Задание для Проблемной рабочей группы № 2 (ПРГ № 2) D2/B5

«Кибербезопасность РЗА и систем управления современных объектов электроэнергетики»

Наименование: Кибербезопасность РЗА и систем управления современных объектов электроэнергетики
Базовые организации: ЗАО «РТСофт», ОАО «СО ЕЭС»
Подкомитет(ы) РНК СИГРЭ: D2 «Информационные системы и телекоммуникации», B5 «Релейная защита и автоматика»
Руководитель ПРГ № 2: Никандров Максим Валерьевич,
эл. почта: nikandrov@igrids.ru
тел: +7 917 659 43 67
Дата начала работы ПРГ: декабрь 2015
Дата завершения работы: декабрь 2017

Актуальность: Изменение ландшафта угроз информационной безопасности электроэнергетических объектов, требования нормативно-правовых и нормативно-технических документов обусловливают необходимость пересмотра функциональных характеристик компонентов инфраструктуры современных объектов электроэнергетики как объектов информационной инфраструктуры электрических сетей.

Сооружение современных технологических объектов с развитой информационной инфраструктурой, использование современных протоколов информационного обмена на базе стандарта МЭК 61850 (широковещательные рассылки и подробное описание передаваемых данных), активное использование высокоскоростных сетей передачи данных – значительно увеличило поверхность для кибернетических атак.

Требования к длительному сроку службы интеллектуальных электронных устройств (ИЭУ), жесткие требования по быстродействию, обусловливают повышенную сложность применения технологий программного и аппаратного шифрования передачи данных активно применяемых в других областях промышленности и телекоммуникации.

Одним из наиболее эффективных методов решения задач обеспечения информационной безопасности (кибербезопасности) компонентов инфраструктуры современных объектов электроэнергетики (микропроцессорные терминалы релейной защиты и автоматики (МП РЗА), контроллеров и других ИЭУ) является создание комплексной системы организационно-технических мероприятий в области информационной безопасности, включающих:

- формирование дополнительных требований к функционалу МП РЗА, контроллеров, телекоммуникационного оборудования и других интеллектуальных устройств, применяемых на объектах электроэнергетики;
- внедрение специализированных технических средств (маршрутизаторов нового поколения, устройств обнаружения и предотвращения вторжения, специализированных программно-технических средств защиты и т.д.);
- корректировка организационно-распорядительной документации по эксплуатации объектов электроэнергетики в части информационной безопасности.

Должна быть инициирована активная проработка технических требований к компонентам современных электроэнергетических объектов, регламентирующая

наличие достаточного набора средств и технологий, обеспечивающих их устойчивость к наиболее вероятным кибернетическим атакам и другим деструктивным воздействиям на информационную инфраструктуру.

Необходимо разработать нормативно-техническую базу для процедуры тестирования и аттестации МП РЗА, контроллеров и систем управления, планируемых к установке на электроэнергетических объектах, на готовность противостоять актуальным киберугрозам (тесты на проникновение, устойчивость к атакам, реверс-инжиниринг и др.).

При реализации данных мероприятий повышается актуальность вопроса «токсичности» применяемых средств и методов защиты на функционирование систем управления технологическими процессами и их компонентов, поиска показателей эффективности и оптимальной стоимости предлагаемых комплексов кибернетической защиты по отношению к стоимости приобретения и владения информационно-технологическими системами объектов электроэнергетики.

Задачи:

1. Анализ отечественного и зарубежного опыта по обеспечению информационной безопасности объектов электроэнергетики, организация переводов документов профильных рабочих групп и исследовательских комитетов CIGRE.
2. Разработка рекомендаций по дополнению технических требований, предъявляемых к МП РЗА и другим ИЭУ, в части информационной безопасности.
3. Разработка материалов рекомендательного характера по построению информационно-технологических систем объектов электроэнергетики с учетом требований по информационной безопасности.
4. Разработка рекомендаций по построению архитектуры объектовой системы информационной безопасности.
5. Разработка рекомендаций и методологии тестирования МП РЗА и других ИЭУ на устойчивость к кибернетическим воздействиям.

Планируемый результат:

1. Выпуск брошюры с описанием разработанных рекомендаций по построению информационно-технологических систем объектов электроэнергетики с учетом требований по информационной безопасности.
2. Выпуск брошюры с описанием: модель угроз для объектов электроэнергетики (включая ИЭУ на базе МЭК 61850), рекомендации по построению архитектуры объектовой системы информационной безопасности.
3. Выпуск брошюры с описанием разработанных рекомендаций к техническим требованиям, предъявляемым к МП РЗА, контроллерам и другим ИЭУ в части информационной безопасности, а также дополнения к методикам тестирования и аттестации.