НИПОМ

ЭНЕРГИЯ ДОВЕРИЯ

ЦИФРОВАЯ ПОДСТАНЦИЯ ОАО «НИПОМ» В КИБЕРЗАЩИЩЕННОМ ИСПОЛНЕНИИ

«Великая держава – это страна,
которая владеет ядерными технологиями,
ракетными технологиями и криптографией»

Дэвид Кан

ПРЕДПОСЫЛКИ СОЗДАНИЯ ЦПС В КИБЕРЗАЩИЩЕННОМ ИСПОЛНЕНИИ

- создание специализированных подразделений в вооруженных силах государств НАТО численностью в десятки тысяч человек, основная задача которых заключается в выведении из строя инфраструктуры жизнеобеспечения и банковской сферы государств - «противников» путем кибератак;
- прямые угрозы первых лиц США о возможных кибератаках на инфраструктуру Российской Федерации;
- геополитическая ситуация (внешний фактор), что привело к ограничению ввоза в РФ продукции высокотехнологичных отраслей и технологий двойного назначения;
- расширение внутренних ограничений (внутренний фактор) на отрасли экономики (предприятия) закономерно и вынужденно попадающие под ограничение использования импортной микроэлектроники и программного обеспечения;
- возникновение новых рисков увеличения вероятности кибератак на критически важные объекты (КВО) инфраструктурных отраслей, последствия которых сопоставимы, например, с аварией на Саяно-Шушенской ГЭС, что заставляет учитывать при создании ЦПС вопросы киберзащиты как часть её ядра, а не как сторонний элемент, который можно будет добавить потом;
- технологическая готовность отечественной аппаратно-программной платформы, что создает благоприятные условия к снижению зависимости от импорта технологий, созданию действительно отечественных (не локализованных) аналогов интеллектуального оборудования ЦПС.

ПРЕДПОСЫЛКИ СОЗДАНИЯ ЦПС В КИБЕРЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Специалистам, профессионально занимающимся вопросами информационной безопасности (кибербезопасности) понятно, что основными возможными источниками так называемых «закладок» (backdoors), позволяющих перехватить управление информационной системой являются:

- микросхема центрального процессора (ЦП);
- микросхема контроллера периферийных интерфейсов (КПИ);
- базовая система ввода-вывода (BIOS);
- операционная система (ОС).

ВОПРОС: Если производство компонентов ЦПС локализовано в РФ или производитель оборудования является отечественным, то где, как и кем изготавливаются ЦП, КПИ для этих компонентов, программируется BIOS и операционная система ?

КИБЕРАТАКИ НА ОБЪЕКТЫ ЭЛЕКТРОЭНЕРГЕТИКИ

Тип нарушителя	Способ атаки	Общее описание атаки	Результат успешной атаки
Внешний Внутренний	Модификация MMS сетевого трафика между SCADA-сервером и МП терминалом РЗА	Реализация компьютерной (сетевой) атаки типа человек по середине MITM. Результатом, которой является нарушение целостности сетевых пакетов. Целью атаки может являться навязывание ложных данных (команд) со стороны SCADA-сервера на МП терминал РЗА. Навязывание ложных данных со стороны МП терминала на SCADA-сервер	Результатом навязывания ложных данных (команд) может быть реализация угроз функциональной безопасности (аварии)
Внешний Внутренний	Модификация сетевого трафика между терминалами МП РЗА	Реализация сетевой атаки типа «человек по середине» MITM, GOOSE Spoofing результатом, которой является нарушение целостности сетевых пакетов протокола GOOSE. Целью атаки может являться навязывание ложных данных о наличии или отсутствии аварийных событий	Результатом навязывания ложных данных (команд) может быть реализация угроз функциональной безопасности (аварии)
Внешний Внутренний	Мониторинг сетевого трафика между SCADA-сервером и МП Терминалом РЗА	Мониторинг сетевого трафика, может выступать стадией «пассивной» атаки, получив дамп «легитимного» трафика, злоумышленник следующим этапом может осуществить атаку типа MITM, навязывая ложные данные различным подсистемам ПС.	Результат ухудшение значений напряжения, частоты, тока, авария на объекте
Внешний Внутренний	Мониторинг сетевого трафика между терминалами РЗА	То же, что и в предыдущем случае, только злоумышленник следующим этапом может осуществить атаку типа GOOSE-spoofing, навязывая ложные данные различным подсистемам ПС	Результат ложное срабатывание РЗА, отключение потребителей, авария на объекте
Внешний Внутренний	Несанкционированное изменение настроек МП терминала РЗА		Аварии на объектах, каскадные аварии участка ЕЭС
Внешний Внутренний	Несанкционированное изменение конфигурации ЦПС		Аварии на объектах, каскадные аварии участка ЕЭС
Внешний Внутренний	Модификация МЭК 61870-5-104 сетевого трафика между ЦУС и ЦПС		Аварии на объектах, каскадные аварии участка ЕЭС

ЦИФРОВАЯ ПОДСТАНЦИЯ КАК ЕДИНИЦА ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ В ИНТЕЛЛЕКТУАЛЬНОЙ ЭЛЕКТРИЧЕСКОЙ СЕТИ

Цифровая подстанция (ЦПС) – это электрическая подстанция (ПС), система технологического управления которой построена на базе стандарта МЭК 61850 с использованием в качестве первичных измерителей цифровых трансформаторов тока (ЦИТТ) и напряжения (ЦИТН), а также выносных устройств сопряжения с объектом (УСО) и интеллектуальных электронных устройств (IED). Отличительной особенностью ЦПС является локализация кабелей связи и управления в силовом оборудовании и/или в шкафах выносных УСО, ЦИТТ, ЦИТН, а для передачи информации используется сеть с коммутацией пакетов Ethernet, настроенная специальным образом (шина процесса и шина подстанции в терминологии МЭК 61850).

Цифровая подстанция (ЦПС) включает в себя:

- подсистему технологической связи и передачи данных МЭК 61850;
- подсистему управления противоаварийной автоматикой;
- подсистему РЗА;
- подсистему АСУ ТП;
- подсистему учета электроэнергии и мощности (АИИСКУЭ);
- подсистему видеонаблюдения, пожарной и охранной сигнализации;
- подсистему единого времени ЦПС, синхронизированную с глобальным временем.

ОСОБЕННОСТИ АРХИТЕКТУРЫ ЦИФРОВОЙ ПОДСТАНЦИИ ОАО «НИПОМ»

По мнению ОАО «НИПОМ» система кибербезопасности для ЦПС должна создаваться на основе отечественной программно-аппаратной базы как еще одна обязательная технологическая подсистема, часть «ядра» построения ЦПС, элементы которой изначально должны быть заложены в каждое IED, УСО и MU.

Для того, чтобы элементы криптографии и шифрования могли быть встроены в элементы «интеллекта» ЦПС с минимальными трудозатратами и затратами на сертификацию, «интеллект» ЦПС должен использовать не узкоспециализированные контроллеры (в подавляющем большинстве импортного производства), а универсальные микропроцессоры с операционными системами, для которых соответствующие криптографические модули уже разработаны.

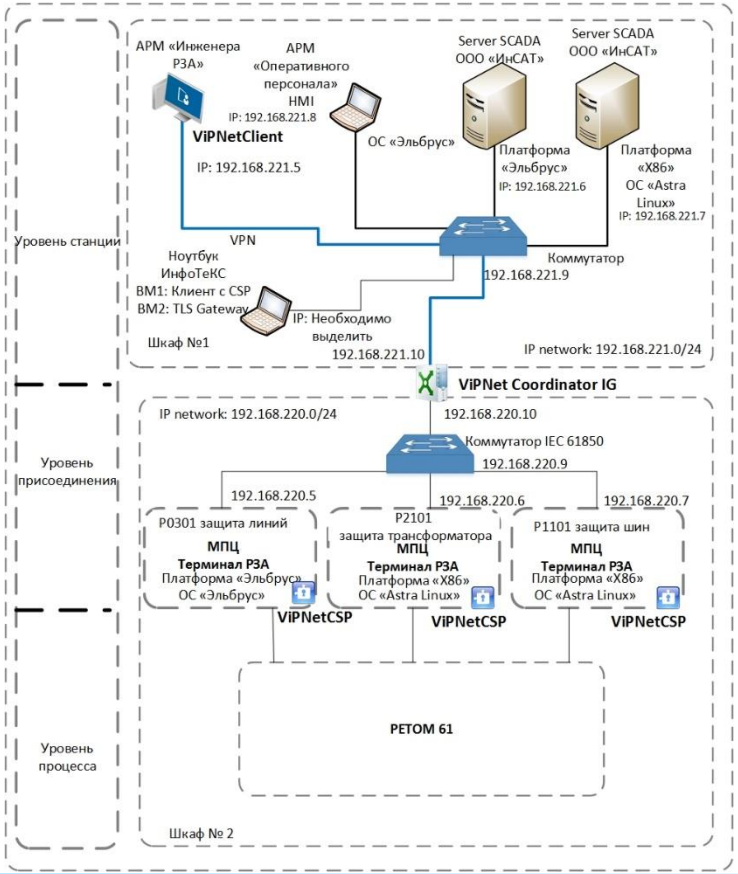
ОСОБЕННОСТИ АРХИТЕКТУРЫ ЦИФРОВОЙ ПОДСТАНЦИИ ОАО «НИПОМ»

В технологии ЦПС, предлагаемой нашей компанией изначально делается упор на использование готовой компонентной базы производителей вычислительных средств в промышленном исполнении.

Примером этого является кроссплатформенная микропроцессорная РЗА ЛЭП 110-220 кВ собственной разработки (в терминах ЦПС – это IED), которая построена на Intel-совместимом промышленном компьютере с разными операционными системами, среди которых несколько дистрибутивов Linux, в том числе и отечественных ROSA и Astra, и, конечно же, полностью российской аппаратно-программной платформе ЭЛЬБРУС. Программное обеспечение РЗА производства ОАО «НИПОМ» имеет международную сертификацию DNV GL на соответствие МЭК 61850.

В случае с реализованной нашей компанией архитектурой ЦПС встраивание элементов криптографии, шифрования и аутентификации в наши IED является стандартной инженерной задачей, которую мы успешно решили.

СХЕМА ЦИФРОВОЙ ПОДСТАНЦИИ ОАО «НИПОМ» В КИБЕРЗАЩИЩЕННОМ ИСПОЛНЕНИИ



ЭКСПОЗИЦИЯ ОАО «НИПОМ» НА ВЫСТАВКЕ «ЭЛЕКТРИЧЕСКИЕ СЕТИ РОССИИ – 2016»

На выставочном стенде ОАО «НИПОМ» (зал А стенд 102) представлены разработки электрооборудования и систем управления для электроэнергетической отрасли. Особое внимание уделено РЗА 110 - 220 кВ в составе ЦПС собственной оригинальной разработки, выполненной совместно с партнерами. Будут демонстрироваться сценарии работы РЗА в составе ЦПС на моделях реального времени и элементы киберзащиты ЦПС, в частности, использование TLS для шифрования трафика ЦПС и авторизация на терминалах РЗА с использованием USB-токенов.

Партнер ОАО «НИПОМ»	Роль в ЦПС ОАО «НИПОМ»
ОАО "ИнфоТеКС"	Разработка средств криптографии и шифрования (ГОСТ) для ЦПС
ООО "ИнСАТ"	Разработка отечественной SCADA-системы MasterSCADA 4D, в том числе и (впервые) для процессоров «ЭЛЬБРУС»
ПАО "ИНЭУМ им. И.С.Брука"	Производитель аппаратно-программных комплексов на процессорах «ЭЛЬБРУС»
ООО НПО "ЦИТ"	Экспериментальное производство цифровых измерительных трансформаторов тока (ЦИТТ) и напряжения (ЦИТН)
Phoenix Contact	Активное сетевое оборудование для организации шины процесса и шины станции МЭК 61850

ДАЛЬНЕЙШЕЕ РАЗВИТИЕ ТЕХНОЛОГИЙ ЦПС ОАО «НИПОМ»

- Развитие ПО в части удобства работы и расширения функциональности в составе ЦПС МЭК 61850
- Совместимость с решениями других производителей на базе стандарта МЭК 61850
- Дальнейшее повышение уровня кибербезопасности нашего изделия
- Учет требований и пожеланий наших Заказчиков

СПАСИБО ЗА ВНИМАНИЕ!

Докладчик:
Зинин Владимир Михайлович
Директор управления перспективных разработок
ОАО «НИПОМ»

Контакты

Адрес: 603140, Нижегородская обл., г. Н. Новгород, пр. Ленина, 20

Телефон: +7 800 100-43-44 (многоканальный)

e-mail: office@nipom.ru

http: www.nipom.ru