Подкомитет Технического комитета РНК СИГРЭ по тематическому направлению D2 «Информационные системы и телекоммуникации»

ОТЧЕТ

об участии в заседании исследовательского комитета D2 «Информационные системы и телекоммуникации» в Лиме (Перу)

12-16 октября 2015 года

Наблюдательный член от РНК СИГРЭ
в Исследовательском Комитете D2, д.т.н. О.В. Синенко

Москва, 2015

В Лиме (Перу) 12-16 октября 2015 года в форме коллоквиума прошло заседание Исследовательского Комитета (ИК) D2 «Информационные системы и коммуникации». На встрече присутствовали регулярные и наблюдательные члены ИК из разных стран. Кроме членов ИК на мероприятие прибыли руководители некоторых действующих рабочих групп и 19 экспертов из девяти стран.

Краткое содержание программы коллоквиума:

1. Доклады руководителя и секретаря ИК D2.
2. Доклады по актуальным темам Исследовательского Комитета D2.
3. Направления современных исследований национальных подкомитетов D2 СИГРЭ.
4. Планы и задачи ИК D2 на 2016 – 2018 г.г.

1. Содержание докладов руководителя и секретаря комитета D2

В 2014-2015 годах были завершены работы по ряду направлений работ и подготовлены следующие публикации Комитета:

1. Техническая брошюра 603, разработанная совместной рабочей группой JWGD2/B5.46 – **«Применение и управление мерами информационной безопасности для систем защиты и управления** (“Application and management of cyber security measures for protection and control systems”), февраль 2015
1. Техническая брошюра 615 (рабочая группа WGD2.31) –**« Архитектура безопасности для цифровых систем в электроэнергетике для цифровых устройств объектов электроэнергетики»** (“Security architecture principles for digital systems in electric power utilities”), июнь 2015
2. Техническая брошюра 618 (рабочая группа WGD2.35) – **«Масштабируемые решения коммуникаций по оптоволоконным сетям связи»** (“Scalable communication transport solution over optical network”), август 2015
3. Статья **«Состояние кибербезопасности»** (“Status of cyber security”) – Журнал “ELECTRA”, октябрь 2014

Был анонсирован новый журнал СИГРЭ “Cigre Science and Engineering Journal” доступный только в электронном виде и имеющий иные цели, чем журнал “ELECTRA”. В новом издании в июне 2015 была опубликована первая статья Комитета D2: G. Dondossola **«Информационная безопасность систем регулирования напряжения в сетях с распределенной энергетикой»** (“Security of communication in voltage control for grids connecting DERs”).

Для отбора статей от Комитета в данное издание предложено создать экспертную группу в составе представителей России, Нидерландов, Австралии и Великобритании.

В преддверии 46-й сессии СИГРЭ председателем Комитета были названы темы двух “Green book”, формируемых на основе Технических брошюр:

- **Разработка информационных технологий и телекоммуникации с обеспечением кибербезопасности** (Development of a I&C and cyber security)
- **Внедрение систем связи для критически значимых коммуникационных сервисов** (Implementing telecommunication networks to deliver critical utility-grade communication services)

Для подготовки материалов для первой из “Green book” отмечена необходимость привлечения экспертов и консультантов из национальных комитетов СИГРЭ.

Данные издания ориентированы на отражение ситуации в мире по использованию в энергосистемах различных стран новых технологий ИТ и телекоммуникаций, причем такие публикации должны предварять их издание в других журналах.

В заключение Председателем Комитета было отмечено, что существующая в настоящее время система организации деятельности исследовательских комитетов СИГРЭ далека от оптимальной и планируются мероприятия по ее совершенствованию.

2. Аннотации докладов, по актуальным задачам ИК D2, представленные на коллоквиум

На ежегодном коллоквиуме Исследовательского комитета D2 («Информационные системы и телекоммуникации») СИГРЭ, проходившем в 2015 году в г. Лима (Перу) были представлены 22 доклада по трем анонсированным ранее тематическим секциям:

- Сети телекоммуникаций в аварийных режимах энергосистемы.
- Сохранение устойчивости бизнеса производства и передачи электроэнергии и его обеспечение в условиях катастроф.
- Лучшие практики реализации экономически эффективных систем кибербезопасности в электроэнергетике.

Секция №1 Сети телекоммуникаций в аварийных режимах энергосистемы

Основные направления докладов на секции:

- применение стандарта IEC 61850 в локальных и общесистемных сетях;
- векторные измерения для задач защиты и автоматизации;
- синхронизация сетевых районов и технология распределения операций по времени;
- возникающие проблемы и последствия нарушений в сети.

D2-01.01 Т.Сато (Япония) «Разработка нового поколения систем передачи информации в передающих сетях (i.QPA-сеть)» (“Development of next-generation power supply information transmission system (i.QPA network)”)

Опыт замены в ходе реконструкции в электрической сети старой АТМ системы связи на IP систему, удовлетворяющей требуемым значениям коэффициента готовности, времени задержки передачи информации и скорости ее передачи в аварийных режимах. В новую систему введена функция резервного копирования объекта, что повысило надежность операций ЦУС. Такая реконструкция сети позволила сократить затраты на установку новой системы за счет использования элементов существующей (ссылка-1, ссылка-2).

D2-01.02 Р.Леаль (Бразилия) «Построение гибких оптических сетей (OTN) для обеспечения передачи данных в аварийных режимах» (“Building a resilient optical network (OTN) transporting critical applications”)

Опыт реализации в бразильской энергосистеме дополнительной разветвленной опто-волоконной информационной сети (OTN), которая накладывается на уже существующую OTN сеть. Это позволяет с помощью использования технологий ITU-T OTN осуществлять передачу как оперативной информации по управлению, так и административной информации для системообразующих и распределительных сетей. Несколько уровней устойчивости такой оптоволоконной сети на SDH и OTN включены в систему автоматического восстановления, осуществляемой в течении нескольких миллисекунд. Сети OTN хорошо вписываются в задачи обеспечения работы систем SCADA и автоматизации подстанций. В статье представлены практические результаты по эксплуатации таких сетей (ссылка-1, ссылка-2).

D2-01.03 К. ди Палма (Аргентина) «Опто-волоконные сети связи (OPGW) для надежных систем управления телекоммуникациями и релейной защиты в системообразующих линиях электропередач» (Optical fiber transmission media (OPGW) for a reliable operation of the telecommunication and protection systems on high voltage transmission system")

Излагаются особенности выбора оптоволоконных кабелей OPGW для задач управления электроэнергетическими системами на стадиях проектирования, выбора производителя, особенностей монтажа и наладки. Изложенные требования существенно отличаются от требований при выборе оптоволоконного кабеля GW и должны проводиться с более высоким уровнем детализации (ссылка-1, ссылка-2).

D2-01.04 А.Квик (Испания) «Анализ опыта эксплуатации кабеля OPPC в энергосистеме Испании» (Analysis of the installation of an OPPC cable in Red Electrica de Espana")

Доклад посвящен особенностям эксплуатации оптоволоконного кабеля OPPC, размещенному в проводе высоковольтной линии - наименее распространенному способу системы передачи информации в энергосистеме Испании. Энергокомпания обладает патентом на технологию такого использования OPPC, но в данной статье приведен более глубокий анализ и особенности монтажа телекоммуникационного кабеля конкретной ЛЭП на острове Тенерифе. Материал содержит изложение накопленного опыта эксплуатации (ссылка-1, ссылка-2).

D2-01.05 Дж.Коста (Уругвай) «GOOS обмен информацией между подстанциями с использованием SDH системы передачи» ("GOOS massages between substations using SDH transport")

В докладе изложены результаты расчетов и тестов при выборе системы оптоволоконной коммуникации в промышленной сети. Одной из задач такой сети было требование обеспечения синхронности с помощью Precision Time Protocol и GOOSE сообщений, как определено в МЭК 61850. На первой стадии проекта было использована синхронная

цифровая иерархия SDH NG, сохраняя время отправки сообщений от центра управления к отдельным станциям. Проведены необходимые измерения по сообщениям GOOSE (ссылка1, ссылка2).

D2-01.06 Р. дель Кастильо (Испания) «Требования стандарта МЭК 61850 для шин станции управления SAS» ("Meeting requirements in a IEC 61850 station bus SAS")

В докладе описан процесс выбора архитектуры системы управления энергосистемой с системообразующими сетями 220 кВ Перу и анализом вариантов ее развития (ссылка-1, ссылка-2).

D2-01.07 Ф.Штайнхаузер (Австрия) «Точная оценка времени доступа к сети связи согласно МЭК 61850» (" Evaluations from accurately acquired and time stamped traffic to assess communication networks for IEC 61850 applications")

Изложена методика оценки временных характеристик информационной системы. Отмечена важность присвоения временных меток с использованием протокола Precision Time (PTP, IEEE 1588), позволяющего получить достаточную точность измерений. Выявлено, что в PRP системах появляются временные расхождения, связанные с топологией сети и типом используемого оборудования (ссылка-1, ссылка-2).

D2-01.08 Д.Дарн (Испания) «Влияние топологии сети на время ее восстановления после аварии. Примеры из практики.» ("Effect of the network topology in the recovery time. A practical case study")

Доклад посвящен взаимодействию оборудования цифровой подстанции с системой связи в энергосистеме. Критерием оценки выбрано время восстановления сети после аварии. Выявлено, что время восстановления сильно зависит от топологии сети и алгоритма системы управления (ссылка-1, ссылка-2).

D2-01.09 Ф.Кастро Цервера (Испания) «Новая система защиты телекоммуникаций IP- сетей» ("A new teleprotection system over IP network")

Описан проблемы при организации каналов связи для задач защиты ЛЭП на базе IP-сетей: задержки по времени являются случайными величинами, зависящими от сетевого трафика и временной метки. Это свойство должно быть использовано для измерения фактического времени задержки при передаче сигнала от передатчика к приемнику, чтобы не нарушать процесс управления энергосистемой. В данном случае система телекоммуникации подвержена кибератакам и должна быть обеспечены соответствующей системой защиты (ссылка-1, ссылка-2).

D2-01.10 Х.Рот (Корея) «Накопители энергии на электростанциях Кореи для регулирования частоты в энергосистеме» (“Energy storage systems for frequency regulation at electric power plants in Korea”)

Система накопителя электроэнергии (ESS) на шинах электростанции позволяет сгладить график выработки, поглощая энергию в режиме малых нагрузок и обеспечивая баланс мощности и регулирование частоты в режиме пиковых нагрузок. Эффективность электростанций повышается за счет работы генераторов в номинальном режиме и отсутствия необходимости обеспечивать резерв их мощности для регулирования частоты. В статье приведена архитектура системы управления накопителем (PMS) по критерию регулирования частоты системы в режиме реального времени и во взаимодействии с системами управления другими субъектов энергосистемы (ссылка-1, ссылка-2).

Секция №2 Сохранение устойчивости бизнеса производства и передачи электроэнергии и его обеспечение в условиях катастроф

Основные направления докладов секции:

- технологии и архитектуры систем, обеспечивающих устойчивую работу энергосистемы;
- создание условий готовности энергосистемы и каналов связи к стихийным бедствиям;
- стратегии восстановления информационных систем после аварий;
- основные способы восстановления систем после аварий.

D2-02.01 Л.Лассани (Нидерланды/Австралия) «Восстановление работы современных энергосистем после стихийных бедствий» (“Disaster Recovery in the modern EPU»)

Восстановление работы энергосистемы после стихийного бедствия во многом связано с состоянием информационных систем и связи. Работа исследовательской группы WG D2.34 была призвана проанализировать опыт восстановления энергосистемы в части работы информационных систем и связи и выработать рекомендации для мирового сообщества энергетиков. Доклад построен на опыте нескольких стран, чьи энергосистемы были подвержены стихийным бедствиям в результате природных или антропогенных катастроф (ссылка-1, ссылка-2).

D2-02.02 Э.Игиджо (Япония) « Планирование обеспечения непрерывности IT-бизнеса (IT-BCP) в Японии в условиях стихийных бедствий» (“IT business continuity plans (IT-BCP) in Japan)

Актуальность такого планирования возросла после землетрясения 2011 года на востоке Японии. Разработан ряд превентивных мероприятий на основе опыта восстановления энергосистемы после катастрофы. Первостепенное значение получила задача сохранения

главного диспетчерского центра системы (предусмотрено специальное оборудование на усиление строительных конструкций и средств крепления оборудования). В плане мероприятий по информационно-управляющим системам предусмотрено создание резервного диспетчерского пункта с разработкой ряда виртуальных сценариев развития ситуации (ссылка-1, ссылка-2).

D2-02.03 К.Саито (Япония) «Практика японских энергокомпаний по усилению живучести электросетей» (“Approach to Strengthening Power Company Networks in Japan”)

Освещается задача усиления сетей и систем телекоммуникаций с учетом дополнительной информации, полученной из анализа прошедшей катастрофы с учетом увеличения потока информации в период будущей катастрофы для задач обеспечения непрерывности бизнеса энергоснабжения (BCP) и ряда профессиональных треннингов персонала компаний (ссылка-1, ссылка-2).

D2-02.04 Т.Харага (Япония) «Применение системы восстановления энергосистемы после катастрофы к процессу обеспечения непрерывности бизнеса энергоснабжения» («Application of the Disaster Recovery Support System for Disaster Recovery and Business Continuity”)

Данный доклад представляет собой введение в важнейший раздел исследований систем обмена информацией и поддержке системы восстановления энергоснабжения в условиях катастрофы, специально разработанной для этой цели и работающей в режиме реального времени для получения точной информации, необходимой для восстановления энергоснабжения (ссылка-1, ссылка-2).

D2-02.05 К.Катсураде (Япония) «Использование спутниковых линий связи для повышения устойчивости работы информационных каналов в условиях катастроф» (“Undertakings to utilize Satellite Line to enhance Communication Network”)

В докладе представлены созданные информационные системы с использованием спутниковых линий связи на ряде японских электростанций, которые хорошо себя зарекомендовали в обеспечении стабильных поставок электроэнергии при землетрясении 2011 года. Опыт случившейся катастрофы показал, что число таких каналов необходимо увеличивать, способствовать расширению доступности к ним для быстрого создания временных информационных систем с новыми нормативными требованиями в период бедствия (прорыв плотины, заражение радионуклидами, землетрясение) (ссылка-1, ссылка-2).

D2-02.06 Х.Л.Фернандо (Колумбия) «План действий центров управления передачей электроэнергии в аварийных ситуациях с использованием технологий

мультиобъектной архитектуры» (“Contingency plan for transmission control centers using multisite architecture”)

При создании системы управления энергосистемой использована многоузловая архитектура в соответствии с мульти-объектной концепцией, разработанной Open System International (OSI) в соответствии с MCA требованиями. Схема предусматривает наличие двух центров управления в различных городах, и работающих самостоятельно. Многоузловая архитектура позволяет одновременную отправку информации от каждой подстанции электропередачи и включает избыточный канал связи между центрами управления передачей. Это позволяет синхронизировать данные SCADA и резервное копирование двух центров управления. Стратегический сценарий включает планы действий в различных чрезвычайных ситуациях. В 2014 году система была испытана в режиме реального времени с удовлетворительными результатами (ссылка-1, ссылка-2).

Секция №3 Лучшие практики реализации экономически эффективных систем кибербезопасности в электроэнергетике

Основные направления докладов на секции:

- этапы внедрения систем кибербезопасности;
- оперативные стратегии и процедуры внедрения систем кибербезопасности;
- оперативный мониторинг и автоматизация адекватного реагирования на инциденты;
- используемые технологии и архитектуры создания систем обеспечения безопасности.

D2-03.01 Г.Фернандес (Испания) «Реализация системы кибербезопасности за пять шагов» (“ Implementing Cyber Security in Five Steps”)

Использование технологий TCP/IP, для задач автоматизации сетевых подстанций и для WAN коммуникаций между ними, связано с необходимостью обеспечения кибербезопасности процесса управления электросетями. В этом случае необходимы меры защиты как от внешних атак, так и от внутренних, с формированием политики восстановления системы управления. В этом случае концепция кибербезопасности может содержать четыре уровня защиты: сеть, Host, приложения и данные. Каждый слой защиты предназначен для конкретного типа угрозы, выполняя функции резерва для предъидущего слоя. В данном докладе приводится материал по эксплуатации защит систем информации и связи от кибератак на уровне подстанции с выработкой пяти этапов контрмер с конкретными рекомендациями (ссылка-1).

D2-03.02 Я.Отсука (Япония) «Использование детектора антивредоносного «белого списка» против угроз кибератак» (“Introduction of anti-malware measures using whitelisting based on behavioral detection”)

Традиционно защита конфидециальной информации от кибератак осуществлялась с помощью детектора «черных списков» (шаблонов). Использование журналов «белых списков» обеспечивает мгновенное обнаружение новых типов вредоносных программ при

условии постоянного обновления журналов таких списков. Статья посвящена реализации защит от вредоносных мер с использованием «белых списков», апробация которых проводится с 2012 года (ссылка-1, ссылка-2).

D2-03.03 И.Гонзалес (Мексика) «Рамки безопасности и контроля доступа для развития корпоративных веб-порталов» ("Framework for the development of secure web system for electrical companies")

Все большее число энергокомпаний ощущают нарушения бизнес процессов из-за влияния кибератак через веб-платформы своих информационных систем и систем управления, особенно при внедрении новых технологий, таких как интеллектуальные сети. Разработанная система является результатом изучения и анализа лучших практик и методов создания безопасного программного обеспечения, стандартов и моделей управления доступом на базе схемы Single Sign-On. Выявлено, что для энергокомпаний системы безопасности, создаваемые на ранней стадии развития программного обеспечения намного дешевле и позволяют сократить текущие расходы на управление безопасностью (ссылка-1, ссылка-2).

D2-03.04 Д.Хольштейн (США) «Реакция инженеров по эксплуатации систем защиты и управления на появление киберугроз» ("P&C engineer's response to cyber-induced faults")

Опросы инженеров эксплуатации систем защиты и управления выявили, что появление ложных сигналов на управление не всегда распознаются ими. Для анализа данного факта была создана совместная проблемная рабочая группа JWG B5/D2.46. Распознавание кибератак и правильное реагирование инженерного состава энергокомпании требует их подготовки на базе трех принципов:(1) ощущение кибератаки; (2) способность понять происходящее; и (3) предвидение последствий выполнения требуемых команд. Такая модель поведения инженерного состава может вызвать опасные задержки по времени при принятии важных решений по управлению энергосистемой (ссылка-1, ссылка-2).

D2-03.05 Ж.Сардона (Колумбия) "Стандарт МЭК 61850 для реализации каналов связи на базе Wi-Fi технологий» (" Enabling mobile technologies on IEC 61850")

Использование мобильной связи для решения задач электроэнергетики позволяет осуществлять оперативный мониторинг за состоянием оборудования подстанции, позволяя сократить число персональных компьютеров. В этом случае информационная безопасность решается на основании требований МЭК 62351 с использованием методов Mobile Security. На практике был использован один MMS сервер и один клиент MMS с использованием Android платформы для задач технического обслуживания подстанций, лабораторных испытаний оборудования и учебных задач (ссылка-1, ссылка-2).

D2-03.06 Л.Луисиани (Нидерланды) «Обеспечение кибер устойчивости информационных и управляющих систем в электроэнергетике на основе IP-сетей» ("Building cyber resilience in EPUs IP networks")

В докладе излагаются принципы создания необходимой архитектуры системы кибербезопасности для обеспечения устойчивой работы средств оперативной технологии.

Киберустойчивость представляет собой баланс между технологией, организацией и процедурами, такими как восстановление работы энергосистемы после аварий (ссылка-1, ссылка-2).

3. Актуальные направления исследований национальных подкомитетов СИГРЭ

Секретарем Комитета D2 г-ном Маурицио Монти на основе отчетов представителей национальных комитетов CIGRE были представлены задачи в области ИТ и телекоммуникаций, исследования которых наиболее актуальны для энергосистем различных стран:

1. **Системы связи для SCADA, поддерживающей коммуникацию с системами распределенной генерации.** (Communication for SCADA supporting distributed energy resources (DERs), prosumers, etc)
2. **Проектирование, монтаж и эксплуатация и обслуживание оптических кабелей связи в грозотросе OPGW** (Design, installation, operation and maintenance of OPGW)
3. **Переход от систем связи на основе TDM (Time Division Multiplexing) к сетям с переключениям пакетов для ответственных сервисов** (Migration from TDM to packet switching networks for critical services)
4. **Стратегия выбора систем передачи данных для существующих и будущих приложений** (Strategic choice to establish a data transmission network for existing and future application)
5. **Интернет вещей в интеллектуальном учете электроэнергии** (Internet of things and relation to smart meters)
6. **Информационная платформа и центр хранения данных в задачах оператора учета (агрегирование данных учета)** (Information platform and data warehouse for system operator (aggregation of meters, etc.).
7. **Роль и место CRM-систем на рынке энергетики** (Role and position of CRM system in the energy market).
8. **Кибербезопасность** (Cyber security).

Высказано мнение, что последние три задачи наиболее актуальны и будут присутствовать в программах вновь создаваемых рабочих групп Комитета SC D2.

4. Актуальные планы и задачи Исследовательского Комитета D2

Решено, что планы по созданию новых рабочих групп будут обсуждены на следующем общем мероприятии Исследовательского Комитета D2.

На сессии СИГРЭ в августе 2016 года предстоит замена руководства исследовательского комитета D2. Кандидатами на посты председателя и секретаря комитета являются представители крупнейших электротехнических и электроэнергетических компаний Франции (Alstom и RTF).

Отмечено, что по причине высокой активности бизнес-процессов в области ИТ и телекоммуникаций, двухлетний срок полномочий представителей национальных комитетов, как правило, недостаточен для реализации намеченной программы.

Актуальна задача поиска лидера исследований по теме “IT security remote services”. Также новых специалистов приглашают для участия в деятельности консультативных рабочих групп AWGD2.01, AWGD2.02.

Ранее намеченное место очередного коллоквиума SC D2 2017 года в г. Дублине (Ирландия) вызвало определенные сомнения членов Комитета. Предложение представителя России о включении городов Москва или С. Петербург в список альтернативных кандидатов на проведение коллоквиума SC D2 в 2016 г. нашло положительный отклик у руководителей Комитета. Ими рекомендовано отправить официальное письмо от РНК СИГРЭ в адрес руководства Исследовательского Комитета D2 с предложением организации коллоквиума в РФ.

5. Заключение

В целом мероприятие в Лиме следует признать успешным, наблюдается особая активность отдельных стран (Франция, Япония, Испания, Нидерланды, Австралия).

В ходе коллоквиума отмечена активизация российского национального подкомитета D2, значимость присутствия России на митинге Комитета и ее оперативное подключение к подготовке публикаций Исследовательского комитета.

С благодарностью воспринято предложение об участии экспертов SC D2 в работе планового семинара российского подкомитета D2 в 2016 г., что будет способствовать повышению роли России в деятельности международных организаций.

В ходе активного общения с нынешним Председателем SC D2 г-ном Карлосом Сометьером было высказано предложение о представлении от РНК кандидатур экспертов для участия в исследованиях по тематике “IT security remote services”.

Особо отмечена значимость присутствия представителей России в роли активных членов SC D2 при подготовке технических брошюр, что может привести к определенным преференциям для РНК при выстраивании долговременных отношений с новыми руководителями головного Комитета SC D2.

В целом работа Подкомитета D2 РНК СИГРЭ признана удовлетворительной.