Т Е Х Н И Ч Е С К И Й К О М И Т Е Т Н П « Р Н К С И Г Р Э »

Проблемная рабочая группа № 2 РНК СИГРЭ D2/B5
«Кибербезопасность РЗА и систем управления современных объектов электроэнергетики»

ПРОТОКОЛ №2

Второго заседания ПРГ № 2 РНК СИГРЭ D2/B5

Дата: 16 марта 2016 г.
Время: 10:00 – 14:00
Место: г. Москва, ул. Верхняя Первомайская, д.51, переговорная № 301
Формат: очное заседание
Председатель: Никандров М.В.

ПОВЕСТКА ЗАСЕДАНИЯ:

№	Тема выступления	Ф.И.О. докладчика / ответственного за подготовку материалов
1.	Вступительное слово	Никандров Максим Валерьевич – руководитель группы
2.	Обсуждение глоссария терминов в области кибербезопасности компонентов инфраструктуры современных объектов электроэнергетики	Никандров Максим Валерьевич – руководитель группы
3.	Управление рисками информационной безопасности и актуальные угрозы системам защиты и управления подстанций	Дорофеев Иван Николаевич, эксперт
4.	Проблемы и угрозы объектов электроэнергетики	Тиморин Александр Александрович - руководитель группы в АО «Лаборатория Касперского»
5.	Уязвимости и другие проблемы МП РЗА и других ИЭУ в части информационной безопасности	Никандров Максим Валерьевич – руководитель группы
6.	Анализ документов NERC CIP. Рекомендации к техническим требованиям, предъявляемым к МП РЗА, контроллерам и другим ИЭУ в части информационной безопасности.	Сергеев Алексей Владимирович - Заместитель заведующего отделом в ООО «НПП ЭКРА»
7.	Анализ трудозатрат и увеличение стоимости ИЭУ при реализации перспективных требований ИБ	Резников Александр Александрович – эксперт ООО «ИЦ Бреслер»
8.	Обсуждение вопросов совещания	

ПРИСУТСТВОВАЛИ:

ООО «Интеллектуальные Сети»
Никандров М.В., руководитель ПРГ №2;
ОАО «СО ЕЭС»
Стешенко Д.М.;
ПАО «Русгидро»
Бикмухаметов Р.Р.;
Жуков Д.А.;
Морозов А.П.;
ПАО «ФСК ЕЭС»
Шеметов А.С.;
ЗАО «РТСофт»
Дорофеев И.Н.;
Литвинов П.В.;
Вериго А.Р.;
ОАО «НТЦ ФСК ЕЭС»
Брагута М.В.;
ЗАО «Информзащита»
Даренский Д.А.;
ОАО «ИнфоТеКС»
Карантаев В.Г.;
ЗАО «Позитив текнолоджиз»
Карпов И.А.;
ООО «НПЦ «КСБ»
Федоров И.А.;
ЗАО «КРОК»
Шипулин А.С.;
ООО «Теквел»
Головин А.В.

СЛУШАЛИ

1. Вступительное руководителя группы Никандрова М.В., который подвел итоги установочного совещания, прошедшего в конце января 2016 г. По итогам установочного совещания утверждены состав группы и план работ.

В соответствии с утвержденным планом проводится второе заседание проблемной рабочей группы. В повестке дня сегодня обсуждение предложенного глоссария, обсуждение модели угроз и риски информационной безопасности, анализ и обсуждение дополнительных требований ИБ к терминалам РЗА и другим интеллектуальным устройствам на основе требований, которые предлагается документами Северо-Американской энергетической компании – NERC CIP.

2. Доклад руководителя группы Никандрова М.В., «Глоссарий терминов и определений в области кибербезопасности компонентов инфраструктуры современных объектов электроэнергетики» в котором было отмечено, что глоссарий должен обеспечить однозначное понимание понятий и взаимодействие всех участников рабочей группы.

В состав группы входят представители операторов электроэнергетических систем нашей страны, разработчики и поставщики вторичного оборудования и эксперты по информационной безопасности. В эти специалисты в своей профессиональной деятельности пользуются определённым количеством узко специализированных терминов. Формат группы уникален, область интересов работы группы лежит на пересечении узкоспециализированных областей: РЗА, АСУ ТП и ИБ.

Цель глоссария – обеспечение понятной всем участникам группы «основы» для диалога и создания итогового документа группы.

Шеметов А.С.

Глоссарий не должен быть большим и дублировать Стандарты, в нем должны быть только основные термины и то что в стандартных тематических сборниках терминов и определений нет. Например:

- организационные мероприятия по кибербезопасности;
- технические мероприятия по кибербезопасности;
- специалист организующий комплекс кибербезопасности – тот, кто владеет полной информацией по безопасности объекта;
- специалист участвующий в кибербезопасности – тот, чьи сведения влияют на информационную безопасность (например, инженер РЗА со знанием паролей);
- точки связи объекта с внешней сетевой инфраструктурой.

Эти параметры, понятные инженерам АСУ ТП, могут быть обработаны группой и быть добавлены в глоссарий.

Литвинов П.В.

Глоссарий – это не застывший документ и должен быть определен механизм добавления и уточнения терминов. Надо сосредоточится на тех понятиях, где возможны различные толкования. Так же необходимо добавить новые термины, которые еще мало известны и распространены в профессиональной среде.

У нашей организации есть опыт создания Информационно-аналитических систем с веб-интерфейсов, содержащих, в то числе и подсистему работы с терминами и определениями. Также существует множество готовых платформ, которые можно использовать для решения задачи эффективной коллективной работы с глоссарием.

3. Доклад эксперта Дорофеева Ивана Николаевича «Управление рисками информационной безопасности и актуальные угрозы системам защиты и управления подстанций».

Эксперт рассказал про варианты управление рисками информационной безопасности: избегание риска, реагирование на риск и принятие риска. Введены следующие понятия риска:

Предотвращение риска - это проведение изменений (технического решения, инструкций, законодательства и т.д.), чтобы уменьшить: мотивацию, уязвимость, ущерб.

Обнаружение риска – это оснащение защищаемой инфраструктуры средствами мониторинга и анализа, позволяющими выявлять инциденты ИБ: анализ трафика в ЛВС, анализ логов устройств.

Противодействие рискам – это регламенты действий персонала при обнаружении инцидента ИБ: активные системы противодействия вторжениям, постфактум анализ инцидента, принятие мероприятий по предотвращению.

Смягчение рисков – это, например, страхование, установка ЭМ блокировок не позволяющих целенаправленное повреждение оборудования средствами АСУ.

Так же было отмечено, что стоимость средств реагирования должна быть меньше чем риск, от которого они защищают. В противном случае экономически целесообразно принять этот риск (возможно с использованием смягчения).

4. Доклад эксперта Тиморина Александра Александровича (Лаборатория Касперского) «Проблемы и угрозы объектов электроэнергетики» в котором докладчик предложил свою классификацию угроз и нарушителей. Привел последние, ранее не известные примеры инцидентов ИБ в АСУ ТП.

Отмечена тенденция снижения уровня подготовки нарушителей, вследствие доступности инструментария для эксплуатации уязвимостей и организации атак. Бурное развитие поисковых систем, в том числе и специализированных типа Shodan позволяет

достаточно эффективно находит системы управления случайно или преднамеренно соединённых с Интернет.

5. Доклад руководителя ПРГ № 2 РНК СИГРЭ D2/B5 Никандрова М.В. «Угрозы кибербезопасности современных объектов электросетевого хозяйства» который рассказал, что в настоящее время найдено достаточно много уязвимостей и угроз для объектов электроэнергетики. Предложена трехуровневая миссиоцентрическая классификация угроз, впервые предложенная Сергеем Гордейчиком.

Особое внимание уделено новой угрозе – возможные атаки непосредственно на интеллектуальные устройства. ИЭУ сегодня – это промышленные компьютеры, у которых есть и будут уязвимости безопасности. В последнее время обнародованы уязвимости, которые выводят из работы терминалы защиты. Для электроэнергетики это особая проблема, потому что контроллеры и терминалы РЗА непосредственно управляют оборудованием. Сегодня МП РЗА является единственной защитой.

Сделаны следующие выводы:

- текущее поколение микропроцессорных устройств релейной защиты создавалось для изолированных сетей передачи данных и абсолютно беззащитны перед угрозами ИБ;
- так как МП РЗА и ПА – основная и единственная защита присоединения – необходимо принимать меры по их защите.
- в МП РЗА нового поколения производства иностранных фирм уже внедряется комплекс мер противодействия угрозам ИБ.

6. Доклад эксперта Сергеева Алексея Владимировича (НПП ЭКРА) «Рекомендации к техническим требованиям, предъявляемым к МП РЗА и другим ИЭУ в части информационной безопасности» По техническим причинам доклад сделал Никандров М.В.

Вопросами кибербезопасности электроэнергетических объектов в США задумались достаточно давно. Результатом данной деятельности стал набор документов NERC CIP. Представляю Вашему вниманию анализ технических требований, которые представлены в данных документах. Все требования можно разделить на несколько параграфов:

Раскрытие информации. В документации к устройству обязательна глава “Порты и сервисы” с описанием:

- открываемых на сетевых интерфейсах портов;
- предоставляемых сервисах;
- процессах запросов доступа и авторизации;
- методы аутентификации.

Минимальный набор сервисов. На устройствах, вводимых в работу, должны быть доступны:

- только порты и сервисы необходимые для получения данных;
- удалённый доступ только тем пользователям, которые были созданы вручную, для которых был задан строгий пароль.

Средство конфигурирования должно обеспечивать:

- проверку блокировки сервисов на портах или проверку блокировки портов;
- формирование отчётов о текущих привилегиях пользователей.

Ввод/вывод из работы и/или включение/выключение портов/сервисов должно сопровождаться событиями системы ИБ, по крайней мере, записью в журнале событий.

Аутентификация и парольная политика:

- заводские пароли должны в обязательном порядке меняться при первом же изменения конфигурации;
- должна быть предусмотрена система, не допускающая простые и повторяющиеся пароли;

– должна быть предусмотрена функция, защищающая от подбора паролей.

Режимы функционирования. Устройство должно функционировать в двух режимах:

– сервисный (могут быть доступны все порты и сервисы);
– рабочий (доступны только те порты и сервисы, которые необходимы для получения данных с устройства или получения данных устройством. Сервисы для конфигурирования должны блокироваться);

На устройстве обязательна возможность отключения функций точек доступа (уход в автономный режим).

Регистрация событий ИБ:

– входе/выходе пользователей из системы;
– неудачных попытках входа;
– о превышении количества неудачных попыток входа;
– изменении уставок (с указанием какая уставка и кем была изменена, старое значение/новое значение).

Записи журнала доступа должны храниться на устройстве в течении 90 календарных дней.

Удаление записей журнала доступа с удалённого рабочего места должно быть запрещено всем пользователям, включая администратора.

Опционально: устройство должно генерировать события, связанные с ИБ, для другой системы по открытому протоколу (например, генерация GOOSE-сообщений или syslog-сообщений).

Сетевая аутентификация

Использование стандарта IEEE 802.1x для аутентификации и авторизации устройств в сети передачи данных

Контроль изменения конфигурации устройства. Устройства должны иметь возможность организации:

– разрешения изменения конфигурации только при подаче физического сигнала на дискретный вход устройства;
– разрешения изменения конфигурации только при подаче логического сигнала (MMS);
– сигнализация факта изменения конфигурации устройства на дискретный выход.

7. Доклад эксперта Резников Александр Александрович (ИЦ Бреслер) «Анализ трудозатрат и увеличение стоимости ИЭУ при реализации перспективных требований ИБ». По техническим причинам доклад сделал Никандров М.В.

Докладчик представляет ведущего производителя электротехническое оборудования в частности МП РЗА.

В части внедрения дополнительных функций информационной безопасности в интеллектуальные устройства (ИЭУ) – трудоёмкость сильно зависит от объема реализуемых требований. В простейшем случае это коснется лишь незначительного изменения программного обеспечения ИЭУ. Трудозатраты в этом случае относительно не высоки.

В более сложных ситуациях может потребоваться развитие аппаратной составляющей (увеличение производительности системы, объемы ОЗУ, ПЗУ, и тп.) или даже конструктивной, например, размещение механической блокировки удаленного доступа на лицевой панели ИЭУ. Изменения в этой части, как правило, более затратные.

Озвучен вопрос необходимости реализации IEEE 802.1x. Необходима оценка прироста увеличения защищенности с учетом выполнения представленных требований. Какие типы/способы, атак/нарушения периметра ИБ данные требования перекрывают?

Высказано мнение, что выполнение этого требования не даст существенного прироста защищенности.

Отмечено что реализацией требований ИБ дело не закончится. Внушительные затраты потребуются на этапе проектирования системы. Определение общей политики безопасности, групп пользователей, пользователей, объектов ИБ, прав доступа к ним.

Стоит отметить, что во время наладки и эксплуатации, таких систем также возникнут дополнительные сложности, а значит и рост накладных расходов. Потребуется разработка процедур и следование им, обеспечение тайны, ведение журналов паролей, анализ событий, связанных с ИБ, и прочее.

ОБСУЖДЕНИЕ:

Шеметов А.С.

Безусловно опыт наших заокеанских коллег интересен и заслуживает внимания. Простые и понятные требования, которые значительно повысят защищенность ИЭУ, необходимо внедрять. Такие требования можно будет оформить СТО ФСК например.

Головин А.В.

Ситуация, когда за периметр будет занесен ноутбук зараженный вирусом, нацеленным на конкретный объект пока из разряда фантастики. Для защиты МП РЗА достаточно надежно защищать периметр и организационных мероприятий.

Дорофеев И.Н.

Требования по ИБ должны формироваться на основе модели угроз, которые вначале необходимо сформулировать. Может сложится ситуация, когда ничего не делать будет дешевле и эффективнее чем принимать требования, которые мешают работе персонала и объекта в целом.

Никандров М.В.

Для оценки последствий внедрения требований ИБ к ИЭУ, системе управления и самой системы защиты необходимы пилотные проекты. Только практическое внедрение позволит оценить приемлемость негативных последствий на нормальное функционирование объекта энергетики, которые несомненно будут.

Бикмухаметов Р.Р.

До перехода к практической реализации пилотных проектов, необходима теоретическая проработка методики требуемых испытаний с оценкой рисков, способов защиты от них и обоснованием необходимости реализации пилотных проектов.

ПОСТАНОВИЛИ:

1. Принять за основу предложенный глоссарий. Окончательно определится с источниками информации и указать их в введении к документу.
   Ответственный: Никандров М.В.

2. Организовать специализированный портал и «файловый обменник», которые позволят эффективно работать с документами, в частности с глоссарием группы.
   Ответственный: Никандров М.В., Литвинов П.В.

3. Для организации работы группы разработать регламент консолидированного принятия решений группы, который позволить разрешать разногласия внутри группы.
   Ответственный: Никандров М.В.

4. В соответствии с утвержденным планом работ начать подготовку раздела итогового документа «Модели угроз для автоматизированных систем защиты и управления объектов электроэнергетики». Для работы над разделом создать подгруппу во главе с Дорофеевым И.Н. Состав подгруппы приведен в Приложении 1.
   Ответственный: Дорофеев И.Н.

5. Продолжить работу над разделом «Рекомендации к техническим требованиям, предъявляемым к МП РЗА и другим ИЭУ в части информационной безопасности». На следующем заседании предоставить консолидированную точку зрения.
   Ответственный: Шеметов А.С., Никандров М.В., Сергеев А.В., Резников А.А.

6. Утвердить изменение в план работы группы. На следующем заседании выслушать доклад по теме «Обеспечение информационной безопасности современных систем РЗА заложенных в стандарте МЭК 62351»
   Ответственный: Карантаев В.Г.

7. Следующее совещание рабочей группы провести в г. Москва в конце июня 2016 г.
   Ответственный: Никандров М.В.

Руководитель рабочей группы  М.В. Никандров

ПРИЛОЖЕНИЕ 1.

Список участников подгруппы подготовки раздела итогового документа

№	ФИО	Место работы	e-mail
Руководитель подгруппы			
1	Дорофеев Иван Николаевич	ЗАО «РТСофт»	Ivan.dorofeev@gmail.com
Участники подгруппы			
2	Даренский Дмитрий Анатольеович	ЗАО «Информзащита»	d.darensky@infosec.ru
3	Карпов Илья Александрович	ЗАО «Позитив технолоджиз»	IKarpov@ptsecurity.com
4	Федоров Иван Александрович	ООО «НПЦ «КСБ»	fedorov@keysystems.ru
5	Карантаев Владимир Геннадьевич	ОАО «ИнфоТеКС»	Vladimir.Karantaev@infotecs.ru