Организация работ по разработке модели угроз

Рабочие материалы третьего заседания ПРГ-2 B5/D2 РНК СИГРЭ

Карантаев Владимир / к.т.н. / Член РНК СИГРЭ
Менеджер
Отдел развития продуктов
Vladimir.Karantaev@infotecs.ru

План доклада:

- Постановка задачи для подгруппы по моделированию угроз ПРГ-2
- Организация работы
- Текущий статус работ
- Планы подгруппы

Постановка задачи:

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

«Кибербезопасность РЗА и систем управления современных объектов электроэнергетики».

Планируемый результат:

- Выпуск брошюры с описанием: модель угроз для объектов электроэнергетики (включая ИЭУ на базе МЭК 61850), рекомендации по построению архитектуры объектовой системы информационной безопасности.

Целью создания и деятельности подгруппы является разработка «Базовой модели угроз для функциональных систем и подсистем подстанций и электростанций (объектов защиты) в интересах ПАО «ФСК ЕЭС» и ПАО « РусГидро».

Ограничения:

При осуществлении работ подгруппы накладываются следующие ограничения на рассматриваемые объекты защиты:

- В работе в качестве объекта защиты не рассматриваются центры управления сетями (ЦУС) МЭС и РСК;
- В работе в качестве объекта защиты не рассматриваются региональные диспетчерские управления СО ЕЭС РФ;
- В работе не рассматриваются объекты защиты тепловых, конденсационных, атомных, ветровых, солнечных, геотермальных электростанций .

Организация работы:

Участники:

Подгруппа состоит из экспертов ряда отраслей:

- электроэнергетика,
- информационная безопасность,
- информационные технологии.

Формат:

Очно-заочные рабочие встречи:

Онлайн совещание – еженедельно,

Очные встречи – по необходимости.

Текущий статус:

- Проведено 4 онлайн совещания;
- Подготовлена первая версия классификатора «Объекты защиты»;
- В работе изучение действующих документов ФСК ЕЭС, СИГРЭ.

Планы подгруппы:

Задачи подгруппы, которые необходимо выполнить для достижения поставленной цели:

- Осуществить классификацию объектов защиты, учитывая сформулированные ограничения;
- Изучить взаимовлияние и влияние на технологический процесс функционирования объектов защиты, сформировать деревья атак;
- Сформировать модель нарушителя;
- Оценить возможность наступления последствий от результатов совершения компьютерных атак на объекты защиты.

Давайте пообщаемся!

Карантаев Владимир / к.т.н. / Член РНК СИГРЭ
Менеджер
Отдел развития продуктов
Vladimir.Karantaev@infotecs.ru