ЦИФРОВАЯ ПОДСТАНЦИЯ – ОБЪЕКТ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

В.М. ЗИНИН (ОАО “НИПОМ”),
А.М. ПОДЛЕСНЫЙ (ООО “ИнСАТ”),
В.Г. КАРАНТАЕВ (ОАО “ИнфоТеКС”)

В статье описываются необходимые требования, которые должны быть соблюдены при разработке цифровой подстанции, в том числе требования к информационной безопасности, а также представлено инновационное решение, удовлетворяющее рассматриваемым требованиям, разработанное совместными усилиями компаний ОАО “НИПОМ”, ООО “ИнСАТ”, ОАО “ИнфоТеКС” и ПАО “ИНЭУМ им. И.С. Брука”.

Ключевые слова: *цифровая подстанция (ЦПС), критическая информационная инфраструктура (КИИ), криптографические средства защиты информации (СКЗИ), несанкционированный доступ (НСД), процессор Эльбрус, ОС Эльбрус, MasterSCADA 4D, стандарт МЭК 61131-3, протокол МЭК 61850 (MMS).*

Используемые технологические решения единой энергетической сети (ЕЭС), созданной более 60 лет назад, по многим параметрам подходят к границе эксплуатационных возможностей. Согласно концепции развития ЕЭС, разработанной в 2011 году [1], следующим шагом может стать интеллектуальная система с активно-адаптивной сетью (ААС), в зарубежной терминологии – Smart Grid. Процесс повышения уровня автоматизации объектов ЕЭС уже идет, привнося новые технологии, применение которых порождает не только всевозможные сложности чисто технологической реализации, но и риски информационной безопасности.

Одной из важнейших составных частей концепции Smart Grid является цифровая подстанция (ЦПС). Под ЦПС понимается подстанция с высоким уровнем автоматизации управления, в которой практически все процессы информационного обмена как между элементами ЦПС, так и с внешними системами, а также управления работой ЦПС осуществляются в цифровом виде на основе протоколов МЭК, в частности по открытому объектно-ориентированному стандарту МЭК 61850. В соответствии с данным стандартом устройства должны поддерживать (рис. 1): возможность приема выборок мгновенных значений (Simpled Values), аналоговых сигналов токов/напряжений, возможность публикации/подписки на GOOSE-сообщения, возможность информационного обмена по технологии “клиент-сервер” по протоколу MMS. MMS работает поверх стека TCP, что влияет на скорость передачи данных, поэтому MMS зачастую используется для решения задач по передаче не критичных к задержкам данных, например передачи команд телеуправления, сбора данных телеизмерений и телесигнализации и их передаче в верхний уровень – SCADA-системы. В отличие от MMS-протокола, GOOSE, наоборот, может использоваться для передачи “быстрых сигналов”, например команд отключения выключателя от защиты, за счет того, что данные в этом протоколе назначаются непосредственно в кадр Ethernet в обход стека TCP [2].

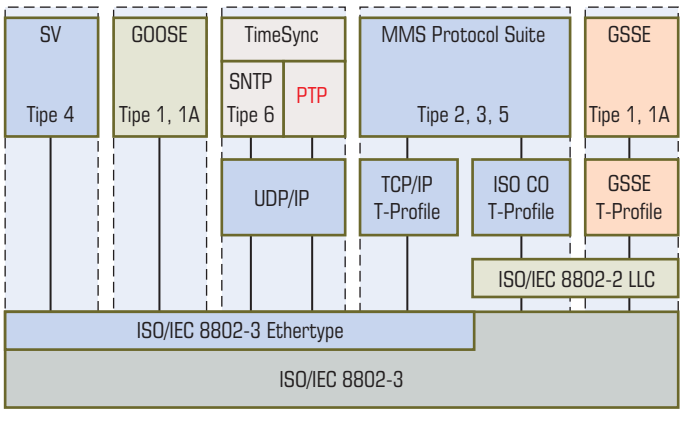

Рис. 1. Обзор функциональности и профили в соответствии с МЭК 61850-8-1

Вновь создаваемые программно-аппаратные комплексы, такие как цифровая подстанция, должны соответствовать действующим нормативно-правовым актам РФ, а также учитывать лучшие мировые практики построения систем киберзащиты.

Удовлетворяющая сформулированным требованиям ЦПС должна иметь высокотехнологичные средства защиты от кибератак, поскольку она в первую очередь является объектом критической информационной инфраструктуры (КИИ), о чем свидетельствует проект Федерального закона № 47571-7 “О безопасности КИИ Российской Федерации”, рекомендованный Комитетом Государственной Думы по энергетике и принятый в первом чтении 27 января 2017 года. Этот законопроект определяет основные принципы госрегулирования в сфере защиты КИИ страны в целях ее устойчивого функционирования при компьютерных атаках. Он был разработан с целью реализации “Доктрины информационной безопасности Российской Федерации”, утвержденной Президентом России 5 декабря 2016 года, в рамках которой защита КИИ определяется как одна из стратегических целей. Согласно законопроекту “к критической инфраструктуре относятся информационные системы и телекоммуникационные сети госорганов, автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности”.

Детализируя указанные требования, создаваемая ЦПС должна обладать следующими характеристиками, обеспечивающими кибербезопасность объекта:

- создаваться на российской доверенной аппаратно-программной платформе с основными компонентами (операционная система, микропроцессор, контроллер периферийных интерфейсов, базовая система ввода/вывода), разработанными в РФ силами российских специалистов и имеющими полную конструкторскую документацию;
- учитывать положения стандартов, разработанных группой IEC TC57: IEC 61850, IEC60870, IEC 62351, в части безопасности коммуникационных протоколов, а также требования стандарта INL Cyber Security Procurement Language 2008, серии стандартов ISO/IEC 27000 в части общих принципов обеспечения безопасности цифровых систем управления и ГОСТ-Р МЭК 62443-3-2013;
- использовать российские гостированные криптографические алгоритмы, которые встраиваются в каждый элемент или каждую подсистему цифровой подстанции.

Рис. 2. Внешний вид терминала РЗА

Еще одной отличительной особенностью построения технологических систем управления в электроэнергетике является то, что применение криптографических средств защиты информации (СКЗИ) в них не должно снижать производительность, так как длительность переходных (аварийных) процессов составляет десятки микросекунд. Во многих применяемых сегодня микроконтроллерах встраивание элементов кибербезопасности либо изначально не предусмотрено разработчиком, либо невозможно, так как их встраивание не позволит обеспечить требуемое быстродействие.

Опираясь на многолетний опыт работы и знания в своих предметных областях, специалисты компаний ОАО “НИПОМ”, ООО “ИнСАТ”, ОАО “ИнфоТеКС” и ПАО “ИНЭУМ им. И.С. Брука” разработали цифровую подстанцию, отвечающую всем указанным требованиям. “Нижний” уровень ЦПС базируется на инновационных терминалах релейной защиты (РЗА) компании ОАО “НИПОМ”. Разработанный терминал РЗА (рис. 2) выполнен в виде кассеты блочной конструкции с задним присоединением внешних проводов и оборудован системой тестового контроля, служащей для проверки работоспособности основных узлов и блоков.

В корпусе терминала РЗА расположены платы дискретных входов/выходов, плата аналоговых входов для подачи измеряемых токов и напряжений, кросс-плата, служащая для согласования кабельной части универсальных плат (AI, DO/DI), блок питания и компьютер в промышленном исполнении с микропроцессором Эльбрус, поскольку функционирование КСЗИ ОС Эльбрус обеспечивает требуемый уровень защиты информации от несанкционированного доступа (НСД) и не влияет на быстродействие системы. Каждая плата DO/DI

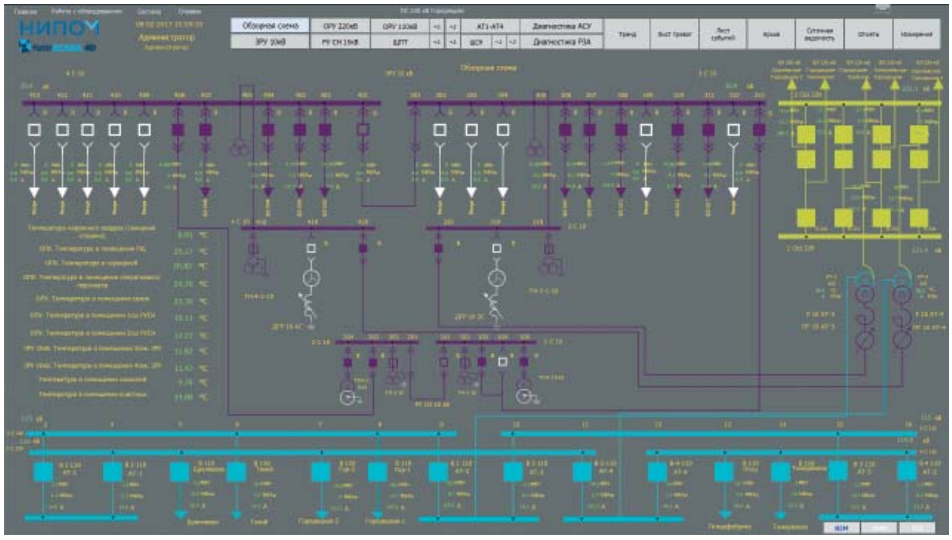

Рис. 3. Вид главной мнемосхемы оператора

содержит 11 каналов DI и 10 каналов DO. Таким образом, в одном корпусе можно выполнить от 33 до 66 каналов DI и от 30 до 60 каналов DO, что позволяет использовать разработанные терминалы РЗА как на объектах с небольшим количеством сигналов, так и на сложных, с большим числом присоединений. Для реализации функций передачи сигналов дифференциальной токовой продольной защиты линии (ДЗЛ) с использованием протокола SV (МЭК 61850) количество портов Ethernet может быть увеличено добавлением стандартной Ethernet-карты в промышленный компьютер без изменения его конструкции. Полное разделение логики терминала и его аппаратного исполнения позволило предоставить широкие возможности для свободно конфигурируемой логики схем защиты. К особенностям терминала, повышающим его киберзащищеность, можно отнести механизмы строгой двухфакторной аутентификации, реализованные ОАО "НИПОМ" совместно с ОАО "ИнфоТеКС".

"Верхний" уровень разработанной системы, как уже было сказано ранее, представляет собой сервер на базе отечественного процессора Эльбрус с одноименной операционной системой, который при необходимости может быть зарезервирован. Кроме того, в зависимости от требований того или иного объекта в решении также может быть использована ОС AstraLinux. В качестве среды сбора и обработки данных используется российская SCADA-система MasterSCADA 4D производства компании ООО "ИнСАТ". MasterSCADA 4D является кроссплатформенной, вертикально-интегрированной программной платформой с объектно-ориентированными методами программирования, в том числе на языках стандарта МЭК 61131-3, и единственной на сегодня SCADA-системой, работающей на ОС Эльбрус. MasterSCADA 4D осуществляет сбор информации с терминала РЗА через встроенный драйвер протокола МЭК 61850 (MMS) и предоставляет данные в виде мнемосхем, отчетов и трендов на автоматизированное рабочее место оператора подстанции. На стартовой (основной) мнемосхеме оператора (рис. 3) отображается однолинейная схема подстанции, присоединения и состояния первичного оборудования.

Также оператору доступна информация, собираемая с терминалов РЗА, с отображением состояния их характеристик, включающих внутреннюю самодиагностику и результаты срабатывания защит (рис. 4), и более детальная информация, содержащаяся на отдельной мнемосхеме, по состоянию дискретных выходов (включая срабатывание защит) и аналоговых входов терминала.

Кроме того, оператор всегда располагает информацией о работоспособности сетевой топологии ЦПС в виде сигнализации состояний (включая АРМы, SCADA-серверы и вторичное коммуникационное оборудование) с фиксацией полного списка тревог в журнале событий. Встроенные механизмы защиты MasterSCADA 4D обеспечивают аутентификацию и идентификацию пользователей в системе, а также разграничение их прав доступа по заранее определенной разработчиком ролевой модели, регистрацию всех действий пользователей от момента идентификации до выхода из системы.

В целях защиты электронного периметра подстанции и реализации принципа многоуровневой защиты были использованы шлюзы

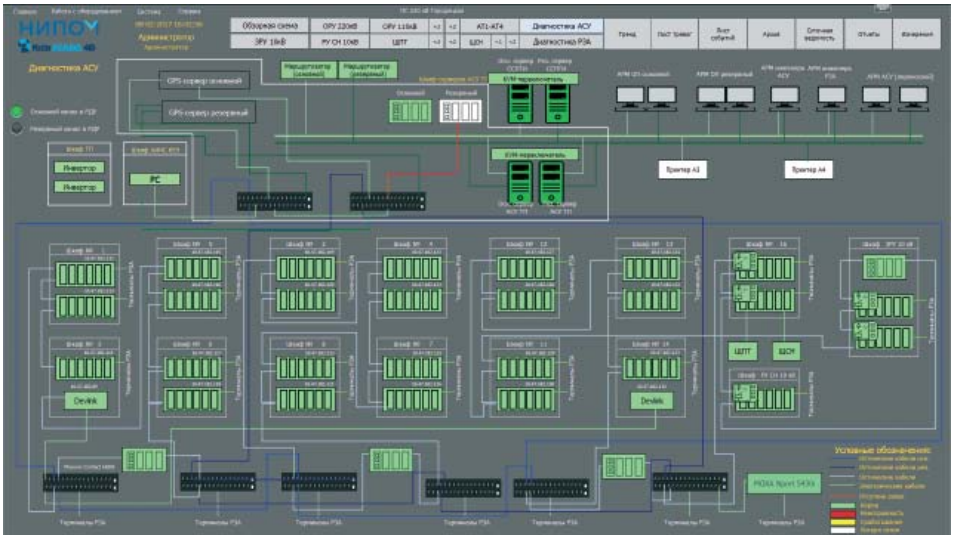

Рис. 4. Мнемосхема диагностики АСУ

безопасности разработки компании ОАО "ИнфоТеКС", – ViPNetCoordinator HW 1000. Локально-вычислительная сеть подстанции была разделена/сегментирована на несколько доменов безопасности, т. е. зон подстанции с разными требованиями по обеспечению ИБ.

Таким образом, с использованием индустриального шлюза безопасности ViPNetCoordinator IG были разграничены права доступа между уровнем станции и уровнями присоединения и шины процесса, что демонстрирует функциональная схема на рис. 5.

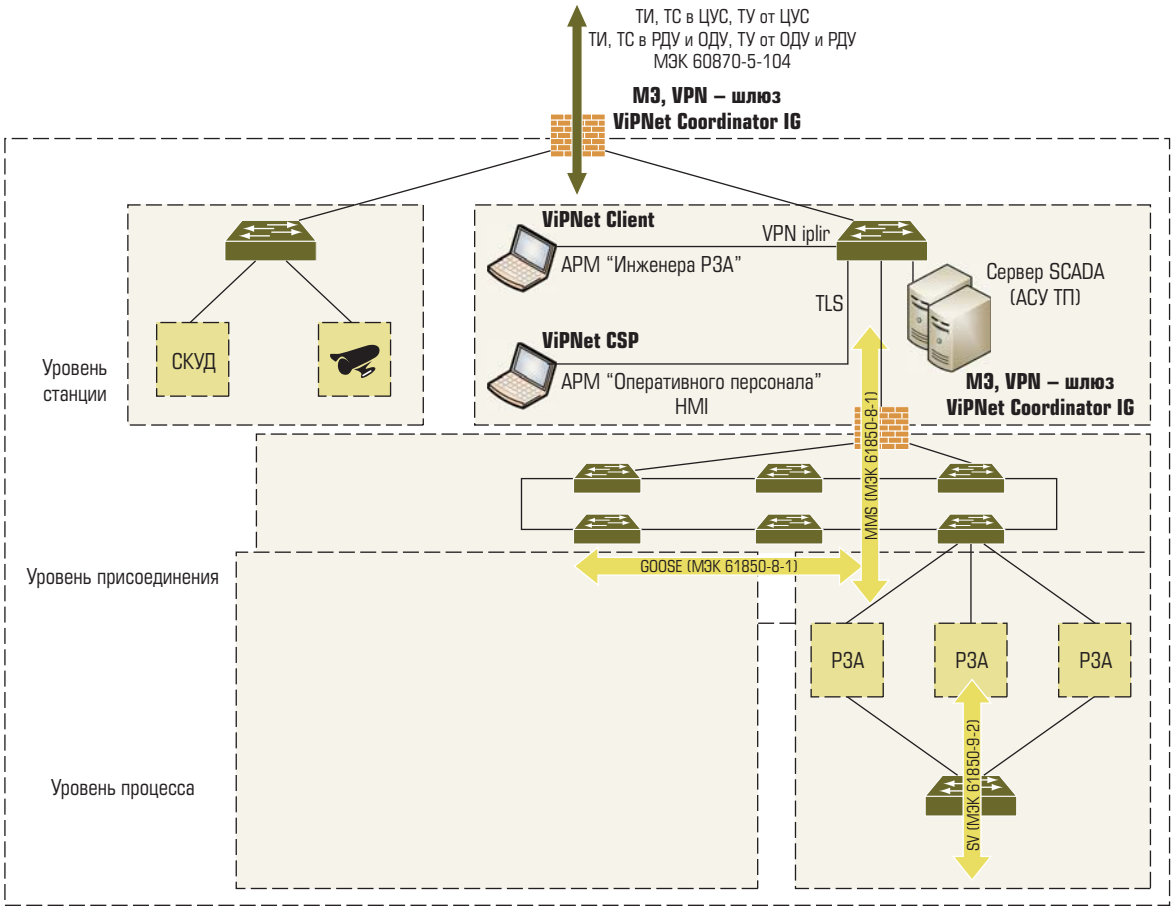

Рис. 5. Функциональная схема ЦПС с использованием средств многоуровневой киберзащиты

Реализация принципа многоуровневой защиты с применением межсетевых экранов является не только возможной, но и необходимой мерой защиты информации на подстанциях, находящихся в эксплуатации и подвергающихся частичной модернизации в соответствии с требованиями Приказа ФСТЭК России от 14 марта 2014 г. № 31 [3].

Применение наложенных средств ЗИ как на вновь создаваемых подстанциях, так и на подстанциях, подвергающихся глубокой модернизации, было бы неправильно признать достаточным, так как остаются высокие риски реализации компьютерных атак на незащищенные телекоммуникационные протоколы: MMS, GOOSE, SV.

В условиях необходимости удовлетворять комплексу требований по функциональной надежности, безопасности, быстродействию телекоммуникационных протоколов, а также по оптимальности затрат наиболее перспективно выглядит реализация концепции встраивания средств криптографической защиты информации в каждый элемент или в каждую подсистему цифровой подстанции.

ОАО “НИПОМ”, ООО “ИнСАТ”, ОАО “ИнфоТеКС” и ПАО “ИНЭУМ им. И.С. Брука” не останавливаются на достигнутом и продолжают совершенствовать разработанную ЦПС с использованием отечественных решений, которые позволяют реализовать киберзащищенное исполнение ЦПС для повышения надежности объектов высоковольтных электрических сетей.

Список литературы

1. *Основные* положения концепции интеллектуальной энергосистемы с активно-адаптивной сетью. Режим доступа: *http://www.fsk-ees.ru/upload/docs/ies_aas.pdf*
2. *International* Electrotechnical Commission. Communication Networks and Systems for Power Utility Automation – Part 8-1: Specific Communication Service Mapping (SCSM)—Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3; IEC 61850-8-1-2011; International Electrotechnical Commission (IEC): Geneva, Switzerland, 2011. [Google Scholar].
3. *Приказ* ФСТЭК России от 14 марта 2014 г. № 31. Режим доступа: *http://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/110-tekhnicheskaya-zashchita-informatsii/dokumenty/prikazy/864-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31*

Зинин Владимир Михайлович *– директор управления перспективных разработок ОАО “НИПОМ”,*
Подлесный Андрей Михайлович *– руководитель отдела продаж программного обеспечения ООО “ИнСАТ”,*
Карантаев Владимир Геннадьевич *– руководитель направления развития бизнеса ОАО “ИнфоТеКС”.*