22.10.2015
Rugrids-Electro - 2015

Создание системы кибербезопасности в электроэнергетике РФ с учетом реализации концепции ИЭС ААС

ПРЕДПОСЫЛКИ

- Создание специализированных подразделений в вооруженных силах государств НАТО, основная задача которых заключается в выведении из строя инфраструктуры жизнеобеспечения и банковской сферы государств - «противников» путем кибератак
- Геополитическая ситуация (внешний фактор), результат - ограничение ввоза в РФ продукции высокотехнологичных отраслей и технологий двойного назначения, особенно в стратегических и инфраструктурных отраслях экономики РФ
- Расширение внутренних ограничений (внутренний фактор), результат - расширение списка отраслей (предприятий) где следует существенно ограничить использование 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, результат - система кибербезопасности для инфраструктурных отраслей экономики РФ должна создаваться как отдельная технологическая система, доступ к документации и архитектуре которой должен быть категорирован и ограничен
- Технологическая готовность отечественной аппаратно-программной платформы, результат – снижение зависимости от импорта технологий, создание отечественных аналогов интеллектуального оборудования для стратегических и инфраструктурных отраслей экономики РФ

НОРМАТИВНАЯ БАЗА

Основополагающие Федеральные документы:

- Доктрина информационной безопасности Российской Федерации (утверждена Президентом Российской Федерации В.В. Путиным 9 сентября 2000 г., № Пр-1895)
- Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации
- Энергетическая стратегия России на период до 2030 г. (утверждена распоряжением Правительства Российской Федерации от 13 ноября 2009 г. № 1715-р)

Базовые отраслевые документы:

- Концепция интеллектуальной электроэнергетической системы России с активно-адаптивной сетью (принята в 2012 году ОАО «ФСК ЕЭС»)
- Положение ОАО «Россети» о единой технической политике в электросетевом комплексе (утверждено Советом директоров ОАО «Россети» (протокол № 138 от 23.10.2013))

ВЫВОД: Требуется усилить направление кибербезопасности в отраслевых нормативных документах, определяющих развитие электроэнергетики РФ, и пересмотреть их формулировку в соответствии с основополагающими федеральными документами.

ЦЕЛЬ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АСУП И АСУ ТП КВО ИНФРАСТРУКТУРЫ РФ

Статья 2 «Основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» гласит:

«Целью государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов (КВО) инфраструктуры Российской Федерации является снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства».

ОСНОВНЫЕ ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ

- **Критически важный объект инфраструктуры Российской Федерации (далее - КВО)** - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта Российской Федерации либо административно- территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок
- **Критическая информационная инфраструктура Российской Федерации (далее - критическая информационная инфраструктура)** - совокупность автоматизированных систем управления КВО и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий

АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ ТЕХНОЛОГИЧЕСКИХ ОБЪЕКТОВ ЕЭС РФ ПРИМЕНИТЕЛЬНО К ВЕРОЯТНЫМ КИБЕРУГРОЗАМ

- Рост микропроцессорного (интеллектуального) оборудования на подстанциях ЕЭС РФ, в том числе со стеком TCP/IP и поддержкой стандарта МЭК 61850
- Доля используемой в этих решениях импортной аппаратной базы и программного обеспечения угрожающе высока и в некоторых случаях близка к 100%. Зачастую за отечественное оборудование выдается импортное оборудование, производство которого в той или иной степени локализовано в РФ
- Встречаются случаи использования на технологических объектах ЕЭС РФ свободно распространяемого ПО и различных пробных версий платного ПО, которые нерегулярно (или вообще) не получают обновлений безопасности и потенциально могут содержать «закладки»
- Сегодняшний подход к реализации функций информационной безопасности на технологических объектах ЕЭС РФ технически формальный (FireWall, VPN, антивирусная защита, разделение сегментов сети на технологический и общего назначения, парольная защита, часто неперсонифицированная)
- Неготовность эксплуатационного персонала технологических объектов ЕЭС РФ противостоять вероятным киберугрозам из-за отсутствия специальных знаний и такой системы

КОНЦЕПЦИЯ ИНТЕЛЛЕКТУАЛЬНОЙ ЭЛЕКТРОЭНЕРГЕТИЧЕСКОЙ СИСТЕМЫ РОССИИ С АКТИВНО-АДАПТИВНОЙ СЕТЬЮ (ИЭС ААС)

В «Концепции интеллектуальной электроэнергетической системы России с активно-адаптивной сетью» принятой в 2012 году ОАО «ФСК ЕЭС» отмечается, что «интеллектуальная электроэнергетическая система с активно-адаптивной сетью (ИЭС ААС) представляет собой электроэнергетическую систему нового поколения, основанную на мультиагентном принципе организации и управления ее функционированием и развитием с целью обеспечения эффективного использования всех ресурсов (природных, социально-производственных и человеческих) для надежного, качественного и эффективного энергоснабжения потребителей за счет гибкого взаимодействия всех ее субъектов (всех видов генерации, электрических сетей и потребителей) на основе современных технологических средств и единой интеллектуальной иерархической системы управления».

НЕВОЗМОЖНОСТЬ ПРИМЕНЕНИЯ СУЩЕСТВУЮЩИХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ (КИБЕРАТАК) ДЛЯ ИЭС ААС

- Известные в мире системы обнаружения вторжений (кибератак) – зарубежные и не могут быть использованы для построения системы кибербезопасности в ИЭС ААС (отечественный аналог «Паутина» – в стадии разработки)
- Применительно к ИЭС ААС недостаточно обнаруживать и предупреждать кибератаки, так как в результате успешного кибернападения будут выведены из строя системы диспетчерского и технологического управления, АСУ ТП и РЗА, энергосистема «ослепнет», что приведет к отключению потребителей и технологическим авариям
- Система кибербезопасности для ИЭС ААС должна обеспечивать минимизацию деструктивных воздействий на национальную энергосистему, вызванных кибератаками, и ее последующее восстановление при условии, что остальные технологические подсистемы скомпрометированы

ЦИФРОВАЯ ПОДСТАНЦИЯ – ЕДИНИЦА ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ В ИЭС ААС

Система кибербезопасности ЦПС

Сеть передачи данных для системы кибербезопасности ЦПС

Подсистема технологической связи и передачи данных ЦПС (включая шину процесса)

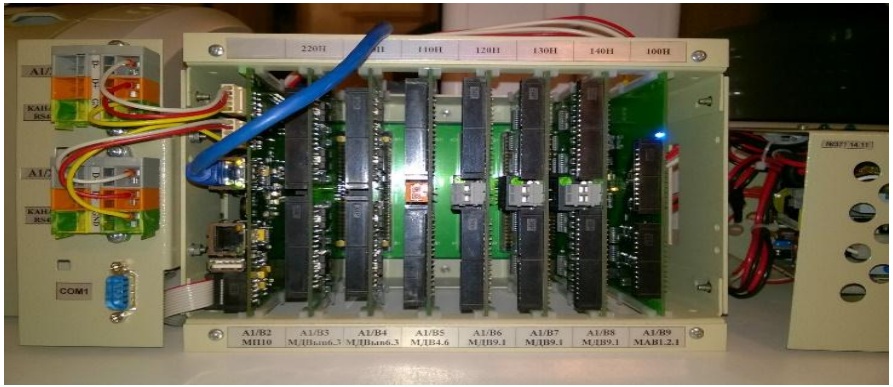
Подсистема управления противоаварийной автоматикой	Подсистема релейной защиты и автоматики	Подсистема АСУ ТП	Подсистема АИИСКУЭ	Подсистема видеонаблюдения, охранной и пожарной сигнализации	Подсистема единого времени ЦПС

ВЫВОД: Скомпрометирована может быть любая из технологических подсистем ЦПС

ТРЕБОВАНИЯ К СИСТЕМЕ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ИЭС ААС

- Система кибербезопасности для ИЭС ААС должна создаваться как параллельная независимая технологическая система обнаружения и предупреждения компьютерных атак объектов электроэнергетики на основе моделирования минимизации деструктивных воздействий на энергосистему и последующего восстановления её нормального функционирования после потери управления в результате кибератаки
- Система кибербезопасности для ИЭС ААС должна обеспечивать восстановление работоспособности энергосистемы с учетом её устойчивости, категорирования потребителей по приоритетам включения нагрузки, минимизации экологических и других рисков (политических, социальных и т.д.)
- В технологическом отношении система кибербезопасности для ИЭС ААС должна использовать отечественную доверенную вычислительную платформу, ключевые компоненты которой (операционная система, микропроцессор, контроллер периферийных интерфейсов, базовая система ввода-вывода) разработаны в РФ, силами российских специалистов и имеют полную конструкторскую документацию
- Интеллектуальное оборудование технологических объектов ЕЭС РФ должно быть заменено на отечественное в рамках программы импортозамещения

ПРИМЕРЫ ОТЕЧЕСТВЕННЫХ РАЗРАБОТОК: КОНТРОЛЛЕР АСУ ТП С ПОЛНОЙ ПОДДЕРЖКОЙ МЭК 61850



- Российское программное обеспечение с поддержкой стандарта МЭК 61850
- Российский процессор и большая часть компонентов
- Отсутствие аналогов отечественного производства
- Полная поддержка протоколов и стеков протоколов ЦПС

- Готовность: опытно-промышленные образцы

ПРИМЕРЫ ОТЕЧЕСТВЕННЫХ РАЗРАБОТОК: КОМПЛЕКС ВЫЧИСЛИТЕЛЬНЫХ СРЕДСТВ НА ОТЕЧЕСТВЕННОЙ ЭЛЕМЕНТНОЙ БАЗЕ «ЭЛЬБРУС»

- Процессор и элементная база российского производства
- Защищенная операционная система «Эльбрус»
- Промышленное исполнение, широкая номенклатура модулей

- Готовность: промышленные образцы

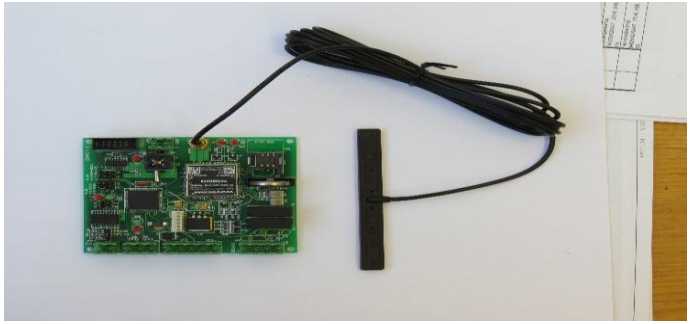
ПРИМЕРЫ ОТЕЧЕСТВЕННЫХ РАЗРАБОТОК: КОНТРОЛЛЕР СРЕДНЕГО УРОВНЯ АСУ ТП ЦИФРОВОЙ ПОДСТАНЦИИ (ЦПС)

- Аппаратная база - вычислительный блок БВ631 («МЦСТ»)
- Российское программное обеспечение с поддержкой стандарта МЭК 61850
- Гибкое программирование и настройка на базе современного стандарта МЭК 61131-3
- Полная поддержка протоколов и стеков протоколов ЦПС

- Готовность: опытно-промышленные образцы

ПРИМЕРЫ ОТЕЧЕСТВЕННЫХ РАЗРАБОТОК: КОНТРОЛЛЕР МАЛОЙ АВТОМАТИЗАЦИИ

- Полностью российская разработка
- Использование российской элементной базы и процессора
- Малое количество входов/выходов
- Широкие возможности использования
- Различные варианты исполнения (размеры, наличие дисплея, корпус и количество входов-выходов).



- Готовность: готов к производству

ПРЕДЛОЖЕНИЯ ПО СОЗДАНИЮ И РАЗВИТИЮ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ИЭС ААС

С учетом развития ИЭС ААС предлагается разработать и в дальнейшем развивать систему кибербезопасности для электроэнергетической отрасли, учитывающую её особенности и основанную на документах Совета безопасности Российской Федерации.

Система кибербезопасности для ИЭС ААС должна состоять из:

- концепции, определяющей единый понятийный аппарат, категорирование КВО, модели угроз КВО с типовыми политиками безопасности
- центров компетенции и производства элементов системы и интеллектуального оборудования с учетом требований кибербезопасности
- методик обучения и учебных программ для электроэнергетических специальностей ВУЗ-ов
- программ переобучения и аттестации действующего персонала энергосистемы РФ
- сертификации программно-аппаратных решений для КВО выполненных исключительно на отечественных микропроцессорах и программном обеспечении.

ПРЕДЛАГАЕМЫЙ ПОРЯДОК РАБОТЫ ПО СОЗДАНИЮ И РАЗВИТИЮ СИСТЕМЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ИЭС ААС

Реализация изложенных предложений может быть осуществлена через создание координационного совета при Министерстве энергетики РФ, а также рабочей группы при координационном совете, состоящей из ведущих специалистов электроэнергетической отрасли РФ.

Рабочая группа призвана решать следующие задачи:

- ❑ разработка концепции системы кибербезопасности для ИЭС ААС;
- ❑ подготовка изменений в законодательные акты РФ и национальные стандарты (ГОСТ-ы), с учетом концепции и гармонизации с международными стандартами (IEC, ISO);
- ❑ разработка предложений и рекомендаций по перспективным НИОКР применительно к создаваемой системе кибербезопасности для ИЭС ААС, повышение приоритета этих НИОКР;
- ❑ разработка требований к государственной сертификации и методик сертификации программно-аппаратных решений для КВО, а, возможно, и создание специализированного сертификационного органа.

ВЫВОД: Предлагаемый подход к созданию системы кибербезопасности для ИЭС ААС целесообразно использовать в газовой и нефтяной отраслях ТЭК РФ, а также управлении жилищно-коммунальным хозяйством РФ с учетом отраслевой технологической специфики

СПАСИБО ЗА ВНИМАНИЕ

Контактная информация:

ОАО «НИПОМ» (Научно-исследовательское предприятие общего машиностроения), Нижегородская область, г. Дзержинск, ул. Зелёная, 10, www.nipom.ru

Зинин Владимир Михайлович

Директор управления перспективных разработок

+7(910)8940133, +7(960)1741464,

v.zinin@nipom.ru

Нижегородский государственный технический университет им. Р.Е. Алексеева

Россия, 603950 Нижний Новгород, ул. Минина, 24

Куликов Александр Леонидович

Кафедра «Электроэнергетика, электроснабжение и силовая электроника»

Профессор, Доктор технических наук

+7(910)791-26-56,

inventor61@mail.ru

НИПОМ®
ЭНЕРГИЯ ДОВЕРИЯ

Докладчик: Зинин В.М.
Директор управления перспективных разработок

НАМ ДОВЕРЯЮТ

«НАУЧНО - ИССЛЕДОВАТЕЛЬСКОЕ ПРЕДПРИЯТИЕ ОБЩЕГО МАШИНОСТРОЕНИЯ»

Адрес:	606007, Россия, Нижегородская обл., г. Дзержинск ул. Зеленая, 10
http:	www.nipom.ru
Телефон:	+7 (8313) 243 888, +7 905 010 33 55
Факс:	+7 (8313) 243 871
E-mail:	office@nipom.ru