Проблемная рабочая группа № 2 РНК СИГРЭ D2/B5
«Кибербезопасность компонентов инфраструктуры современных объектов электроэнергетики»

ПРОТОКОЛ №1

установочного заседания ПРГ № 2 РНК СИГРЭ D2/B5

Дата: 27 января 2015 г.
Время: 10:00 – 13:00
Место: г. Москва, ул. Верхняя Первомайская, д.51, переговорная № 301
Формат: очное заседание
Председатель: Никандров М.В.

ПОВЕСТКА ЗАСЕДАНИЯ:

№	Тема выступление	Ф.И.О. докладчика / ответственного за подготовку материалов
1.	Вступительное слово	Жуков Андрей Васильевич – заместитель директора по управлению режимами ЕЭС ОАО «СО ЕЭС»
2.	Сообщение о формировании проблемной рабочей группы №2	Никандров Максим Валерьевич – руководитель группы
3.	Опыт участия и результаты работы аналогичных групп в Европе	Гордейчик Сергей Владимирович – директор департамента R&D АО Лаборатория Касперского
4.	Презентация концепции «Контролируемой деградации систем управления»	Никандров Максим Валерьевич – руководитель группы
5.	Позиция ПАО «ФСК ЕЭС» на концепцию построения системы кибербезопасности	Шеметов Андрей Сергеевич - Заместитель начальника Департамента релейной защиты, метрологии и автоматизированных систем управления технологическими процессами
6.	Позиция ПАО «Русгидро» на концепцию построения систем кибербезопасности	Бикмухаметов Ринат Рафгатович – начальник управления АСУТП
7.	Выступление представителей ЗАО «РТСофт»	Литвинов Павел Васильевич - начальник аналитического отдела

ПРИСУТСТВОВАЛИ:

ООО «Интеллектуальные Сети»

Никандров М.В. – директор, руководитель Рабочей группы;

ОАО «СО ЕЭС»

Жуков А.В. – заместитель директора по управлению режимами ЕЭС;

Стешенко Д.М. - Ведущий специалист Отдела мониторинга эксплуатации РЗА;

ПАО «Русгидро»

Бикмухаметов Р.Р. – начальник управления АСУТП;

Жуков Д.А. – эксперт управления АСУТП;

Морозов А.П. – главный эксперт управления РЗиПА;

ПАО «ФСК ЕЭС»

Шеметов А.С. - Заместитель начальника Департамента релейной защиты, метрологии и автоматизированных систем управления технологическими процессами;

АО «Лаборатория Касперского»

Гордейчик Сергей Владимирович – директор департамента R&D;

ЗАО «РТСофт»

Машинский Ю.В. - руководитель группы автоматизации подстанций;

Чехов В.И. – консультант Технической дирекции по электроэнергетике;

Литвинов П.В. - начальник аналитического отдела;

Вериго А.Р. – руководитель группы АСТУ.

СЛУШАЛИ

1. Вступительное слово заместителя директора по управлению режимами ЕЭС ОАО «СО ЕЭС» Жукова А.В., который отметил, что вопросы кибербезопасности АСУ ТП актуальны и важны. Самое интересное мероприятие по данной методике произошло на конференции СИГРЭ в г. Екатеринбург в 2013 г. На нем было отмечено, что проблема актуальна и рассматривается уже на государственном уровне, готовятся документы и законодательная база. Участниками конференции было предложено, не дожидаясь Федерального законодательства, начать разрабатывать свой подход и комплекс документов, определяющих требования к информационной и кибербезопасности. Было предложено создать совместную рабочую группу подкомитетов релейной защиты и информационных систем, так как все понимают, что развитие технологии производства и передачи электроэнергии в дальнейшем пойдет путем повышений уровня автоматизации и информатизации.

В прошлом году группа была создана, но опыт предыдущих лет и ранее созданных групп показал, что процесс работы не до конца выстроен. Работа рабочих групп проводится на общественных началах, это исследовательская работа и задачи группы - это изучение вопроса и формирование общественного технического мнения по проблеме. В данном случае полезно будет направить силы на разработку подходов, стандартов и других руководящих документов, которые будут приняты техническим сообществом и применены при разработке, проектировании и эксплуатации объектов и устройств электроэнергетики.

Было принято решение о проведении установочного совещания с целью запуска реального процесса. В работе необходимо учесть мнения заинтересованных сторон: электроэнергетических компаний, проектных организаций и разработчиков оборудования

и ПО. Рабочая группа в этом году должна поставить определённые задачи и приступить к их реализации.

2. Доклад руководителя ПРГ № 2 РНК СИГРЭ D2/B5 Никандрова М.В., который отметил, что группа создана путем объединения профильных рабочих групп подкомитетов РНК СИГРЭ B5 «Релейная защита и автоматика» и D2 «Информационные системы и телекоммуникации». Группа ставит перед собой амбициозные планы – разработать документы в области информационной безопасности АСУ ТП электроэнергетических компаний, которые станут основой для внутренних стандартов операторов КВО электроэнергетики.

Цель – выработка общего национального подхода к созданию комплекса киберзащиты АСУ ТП электроэнергетических комплексов. Хотя компании по генерации, передачи и распределению электрической энергии у нас разные как по организационной структуре, технологическим особенностям и типам управления, но все они в совокупности составляют единую электроэнергетическую систему нашей страны – поэтому подходы к решению данной проблемы у них должны быть общими.

В состав группы вошли представители крупных операторов электроэнергетических систем нашей страны: Системный Оператор, Россети, ФСК ЕЭС, Русгидро, Мосэнерго, Росатом. Со стороны производителей вторичного оборудования для электроэнергетики присутствуют представители НПП ЭКРА, ИЦ Бреслер, Теквел. Экспертное заключения о применяемых подходах и решений по кибербезопасности мы надеемся получить от представителей области Информационной безопасности: Лаборатории Касперского, Позитивные Технологии, КРОК и Информзащита.

3. Доклад директора департамента R&D АО «Лаборатория Касперского» Гордейчика С.В., который рассказал про свой опыт работы аналогичной группы в Италии. Работа организована под эгидой ENISA с целью разработки Европейского стандарта по кибербезопасности применительно к энергетическому комплексу, но развития по дпнном направлению не получилось и пошли по пути созданию Итальянского стандарта. Возглавило группу компания Ansaldo. В результате коллеги приняли концепцию NIST кибербезопасности SMART GRID. По результатам обсуждения были добавлены телекоммуникационные компании, которые представляют сервис по организации связи между компонентами.

Были сформулированы цели – синхронизация усилий в области безопасности энергетики. Разные организации делают свои шаги, решено было обмениваться информацией в этом направлении и вынести этот стандарт на уровень руководства страны для закрепления этих решений законодательно. Были обозначены следующие задачи:

- управление уровнем доверия к микропроцессорным системам;
- управление уровнем защищенности информационных систем связанных;
- управление эффективностью средств защиты;
- выявление и расследование инцидентов кибербезопасности, восстановление в случае сбоев.

Разработана методика, которая формирует требования к тестированию оборудования и комплексов с точки зрения кибербезопасности. Введено понятие комплексное тестирование на :

- кибербезопасность, уязвимости;
- функциональная безопасность;
- недекларированные и избыточные функции;

- совместимость с средствами защиты;
- соответствие требований внешних регуляторов;
- устойчивости функционирования в информационной среде.

Такое тестирование должно стать частью тестирования на функциональную безопасность. Результатом тестирование является сертификат компании, в данном случае сертификат Ansaldo. Кроме того, должны быть учтены требования регуляторов и соответствие требования по ИБ для данного класса устройств:

- сертификат по требованиям кибербезопасности;
- сертификаты внешних регуляторов;
- стандарт по кибербезопасности:
    - встроенные средства защиты;
    - дополнительные средства защиты;
    - требования регулирующих органов;
- список известных уязвимостей, НДВ, связанных рисков.

В процессе внедрение и эксплуатации необходимо выполнят следующие мероприятия:

- согласование типовых проектов
- внедрение или сопряжение средств защиты
- раздел кибербезопасности в ТРП
- листы самооценки на основе методики/анализа средств защиты
- выборочные аудиты.

Вторая рабочая группа, в которой мы учувствуем – это группа, созданная в РЖД. Над вопросами кибербезопасности они работают уже два года. На базе НИИАС создан центр кибербезопасности, им руководит Макаров Б.А. Разработаны методики анализа защищенности, разработаны требования кибербезопасности. Сейчас ведется разработка методики учета влияния кибербезопасности на функциональную безопасность и безопасность движения.

Эта группа уже имеет достаточный опыт, поэтому имеет смысл пообщаться с ними и перенять их опыт.

4. Доклад руководителя ПРГ № 2 РНК СИГРЭ D2/B5 Никандрова М.В. «Вариант концепции построения системы безопасности электроэнергетических объектов»

Отмечено, что обстановка меняется быстрее чем мы на нее реагируем. Угрозы кибербезопасности очевидны и нарастают. Современным типам угроз, таким как новые методы преодоления «защитного периметра», легальные и непреднамеренные «бекдоры», реальная угроза основному технологическому процессу - нам сегодня противопоставить практически нечего.

Электроэнергетические систему управления достаточно сильно отличаются от общепромышленных – поэтому решение по системе защиты должно быть специфическим.

Следует признать, что защита только на периметре не эффективная и заранее проигрышна. Уже сейчас существует множество способов по преодолению «периметра» и однозначно в будущем появятся новые, значительно более изощрённые. Современные и перспективные системы защиты работают и, в ближайшее время, продолжат работать только на обнаружение угроз и атак. Это не потому что комплексы защиты так совершенны, а потому что наши системы управления не готовы к каким-либо воздействиям на свою информационную инфраструктуру. Возникает вопрос – что же делать, если даже внедрив системы защиты на периметре и внутри систем управления мы не сильно повышаем защищенность?

Предлагаю Вашему вниманию концепцию «**Контролируемой деградации системы управления**». Суть ее в том, что во время инцидента: атаки, заражения или других

кибервоздействий мы сознательно отказываемся от некоторых функций и отходим **на заранее подготовленные «рубежи деградации».**

Например, если объектовая система защиты обнаружила аномалию во внутренней сети энергообъекта – то мы отключаем второстепенные системы, которые непосредственно не отвечают за основной технологический процесс и сегментируем локальную сеть. Возможно, отключаем второстепенные сегменты, тем самым мы сильно уменьшаем среду, где развивается кибер-инцидент (высокоскоростные сети и вычислительные мощности под управлением многозадачных операционных систем). Это первый уровень деградации, который может включаться персоналом или удаленно, в том числе в качестве превентивной меры.

Следующий уровень – максимальная «деградация»: в работе остаются только основные защиты и функции управления. Максимально ручной режим. Этот режим включается персоналом по месту в случае серьезных инцидентов.

Основная идея, что и защиты, и система управления и персонал должны быть готовы к этим переходам, а не усугублять ситуацию своими хаотичными действиями.

Под эту концепцию необходимо подготовить 4 рамочных комплекта документов:

- рекомендаций к техническим требованиям, предъявляемым к МП РЗА, контроллерам и другим ИЭУ в части информационной безопасности, а также дополнения к методикам тестирования и аттестации;
- рекомендаций по построению информационно-технологических систем объектов электроэнергетики с учетом требований по информационной безопасности;
- рекомендации по построению архитектуры объектовой системы информационной безопасности;
- порядок действий персонала в случае кибер-инцидентов и порядок восстановления систему управления и защиты.

ОБСУЖДЕНИЕ:

Жуков А.В. По правилам устройства электроустановок, если оборудование остается без защиты – то его необходимо отключить, так что диспетчера и операторы будут действовать в рамках имеющихся правил.

Терминалы защитной автоматики интегрированы в систему управления (АСУ), если мы начинаем деградировать систему, то мы отказываемся от основных защит и отключаемся от АСУ, убираем весь информационный обмен, остаемся только на внутренней регистрации. Я считаю, что в этом плане надо послушать людей, которые разрабатывают системы управления. Все таки тенденции сейчас идут к необслуживаемым объектам, без персонала и системы управления мы не сможем управлять объектом. Так же возникает большая проблема доставки персонала на объекты для ручного управления.

Машинский Ю.В

Я бы предложил посмотреть на решения европейцев, они изначально строили свои сети как не обслуживаемые и дистанционной управляемые. Надо посмотреть их опыт, который они наверняка наработали.

Шеметов А.С.

Работы в области Киберзащиты проводить нужно, опасность кибератак и деградация сети в результате киберинцидентов существует, но остается вопрос: зачем проводить данные атаки, как токовых целей нет. Не надо преувеличивать проблему.

По приказу ФСТЭК надо сертифицировать средства защиты периметра. Существуют мнение, что все применяемое оборудование необходимо проводить через сертификацию во ФСТЭК, но существует реальная опасность, что это значительно повысит стоимость оборудования и многие зарубежные вендоры откажутся от данной процедуры и уйдут с российского рынка. В итоге мы и своих производителей загоним в долговую яму и лишимся поставок зарубежного оборудования.

В сегодняшней не простой экономической ситуации денег на дорогие системы защиты нет.

В ФСК вышел №366 приказ, в котором прописан ряд организационных мероприятий в части организационных мероприятий в части информационной безопасности. Необходимо строить системы управления исключающие прямой доступ к устройствам защиты. Необходимо сосредоточится на защите периметра и системе, которая разделит сети. Выработать набор методов и средств для защиты на периметре.

Основная опасность исходит от персонала: бывших и работающих сотрудников. Поэтому необходимы комплекс мероприятий по изменению паролей и учетных записей, которыми пользовался бывший или переведенный на другое место сотрудник.

Эффективным способом повышение кибербезопасности может стать реальное, а не формальное импортозамещение. Мы сейчас реально можем строить объекты на отечественном оборудовании.

Бикмухаметов Р.Р.

Кратко опишу как обстоят дела в компании Русгидро. Большинство вопросов, затронутых в ходе дискуссии актуальны для нас.

Сегодня мы так же в первую очередь обращаем внимание на информационный периметр, в этом плане у нас выпущены определенные приказы и распоряжения. При внедрении есть некоторые проблемы, которые решаются в рабочем порядке. Особенность нашего технологического процесса ставить нас в большую зависимость от интеграции подсистем в единый комплекс. Остановка информационного обмена между системами для нас создает большие проблемы.

Еще один аспект – это импортозамещение. Можно контактировать тот факт, что с отечественным производителем проще контактировать, в том числе и по вопросам информационной безопасности.

В компании ведется методологическая и технологическая подготовка условий для нормальной эксплуатации систем управления. Мы надеемся, что в результате работы этой рабочей группы появится общая основа для нормативной документации.

Предлагаемый нами один из аспектов повышения общего уровня информационной безопасности - это создание «Централизованной защищенной системы регистрации технологической информации». Данная система должна стать тем разделителем, которая отделить информационные системы АСУ ТП от других систем.

По опыту нашей работы в области Информационной безопасности считаем необходимым утвердить глоссарии, так как одни те же вещи мы называем разными названиями, поэтому необходимо определится с терминологией.

ПОСТАНОВИЛИ:

1. Утвердить состав рабочей группы согласно приложению №1 к настоящему протоколу.
2. Утвердить программу деятельности Рабочей группы согласно приложению №2 к настоящему протоколу.
3. Следующее совещание рабочей группы провести в г. Москва в начале марта 2016 г.

Руководитель рабочей группы М.В. Никандров

ПРИЛОЖЕНИЕ 1.

Список участников ПРГ №2 РНК СИГРЭ D2/B5

№	ФИО	Место работы	e-mail
1	Беляков Денис Николаевич	ПАО «Мосэнерго»	BelyakovDN@mosenergo.ru
2	Бикмухаметов Ринат Рафгатович	ПАО «Русгидро»	BikmukhametovRR@rushydro.ru
3	Брагута Максим Валериевич	ОАО «НТЦ ФСК ЕЭС»	Braguta_MV@ntc-power.ru
4	Вериго Андрей Ромуальдович	ЗАО «РТСофт»	verigo_ar@rtsoft.msk.ru
5	Головин Александр Валерьевич	ООО «Теквел»	gav@tekvel.ru
6	Гордейчик Сергей Владимирович	АО «Лаборатория Касперского»	Sergey.Gordeychik@kaspersky.com
7	Даренский Дмитрий Анатольеович	ЗАО «Информзащита»	d.darensky@infosec.ru
8	Дорофеев Иван Николаевич	АО «Лаборатория Касперского»	Ivan.Dorofeev@kaspersky.com
9	Зайцев Алексей Андреевич	ПАО «Россети»	Zaytsev-AA@rosseti.ru
10	Карпов Илья Александрович	ЗАО «Позитив технолоджиз»	IKarpov@ptsecurity.com
11	Литвинов Павел Васильевич	ЗАО «РТСофт»	litvinov_pv@rtsoft.msk.ru
12	Мальцев Максим Ильич	ПАО «Русгидро»	MaltsevMI@rushydro.ru
13	Морозов Алексей Павлович	ПАО «Русгидро»	MorozovAP@rushydro.ru
14	Никандров Максим Валерьевич	ООО «Интеллектуальные Сети»	nikandrov@igrids.ru
15	Пенский Виктор Владимирович	ПАО «Россети»	PenskyVV@rosseti.ru
16	Резников Александр Александрович	ООО «ИЦ Бреслер»	reznikov_aa@ic-bresler.ru
17	Стешенко Дмитрий Михайлович	ОАО «СО ЕЭС»	steshenko-dm@so-ups.ru
18	Селезнев Михаил Игоревич	ПАО «ФСК ЕЭС»	seleznev-mi@fsk-ees.ru
19	Сергеев Алексей Владимирович	ООО «НПП ЭКРА»	aleksey.sergeyev@yandex.ru
20	Федоров Иван Александрович	ООО «НПЦ «КСБ»	fedorov@keysystems.ru
21	Шеметов Андрей Сергеевич	ПАО «ФСК ЕЭС»	shemetov-as@fsk-ees.ru
22	Шипулин Антон Сергеевич	ЗАО «КРОК»	shipulin.anton@gmail.com

ПРИЛОЖЕНИЕ 2.

План работ ПРГ №2 РНК СИГРЭ D2/B5 на период 2016 – 2017 гг.

№	Наименование работы	Содержание работы	Срок исполнения
1.	Установочное собрание рабочей группы	Обсуждение целей, задач, планов работы и подходов к организации работ в ПРГ №2 РНК СИГРЭ D2/B5 на период 2016 – 2017 гг. Определение подхода к формированию персонального состава и требований к участникам группы.	27.01.2016 г.
2.	Формирование плана работ ПРГ №2 РНК СИГРЭ D2/B5 на период 2016 – 2017 гг.	Разработка проекта плана работ и заседаний ПРГ №2 на 2016 и 2017 годы с определением промежуточных контрольных точек.	10.02.2016 г.
3.	Формирование структуры целевого отчета ПРГ №2 РНК СИГРЭ D2/B5 по совокупности всех намеченных работ:	Разработка базовой структуры разделов, глав и приложений отчета.	03.03.2016 г.
3.1.	Название разделов целевого отчета ПРГ №2 РНК СИГРЭ D2/B5	Глоссарий терминов и определений	03.03.2016 г.
3.2.		Анализ изменения ландшафта угроз. Обзор мирового опыта по обеспечению информационной безопасности объектов электроэнергетики. Модели угроз для автоматизированных систем защиты и управления объектов электроэнергетики.	II квартал 2016 г.
3.3.		Рекомендации к техническим требованиям, предъявляемым к МП РЗА, контроллерам и другим ИЭУ в части информационной безопасности, а также дополнения к методикам тестирования и аттестации.	IV квартал 2016 г.
3.4.		Методология выбора средств противодействия актуальным угрозам. Рекомендации и типовые архитектуры объектовой системы информационной безопасности.	I квартал 2017 г.
3.5.		Рекомендации по построению информационно-технологических систем объектов электроэнергетики с учетом требований по информационной безопасности.	III квартал 2017 г.
4.	Организация круглого стола на конференции РЗА 2016	Доклад о работе по глоссарию и планах работы группы	май 2016 г.
5.	Совещание касательно раздела 3.2 программы работы группы		II квартал 2016 г.
6.	Организация круглого стола на RUGRIDS-ELECTRO 2016	Доклад о работе группы и обсуждение раздела 3.3	октябрь 2016 г.
7.	Совещание касательно раздела 3.3 программы работы группы		IV квартал 2016 г.
8.	Выступления на «Электрические Сети Россси 2016»	Доклад о модели угроз для объектов электроэнергетики	декабрь 2016 г.
9.	Совещание касательно раздела 3.4 программы работы группы		I квартал 2017 г.
10.	Организация круглого стола на конференции «Современные направления развития систем релейной защиты и автоматики энергосистем»	Доклад о типовых архитектуры объектовой системы информационной безопасности	июнь 2017 г.
11.	Совещание касательно раздела 3.5 программы работы группы		III квартал 2017 г.
12.	Выпуск целевого отчета ПРГ №2 РНК СИГРЭ D2/B5		ноябрь 2017 г.
13.	Подведение результатов деятельности рабочей группы		декабрь 2017 г.