



Некоммерческое партнерство
«НАУЧНО-ТЕХНИЧЕСКИЙ СОВЕТ
Единой энергетической системы»

109044 г. Москва, Воронцовский пер., дом 2
Тел. (495) 912-1078, 912-5799, факс (495) 632-7285
E-mail: dtv@nts-ees.ru. <http://www.nts-ees.ru/>

УТВЕРЖДАЮ
Председатель Научно-технической
коллегии НП «НТС ЕЭС», д.т.н.,
профессор


Н.Д. Роголёв

«17» октября 2016 г.

ПРОТОКОЛ

заседания секции «Информационные технологии» НП «НТС ЕЭС» по теме:
**« Актуальные вопросы обеспечения информационной безопасности
автоматизированных систем технологического управления
электросетевого комплекса»**

30 сентября 2016 года

№ 3

г. Москва

Присутствовали:
Всего: 8 чел.

С вступительным словом выступил председатель секции «Информационные технологии», заместитель директора по информационным технологиям Филиала ОАО «СО ЕЭС» Московское РДУ И.А. Щипицин.

С докладом «Практический подход к защите информации АСТУ объектов электросетей. Опыт ПАО «МОЭСК» выступил директор по развитию ЗАО «РКСС» Панов И.С.

В своем докладе Панов И.С. отметил следующее:

1. В течение 2014-2015 гг ЗАО «РКСС» выполняла проект «Пилотная зона в области информационной безопасности оперативно-технологического управления ПАО «МОЭСК». Проект инициирован приказом Генерального директора ПАО «МОЭСК» Синютина П.А. и включал следующие основные цели и задачи:

- Оценка рисков и градация угроз безопасности по значимости для формирования для формирования требований по обеспечению безопасности автоматизированных систем технологического управления (АСТУ) пилотной зоны
- Разработка и проведение лабораторных, а также полигонных испытаний решений по защите информации, обрабатываемой АСТУ
- Апробирование и адаптация существующих и перспективных средств защиты информации АСТУ с фокусом на импортозамещающие технологии
- Разработка рекомендаций по ключевым аспектам защиты информации АСТУ

2. В презентации представлен системный подход по выполнению задач поэтапного приведения в соответствие характеристик эксплуатируемых систем АСТУ требованиям нормативных регуляторов и стандартов РФ в области информационной безопасности, который включает:

- систематизацию и детализацию требований регуляторов применительно к отраслевой специфике применяемых средств автоматизации (далее средств АСТУ), включая требования к аттестации систем информационной безопасности
- классификацию информации, обрабатываемой в АСТУ и формирование требований к защите каждой категории информации
- определение актуальных угроз безопасности информации АСТУ и рисков от их возможной реализации
- определение целей по снижению рисков от возможной реализации угроз безопасности информации АСТУ
- утверждение мер по защите информации АСТУ исходя из критериев реализуемости на существующем уровне технологий и экономической целесообразности
- формирование типовых проектных решений на базе сертифицированных средств защиты информации
- регламентацию процесса внедрения типовых решений для каждой компоненты АСТУ
- согласование вопросов аттестации систем защиты информации АСТУ.

3. Заявлено, что силами специалистов ЗАО «РКСС» и их технологических партнёров, разработаны и успешно апробированы перспективные средства защиты информации АСТУ, которые могут быть применены для компенсации самых актуальных угроз безопасности информации АСТУ, в частности:

- средства мониторинга сетевого трафика АСУ ТП и выявления сетевых аномалий
- средства межсетевого экранирования сегментов ЛВС АСУ ТП
- средства мониторинга и анализа событий безопасности АСУ ТП
- средства обеспечения целостности информации при передаче по цифровым каналам связи в формате специализированных протоколов
- средства организации доверенных каналов телеуправления
- средства организации доверенной вычислительной среды, позволяющие беспрепятственно использовать заимствованные (недоверенные) приложения без необходимости исследования степени их доверия (НДВ)
- средства аутентификации внешних пользователей и процессов АСУ ТП

В обсуждении доклада приняли участие: заместитель директора по информационным технологиям Филиала ОАО «СО ЕЭС» Московское РДУ Щипицин И.А., начальник аналитического отдела АО РТСофт Литвинов П.В., заместитель директора департамента развития и эксплуатации технологических АСУ ПАО «МОЭСК» Пономарев Д.И.

Отметили:

Реализация всего комплекса технических мер обеспечения информационной безопасности АСТУ потребует значительных затрат. Необходима разработка системного проекта обеспечения информационной безопасности АСТУ, в котором должны быть определены технические решения по защите информации для каждой подсистемы и сегмента АСТУ, выполнено обоснование затрат и расчет технико-экономического эффекта, а также разработана дорожная карта построения системы обеспечения информационной безопасности АСТУ с выделением первоочередных, наиболее приоритетных задач.

Перспективность, для обеспечения информационной безопасности, загрузки операционной системы в защищенной контролируемой виртуальной машине – путем использования специализированного гипервизора. Подобный гипервизор разработан ООО «Линтехно» при МГТУ им. Н.Э. Баумана».

Целесообразность комбинирования средств защиты. Например, путем организации каналов однонаправленной передачи данных в изолированные (локальные) защищенные сети.

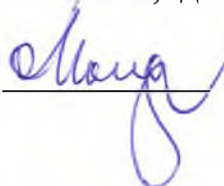
Обсудили:

Опыт разработки и применения в АО «РТСофт» программных и технических средств организации доверенной вычислительной среды, с гарантированной блокировкой недокументированных функций ПТК, использующих компоненты зарубежного производства, на примере защищенного комплекта программ (ЗКП) «Plato RT».

Заслушав доклад и выступления участников дискуссии заседания, заседание решило:

1. Принять доклад к сведению. Подтвердить актуальность вопросов обеспечения информационной безопасности автоматизированных систем технологического управления объектов электросетевого комплекса.
2. ПАО «МОЭСК» продолжить работы по организации пилотной зоны по отработке решений информационной безопасности при передаче телеинформации между объектовыми ССПИ и ДП.
3. Рекомендовать субъектам электроэнергетики операционной зоны Филиала ОАО «СО ЕЭС» Московское РДУ рассмотреть возможность включения в программы по импортозамещению в области ИТ оборудования возможность применения программных и технических средств организации доверенной вычислительной среды.

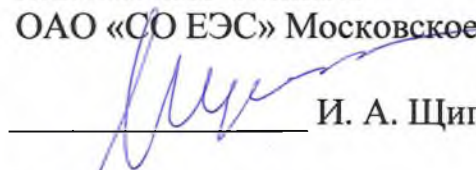
Первый заместитель Председателя
Научно-технической коллегии НП
«НТС ЕЭС», д.т.н., профессор


В.В. Молодук


Ученый секретарь Научно-
технической коллегии НП «НТС
ЕЭС», к.т.н.


Я.Ш. Исамухамедов

Председатель секции
«Информационные технологии»
НП «НТС ЕЭС», заместитель
директора по информационным
технологиям Филиала
ОАО «СО ЕЭС» Московское РДУ


И. А. Щипицин

Секретарь секции
«Информационные технологии» НП
«НТС ЕЭС»


Е.О. Базилюк