналого-цифровые или цифро-аналоговые преобразования (устройства-преобразователи);

– устройства, выполняющие вычисления на основании цифровых данных и предоставляющие их в цифровом виде (устройства-вычислители).

Для устройств-преобразователей рекомендуется предусмотреть механизмы контроля целостности калибровочных параметров, а функцию проверки целостности включить в самодиагностику, выполняемую устройством на периодической основе.

Устройства-вычислители должны быть реализованы в виде комплекса, состоящего из аппаратной платформы и автономного программного обеспечения.

В автономном программном обеспечении должно быть проведено разделение программного обеспечения (согласно МИ 2891-94) на метрологическую (метрологическое ядро) и информационную части.

Рекомендуется предусматривать механизмы раздельного обновления метрологического ядра и информационной части автономного ПО.

Номер версии автономного ПО должен состоять из двух частей: версия метрологического ядра и версия информационной части. Способ формирования версии метрологического ядра приведен в МИ 2891.

Обновление информационной части производится с соблюдением требований к применению информационных обновлений.

Метрологическое ядро должно проходить сертификационные испытания и иметь действующий сертификат соответствия. В сертификате соответствия должна быть указана версия метрологического ядра.

Метрологическое ядро, прошедшее сертификационные испытания, подписывается ключом подписи сертификационного центра. Копия метрологического ядра хранится в сертификационном центре.

В автономном ПО должны быть предусмотрены механизмы защиты от сбоев (например, недостаток вычислительной мощности или потери коммуникационных пакетов SV). Факт сбоя при вычислении метрологической величины должен быть представлен в журнале качества соответствующего параметра (поле quality IEC 61850-7-3).

Обновление метрологического ядра допускается при предоставлении производителем сертификата на ПО новой версии.

В автономном ПО должны быть предусмотрены механизмы идентификации. Запуск механизма идентификации производится автоматически при запуске устройства и по команде пользователя. Реализация механизма идентификации относится к метрологическому ядру. Результаты идентификации должны быть доступны через локальный интерфейс (например, ЧМИ) и через коммуникационный интерфейс (удаленно).

Операция обновления метрологического ядра должна фиксироваться в журнале событий, доступном через удаленные интерфейсы.

Версия ПО должна включаться в объем данных, защищаемых электронной цифровой подписью (ЭЦП) производителя (сертификат обновлений).

5.3.24. Требования к защите конфигурационных параметров IED. В рамках данного подраздела под конфигурационными параметрами IED понимаются конфигурационные параметры, допускающие изменение в процессе эксплуатации, если не указано иное.

Для групп конфигурационных параметров, требующих одновременности вступления их в действие, рекомендуется использовать механизм «набора конфигурационных параметров» (setting group, согласно IEC 61850-7-2).

Изменение конфигурационных параметров в рамках IED должно производиться с использованием файлов SCL. Процесс конфигурирования должен быть основан на использовании SCL control block (см. IEC 61850-8.1, приложение D).

5.3.25. Требования к документированию и демонстрации функциональных возможностей IED. Для обеспечения защиты от угроз ЦПС коммерческого характера должно быть обеспечено унифицированное документирование функций устройств. Для данной цели требуется предоставление следующих документов:

– PICS (protocol implementation conformance statement) – описание реализации протокола, содержащее поддерживаемые информационные сервисы;

– MICS (model implementation conformance statement) – описание логических узлов, характеризующих функции устройства;

– PIXIT (protocol implementation extra information for testing) – описание реализации протокола IEC 61850, содержащее дополнительные сведения по испытаниям, а также описание принятых решений по известным ошибкам, недочетам, неточностям, выявленным после публикации действующей версии стандарта;

– ICD (IED capability description) – файл устройства в формате SCL (расширение формата XML), представляющий в машинной форме данные, содержащиеся в предыдущих документах.

Для повышения качества ПНР производителю рекомендуется предоставление программного эмулятора работы устройств.

Целесообразно создать открытую техническую библиотеку файлов PICS, MICS, PIXIT, ICD различных производителей, производителям обеспечить доступ к данной библиотеке с возможностью обновления данных, проектным организациям доступ на чтение данных.

5.3.26. Требования к защите от ошибок конфигурирования коммуникационной части IED. При выполнении конфигурирования коммуникационной части IED существуют следующие потенциальные угрозы:

– отказ функционирования коммуникационной среды;

– отказ в функционировании стороннего устройства в связи с повышенным объемом трафика, адресованного данному устройству, в связи с некорректной настройкой источника данных;

– отказ в функционировании устройства в связи с получением излишнего трафика, в связи с некорректной настройкой источника данных;

– недоступность устройства через коммуникационную среду.

Мерами противодействия данному виду угрозы являются:

– корректная политика производителя в части коммуникационных настроек, включая настройки по умолчанию;

– устойчивость IED к избыточному трафику;

– выполнение функции самоконтроля корректности коммуникационных параметров перед их применением.

5.3.27. Защита от генерации избыточного (паразитного) трафика. В рамках данного подраздела избыточным (паразитным) трафиком называются коммуникационные пакеты, не предусмотренные проектными решениями, сообщения и данные, не используемые либо используемые некорректно.

Базовым механизмом защиты от избыточного трафика является блокирование коммуникационных пакетов с настройками по умолчанию, запрет любого типа трафика, за исключением предусмотренного проектными решениями.

К коммуникационному оборудованию предъявляются симметричные требования – фильтрация пакетов, обладающих признаками трафика, генерируемого устройством со значениями по умолчанию.

На получателей данных возлагаются задачи проверки значений конфигурационных параметров источника, перед включением соответствующих блоков управления (GSEControl и SampledValueControl, IEC 61850-7-2).

Ко всем устройствам, функционирующим в рамках ЦПС, предъявляются требования селективности и устойчивости. Селективность устройства к получаемым данным подразумевает у него наличие конфигурационных параметров, уникальным образом характеризующих корректность источника данных (MAC адресата, уникальный идентификатор – например MsvID для SV, AppID для GOOSE). Данные, не соответствующие данным характеристикам, должны игнорироваться. Устойчивость IED к избыточному трафику подразумевает корректность функционирования устройства при получении коммуникационных пакетов, отличающихся по количеству и содержанию от пакетов, предусмотрен-

ных производителем для штатной работы (например, получение измерительного потока SV устройством РЗА, рассчитанным на получение SV со значительно меньшим количеством пакетов в секунду).

5.3.28. Защита от ошибок при конфигурировании коммуникационных параметров. В части защиты от ошибок при конфигурировании выступают следующие механизмы:

– функция самоконтроля конфигурационных параметров – устройство производит проверку на корректность введенного параметра;

– встроенные сервисные функции по проверке коммуникационных настроек – предоставление пользователю возможности установить тестовое соединение и получить подтверждение корректности настроек (например, в части соединения с NTP сервером);

– механизм отката конфигурации – функциональность, позволяющая избежать случаев коммуникационной недоступности устройства, возникающих в силу ошибок коммуникационных параметров.

Производителям устройств рекомендуется реализовать функцию расширенного самоописания: устройство выступает источником информации о своих технических характеристиках, содержит минимально необходимую часть руководства по эксплуатации. В качестве технической реализации функции рекомендуется использовать встроенный в IED WEB-сервер.

5.3.29. Требования к защите от ошибок при конфигурации технологических параметров. В рамках ЦПС должен применяться единый инструмент конфигурирования на базе языка SCL (IEC 61850-6).

Перед началом монтажных работ рекомендуется проводить испытания с использованием созданного файла подстанции и программных эмуляторов устройств. В составе испытаний имитировать штатный режим работы и аварийные ситуации.

Файл подстанции должен быть заварен ЭЦП специализированного технического центра. Не допускается выполнение пуско-наладочных работ без наличия файла конфигурации подстанции, заверенного ЭЦП.

В ТЗ генерального проектировщика рекомендуется включать требования по предоставлению ICD-файлов устройств, заложенных в спецификацию оборудования. При наличии технической компетенции генерального проектировщика также рекомендуется включать требования к разработке файла конфигурации подстанции в рамках проектной документации на ЦПС.

В архитектуру устройств рекомендуется включить поддержку механизмов посылки и обработки тестовых сообщений (см. IEC 61850-7-2, раздел 6 Common data attribute types). Механизм тестовых сообщений должен быть поддержан для данных, используемых в рамках выполне-

ния базовой функциональности устройства (Functional Constraints (FC) – ST, SV, MX, CO, согласно IEC 61850-7-4).

5.3.30. Требования к обеспечению информационной безопасности при подключении к удаленному клиенту. При удаленном доступе к ресурсам ЦПС следует использовать механизмы аутентификации, описанные в данном разделе ранее. Удаленный клиент вместо сервера ИБ ЦПС должен использовать подключение к головному серверу ИБ.

В зависимости от требований к временным задержкам при передаче оперативных данных должны применять: ЭЦП для данных, передаваемых с минимальными задержками, и шифрование для данных, допускающих задержки на шифрование и расшифровку.

Рекомендуется на уровне межподстанционного шлюза ограничить перечень клиентов, которым разрешен удаленный доступ к ресурсам ЦПС (на уровне IP-адресов или MAC-адресов).

Если при передаче данных используется протокол ГОСТ Р МЭК 60870-5-104, для обеспечения информационной безопасности рекомендуется использовать решения IEC 62351-5.

5.3.31. Требования к обеспечению информационной безопасности при выполнении работ на ЦПС сторонними организациями. Информационный доступ к ресурсам ЦПС представителей сторонних организаций осуществляется с использованием описанных ранее механизмов аутентификации (системы сертификатов). Выдачу временного сертификата для выполнения работ на ЦПС рекомендуется осуществлять на специализированном физическом носителе, не допускающем тиражирование сертификата. Срок действия сертификата должен быть согласован со сроком начала и сроком окончания работ. По окончании работ физический носитель должен быть возвращен подразделению службы ИБ, допустившему стороннюю организацию к работам. Подразделения служб ИБ обязаны вести журнал выдачи/сдачи физических носителей цифровых сертификатов.

5.3.32. Комплексная безопасность. В рамках ЦПС должен быть обеспечен высокий уровень комплексной (инфраструктурной безопасности). Переход к необслуживаемым (без постоянного присутствия персонала) подстанциям повышает требования к реализации следующих подсистем системы комплексной безопасности:

- охранно-пожарная сигнализация;
- охранное видеонаблюдение;
- система контроля доступа на объект;
- технологическое видеонаблюдение;
- вспомогательные подсистемы (метеорологическое наблюдение, система освещения подстанции и т.д.).

В рамках ЦПС к данным системам предъявляются дополнительные требования в следующей части:

– подсистемы должны иметь интерфейс для интеграции в общее информационное пространство ЦПС;

– проектирование ЦПС должно вестись комплексно, т.е. с учетом не только технологических функций ЦПС, но и требований системы комплексной безопасности.

С целью интеграции подсистем в информационное пространство ЦПС должны применяться специализированные контроллеры, отражающие диагностические данные (работоспособность, режим работы) как самой подсистемы, так и ее модулей.

Для части подсистем должен быть предусмотрен обмен оперативной информацией, т.е. контроллеры генерируют информационные сигналы, которые учитываются в технологическом процессе.

Подсистемы должны использовать общую коммуникационную сеть для передачи собственных данных.

5.3.33. Охранно-пожарная сигнализация. Передачу данных охранно-пожарной сигнализации рекомендуется производить по основному технологическому каналу и резервировать беспроводным каналом передачи данных.

В части пожарной сигнализации рекомендуется предусмотреть информационный обмен с системами РЗА и ПА, связанный с выборочным отключением силового оборудования при возникновении пожара. Рекомендуемый механизм информационного взаимодействия GOOSE-сообщения – согласно IEC 61850-8.1.

5.3.34. Система контроля доступа. Для ПС без постоянного обслуживающего персонала основное внимание должно быть уделено средствам, препятствующим проникновению на охраняемый объект и к центрам его управления. Системы контроля доступа должны выполняться для нескольких зон (внешний периметр, вход в здание, вход в помещение). Системы должны иметь автономное питание, постоянную связь с централизованными охранными организациями и МЧС.

Рекомендуется обеспечить информационное взаимодействие системы контроля доступа с системой охранного видеонаблюдения в части долговременной видеорегистрации факта доступа на ТП.

5.3.35. Охранное видеонаблюдение. Режим функционирования системы охранного видеонаблюдения – без постоянного наблюдения. Цели создания охранного видеонаблюдения: регистрация нарушений, верификация сигналов охранно-пожарной сигнализации.

Рекомендуется использование IP-видеокамер. Передача данных должна производиться по волоконно-оптическим кабелям в рамках общей коммуникационной сети ЦПС.

При проектировании схем прокладки волоконно-оптических кабелей рекомендуется закладывать дополнительные оптические волокна для целей охранного и технологического видеонаблюдения.

Функционирование камер охранного видеонаблюдения не должно зависеть от работоспособности системы освещения. В связи с этим рекомендуется использовать видеокамеры с автоматическим переключением на «ночной» режим (использование светочувствительных камер или камер со встроенными ИК-прожекторами). При проектировании системы охранного видеонаблюдения следует принять меры по защите от засветки видеокамер системой освещения, фарами автомобилей (размещение, АРД и т.д.).

Зона видеонаблюдения охранных видеокамер должна охватывать весь периметр энергообъекта. При проектировании необходимо учесть расположение зданий и лесопосадок для исключения появления мертвых зон. Особое внимание обратить на места санкционированного проникновения на территорию подстанции (калитки, ворота).

При проектировании необходимо предусмотреть математическое обеспечение в части расчетов МРД (минимальное различение детали) по Р 78.36.008-99. Для видеокамер, контролирующих периметр, следует обеспечить МРД по горизонтали не менее 15 (функциональная задача «различение»), для видеокамер, контролирующих места санкционированного проникновения на территорию подстанции, МРД не менее 2 (функциональная задача «идентификация»).

Для видеосервера ЦПС рекомендуется предусмотреть выполнение автоматизированной функции формирования видеоархивов юридически ценной информации. В рамках выполнения данной функции для массивов видеоинформации, имеющих юридическую или административную ценность, следует обеспечить достоверность и целостность данных, используя механизм формирования контрольной суммы и подпись ЭЦП.

Для охранного видеонаблюдения рекомендуется использование одностороннего аудиоканала (от камеры к серверу).

5.3.36. Технологическое видеонаблюдение. Режим функционирования системы технологического видеонаблюдения – без постоянного наблюдения.

Цели создания технологического видеонаблюдения: визуальное подтверждение состояния коммутационных аппаратов, удаленный видеоконтроль работы выездных бригад, визуальная диагностика силового оборудования и контактных соединений (при тепловизионном контроле).

Требования к видеокамерам общего технологического видеонаблюдения аналогично требованиям к видеокамерам охранного видеонаблюдения.

Для сокращения количества оборудования рекомендуется использовать управляемые поворотные системы для видеокамер.

Технологическое видеонаблюдение должно обеспечивать удаленный контроль положения разъединителей.

Рекомендуется предусмотреть тепловизионное видеонаблюдение основных силовых аппаратов и наиболее важных контактных соединений (например, в части высшего напряжения).

В рамках технологического видеонаблюдения рекомендуется выборочное использование двухстороннего аудиоканала.

В рамках тепловизионного наблюдения рекомендуется предусмотреть автоматизированную функцию сигнализации, основанную на алгоритмах распознавания видеосигнала.

5.3.37. Система освещения. Для подстанций без постоянного присутствия персонала следует предусмотреть минимальный объем постоянного освещения в ночное время суток. Объем определяется исходя из требований ГО. Прочее освещение рекомендуется выполнять удаленно управляемым с возможностью локального управления и локальной блокировки удаленного управления.

В рамках системы уличного освещения рекомендуется использование светодиодных осветительных приборов.

5.3.38. Вспомогательные системы. Результаты работы вспомогательных систем должны быть интегрированы в общее информационное пространство ЦПС посредством протокола IEC 61850.

В рамках ЦПС рекомендуется создание не менее двух точек контроля состояния окружающей среды (температура, влажность и т.д.): в ОРУ и ОПУ. Данные измерения данной системы должны быть доступны в рамках IED с поддержкой логических узлов MMET, MENV, MHYD (согласно IEC 61805-7-4). Полнота поддержки данных логических узлов определяется требованиями системы к объему данного вида неоперативной технологической информации.

В состав ЦПС должна быть включена подсистема контроля работоспособности системы отопления и вентиляции. Данная функция должна быть реализована в виде логического узла CCGR (согласно IEC 61805-7-4). При размещении оборудования в телекоммуникационных стойках (в ОПУ) рекомендуется обеспечить контроль работоспособности локальной системы охлаждения. Для интеллектуальных устройств, размещаемых в ОРУ, рекомендуется обеспечить контроль условий эксплуатации (в части температуры и работоспособности вспомогательных подсистем охлаждения и обогрева).

Итак, можно отметить, что сферой действия данной методологии являются электрические подстанции ЕНЭС, как правило, с напряжением 220 кВ и выше, при создании или комплексной реконструкции и

техническом перевооружении которых предполагается внедрение ЦПС. Однако данная концепция актуальна и для подстанций других классов напряжения с микропроцессорными устройствами, напрямую работающими на базе протоколов IEC 61850-8.1 и 61850-9.2, и прежде всего в тех случаях, когда речь идет о внедрении на этих подстанциях полноценных программно-аппаратных комплексов.

## Выводы

1. Инфраструктура передачи информации – кибернетический архитектурный элемент ЦСП – с физической структурой из различных компонентов (структурированные кабельные системы, активное оборудование и др.) и логической структурой, включающей терминальные (передатчики и приемники данных) и сетевые элементы (станционную и технологическую шины и др.).

2. Общее (системное) программное обеспечение на основе средств организации внутрисистемных, внесистемных коммуникаций и операционных систем реального времени обеспечивает функционирование АСУ ТП в целом, а технологическое **(**специальное) ПО с совокупностью отдельных программных компонентов (модулей или их комплексов), резидентных в устройствах разных уровней ПТК, решает задачи обработки информации и контроля, анализа, диагностики и управления.

3. Информационное обеспечение ЦПС на основе общей информационной модели CIM при взаимодействии с центрами управления позволяет создать единую информационную модель физического объекта (подстанции) в общей интегрированной среде большой системы – АСТУ ОАО «ФСК ЕЭС».

4. Метрологическое обеспечение ЦПС на основе структуры с измерительными, вычислительными и связующими компонентами, а также набора базисных принципов (вертикальная дифференциация и горизонтальная интеграция) позволяет организовать методы и способы, которыми достигаются единство и высокая точность измерений в измерительной системе.

5. Надежность ЦПС обеспечивается разработкой единой программы и определяется соответственно: надежностью компонентов; применением самодиагностики и функциональной диагностики оборудования; резервированием компонентов; регламентами проведения работ по техническому обслуживанию и ремонтами оборудования программно-аппаратного комплекса, эффективность адаптивной диагностики микропроцессорных средств ЦПС которых определяет информационная технология творчества, рассмотренная в шестой главе.