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/
ИНН 7717150757

"УТВЕРЖДАЮ"
Председатель Научно–технической
коллегии НП "НТС ЕЭС"
член-корр. РАН, д.т.н., профессор
_____ А.Ф. Дьяков
"06" декабря 2012 г.

ПРОТОКОЛ

заседания секции Автоматизированный учет электроэнергии и управление электропотреблением Научно-технической коллегии НП "НТС ЕЭС"
по теме
"Информационная безопасность технологических информационных систем (Виртуализация проверок АИИС КУЭ)"

20 ноября 2012 № 1 г. Москва

Присутствовали: 48 человек

На заседании выступили:

С вступительным словом

Председатель секции Автоматизированный учет электроэнергии и управление электропотреблением НТК НП "НТС ЕЭС" А.В.Покатилов.

С докладом

"Информационная безопасность технологических информационных систем (Виртуализация проверок АИИС КУЭ)" (Приложение 1)
Генгринович Е.Л., исполнительный директор SNITE GROUP GMBH

Виртуализация проверок АИИС КУЭ на Оптовом Рынке Электроэнергии (удаленный контроль) (Приложение 2)
Егоров С.А. технический директор ЗАО ИТФ "Системы и технологии",
г. Владимир.

Заслушав выступления и обсуждения в дискуссии, секция Автоматизированный учет электроэнергии и управление электропотреблением НТК НП "НТС ЕЭС" отметила:

В качестве постановки задачи, при подготовке докладов, использовались данные предоставленные коммерческим оператором (КО) ОАО "Администратор торговой системы".

Меняя порядок проведения проверок АИИС КУЭ Субъектов ОРЭМ, КО совершает действия, которые помимо "положительных" возможностей могут принести и потенциальные "опасности".

В докладе Генгриновича Е.Л. сформулирован ряд потенциальных угроз и методов их нивелирования, как с точки зрения Субъекта ОРЭМ, так и с точки зрения КО.

Например, такие как

1. Ошибки персонала
2. Преднамеренные действия по сокрытию (изменению информации)
3. Утечка информации
4. Ошибки программного обеспечения
5. Некорректная работа программно-аппаратных комплексов
6. Нарушения методологии работы
7. Искажения отчетности

Это конечно далеко не полный перечень рисков, какие-то из них могут быть более опасными, какие-то менее, причем для каждой конкретной задачи опасность одних и тех же рисков может быть разная. Поэтому проектирование системы информационной безопасности всегда начинается с построения конкретной модели угроз.

Отмечено, что целый ряд происшествий по всему миру, включая Россию, наглядно демонстрирует реальную опасность беспечного отношения к информационной безопасности при реализации тех или иных проектов. Современные технологии очень удобны, но, часто, настолько же уязвимы для внешних воздействий.

Для Субъекта ОРЭМ переход на дистанционные проверки и мониторинг АИИС КУЭ со стороны КО требует, прежде всего, разработки нового раздела ТРП на АИИС КУЭ или отдельного ТРП на информационное взаимодействие. Любая крупная компания имеет набор требований по организации доступа в ведомственную сеть внешних пользователей, поэтому, прежде всего, придется учесть внутрикорпоративные требования и найти решение, которое им бы удовлетворяло, затем необходимо будет учесть типовые решения и сценарии, которые в будущем утвердит КО. Таким образом, новый раздел ТРП (отдельный ТРП) необходимо будет согласовать как внутри компании, так и КО.

В докладе Генгриновича Е.Л. рассмотрены инструменты, которые могли бы быть использованы при установлении соединения между сетью КО и сетью субъекта ОРЭМ. Это, прежде всего, ДиодДанных – физическое устройство, гарантирующее на физическом уровне, однонаправленный поток данных из одного сегмента IP-сети в другой. Приведены примеры

оптимальной конфигурации, используемой для аудиторских и сервисных компаний и уже хорошо зарекомендовавшая себя во всем мире (МАГАТЭ, европейские регуляторы энергорынков).

Физическая идентификация при доступе в сеть Субъекта ОРЭМ - продукт Portnox компании Access Layer. Любое подключение к серверу КО или Субъекта, не важно, через какие средства виртуализации оно будет проведено, можно однозначно идентифицировать и принять решение о его допустимости.

Получение доступа к приложениям и базам данных - продукт PSM компании CyberArk.

Система внутреннего контроля за действиями пользователей – продукт Intellinx.

Все решения имеют солидную историю на рынке, включая целый ряд внедрений в России.

Определены организационные меры, которые необходимо проработать КО:

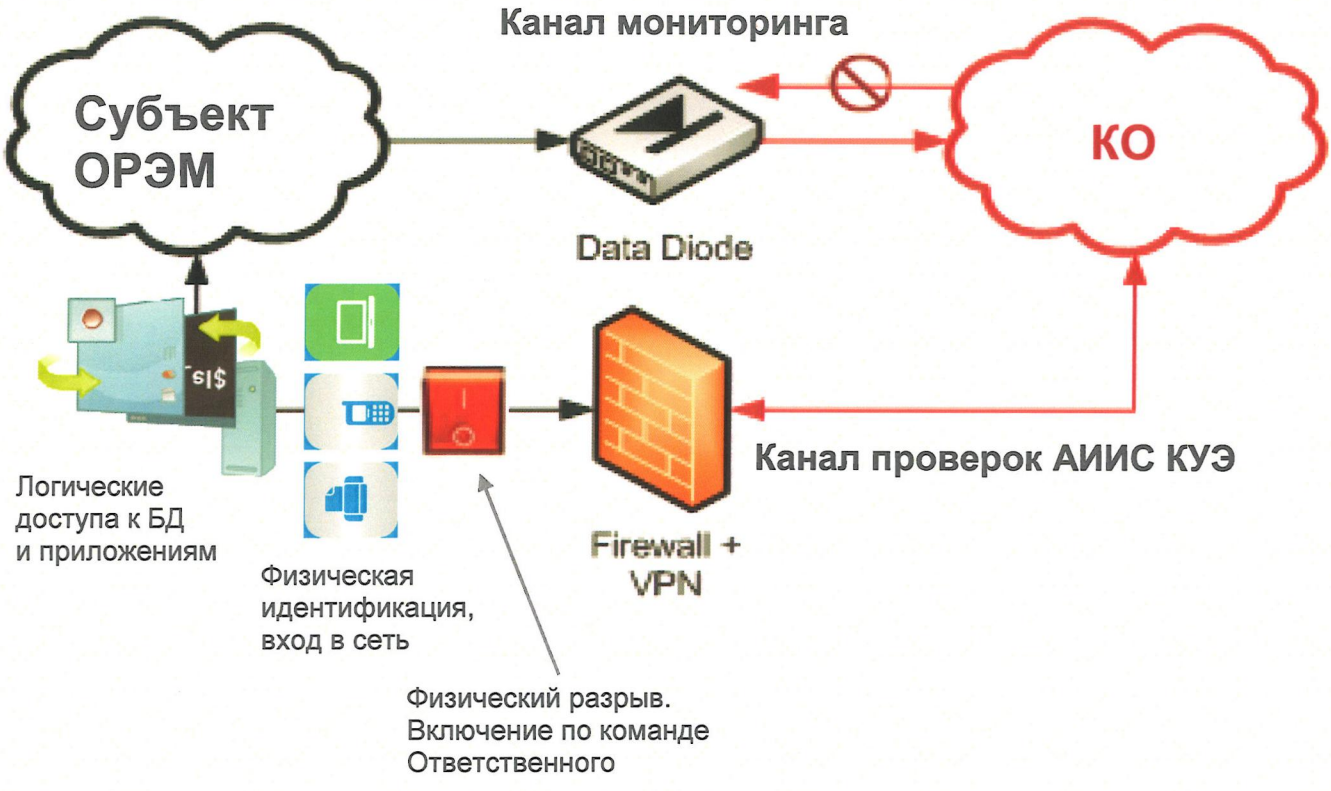
- Разработать, согласовать и утвердить проект организации выделенного сегмента информационной сети КО, в целях мониторинга, анализа и контроля АИИС КУЭ Субъектов ОРЭМ
- Выполнить работы по созданию и сдаче в эксплуатацию выделенного сегмента
- Разработать и утвердить:
  - перечень событий, форм, данных и отчетов АИИС КУЭ Субъектов ОРЭМ, которые будут подвергаться онлайн-мониторингу со стороны КО
  - перечень функций АИИС КУЭ Субъектов ОРЭМ, которые должны быть доступны КО при проведении дистанционных проверок
  - регламент проведения дистанционных проверок
  - типовые решения для систем безопасного информационного взаимодействия (БИВ) Субъектов ОРЭМ с КО.

А также возможный перечень требований КО к Субъектам ОРЭМ:

- В документации на АИИС КУЭ предусмотреть сценарии удаленного доступа со стороны КО (внести изменения в ПМИ, ТЗ, ТРП, протоколы предварительных испытаний), в соответствии с требованиями КО по мониторингу и проведению дистанционных проверок
- Доработать и сдать в постоянную эксплуатацию программное обеспечение АИИС КУЭ
- Разработать, согласовать и утвердить проект системы БИВ с КО
- Внедрить систему БИВ и предоставить КО результаты испытаний системы при вводе в постоянную эксплуатацию

Предложена схема безопасного информационного взаимодействия КО с Субъектами ОРЭМ:

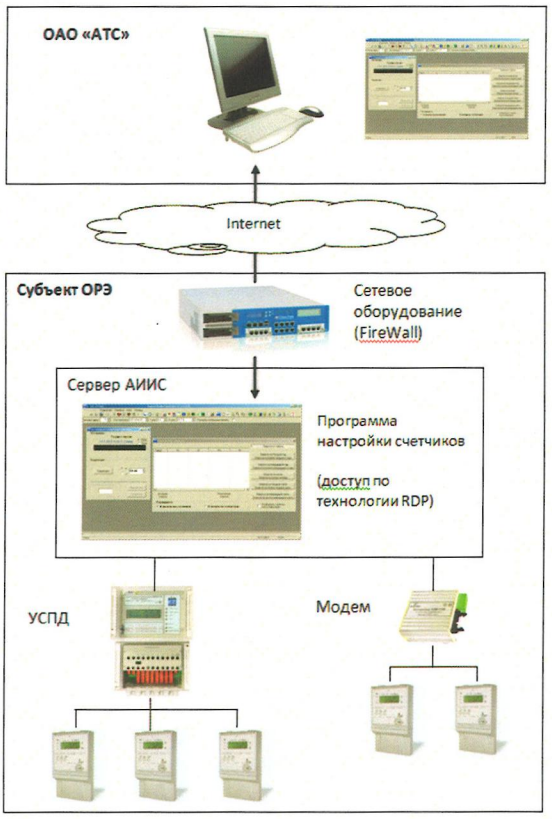
Схема безопасного взаимодействия



В докладе Генгриновича Е.Л. отмечено, что базируясь на международном опыте, данная схема обеспечит максимальный уровень информационной безопасности при гарантии реализации всех, запрашиваемых КО функций.

ЗАО ИТФ "Системы и технологии", как разработчик АИИС КУЭ, предоставил предложения по прикладным вариантам организации дистанционного доступа к системам КУ.

1. Быстрое решение



•Доступ к серверу субъекта ОРЭ через сеть Internet по технологии «удаленный рабочий стол» (RDP)

•Сбор данных со счетчиков при помощи «заводской» программы настройки. В случае трехуровневой системы – УСПД должен обеспечить «сквозной канал» до счетчика.

/чение конечных результатов и сравнение ние через дополнительное ПО (таблицы Excel).

Для реализации данного подхода в устройствах и программном обеспечении от ЗАО ИТФ "СИСТЕМЫ И ТЕХНОЛОГИИ" поддерживается "технология сквозного доступа" до счетчика.

Отмечены плюсы и минусы "быстрого решения".

Плюсы:

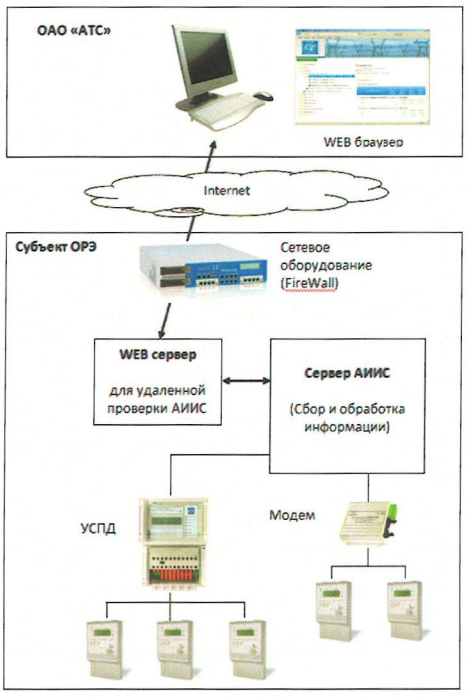
- Работа со счетчиками через заводское ПО (конфигуратор) обеспечивает высокую степень доверия данным и максимальный объем информации.

Минусы:

- Безопасность – внешний пользователь получает доступ к удаленному рабочему столу внутри корпоративной сети предприятия, а так же пароли на доступ к БД и счетчикам. Даже если отбросить злонамеренные действия пользователя возможны изменения настроек счетчика "случайным кликом" в конфигураторе.
- ПО настройки счетчика как правило не проводит аутентификацию оператора и не ведет журнал его действий, для контроля требуется "аналог видеорегистратора" работы с программой.
- При проверке применяется ПО от нескольких производителей с различными интерфейсами, требуется план сопоставления кодов точек выданных ОАО "АТС" и физических адресов устройств/каналов измерения. В результате не исключены ошибки при сопоставлении значений "от другого устройства" и методика испытаний будет достаточно сложной. Так же требуется отслеживать актуальность версии ПО конфигурирования счетчиков.
- Для получения конечного результата необходима дополнительная обработка данных (например умножение на коэффициент

трансформации в Excel), в ходе которой могут быть допущены ошибки и в результате принято неверное решение.

2. Предлагаемое решение



- Для удаленной проверки АИИС предоставляется WEB доступ к данным системы с правами только на чтение
- Через WEB интерфейс оператору доступны следующие функции:
- Получить данные и журналы событий из БД сервера АИИС.
- Опросить данные и журналы непосредственно со счетчиков.
- Выполнить сравнение значений счетчика с данными из БД и XML (80020, 80030, 51070)
- Сетевая безопасность обеспечивается набором типовых решений для WEB порталов.
- Все действия оператора журналируются.

Предлагаемое решение – это безопасность. Для WEB порталов имеется набор типовых решений по защите IT структуры предприятия на случай если требуется предоставлять доступ пользователям из общедоступных сетей (Интернет). В случае взлома WEB сервера "злоумышленник" не получит доступ к серверу сбора и базы данных.

Отмечены преимущества предлагаемого решения:

1. Механизм сбора данных со счетчиков в протестирован производителями ПО для АИИС (в частности "Пирамида 2000") и проверен при испытаниях на утверждение типа средства измерения, поэтому достоверность предоставляемых данных ни чуть не меньше чем при работе через конфигуратор счетчика.
2. У пользователя нет прямого доступа к серверу сбора и отсутствуют возможность изменения настроек системы. Даже в случае "атаки" на Web-сервер максимальный эффект – это временная недоступность сервиса удаленной проверки.
3. Доступ ко всем необходимым для контроля АИИС функциям через единый интерфейс – упрощается методика проверки. Проверяющий работает в терминах (кодах) АИИС без дополнительных таблиц соответствия - исключается путаница с переводом названий и отображаемых величин.

4. Аутентификация и журналирование всех действий пользователя в удобном для контроля и анализа виде – именно журнал событий, а не видео.
5. Возможность оперативного пересчета значений и сравнения данных в одной программной среде без дополнительных ручных операций переноса.

В обсуждении приняли участие: Член Правления - Первый заместитель Председателя Правления ОАО "АТС" Ананьев С.А., председатель секции Покатилов А.В. ОАО "АТС", заместитель председателя секции Щуров В.М. ОАО "НТЦ ФСК", Генгринович Е.Л. SNITE GROUP GMBH, Щитников А.Я. ЗАО ИТФ "Системы и технологии" г.Владимир, Егоров С.А. ЗАО ИТФ "Системы и технологии" г.Владимир, Крупин А.В. ООО "Прософт-Системы" г.Екатеринбург, Стефанов А.С. ОАО "СО ЕЭС" – ОДУ Центра, Новиков В.В. ФГУП "ВНИИМС", Коньков А.С. ООО "Русэнергоресурс", Валобуев Е.А. ООО "Русэнергосбыт", Здановский В.Е, ОАО "ФСК ЕЭС", Швейко Ю.Ю. ОАО "АТС".

В ходе обсуждений, было отмечено, что КО вынужден начать дистанционный контроль систем КУ, ввиду того, что количество выездных проверок на места увеличилось в связи с увеличением численности субъектов ОРЭМ, новым строительством, изменениями в Регламентах ОРЭМ, которые разрешили Гарантирующим поставщикам и Поставщикам электроэнергии (генерации) сдавать систему коммерческого учета по сечениям.

Отмечено, что дистанционные проверки будут затруднены, если оборудование системы коммерческого учета располагается на подстанциях сетевых организаций или потребителей розницы, а также на подстанциях ОАО "ФСК ЕЭС". Также сложности могут возникнуть, так как системы сбора весьма разнотипны и не всегда сценарий подходит для всех систем. Поэтому постановочной задачи КО для исполнителей заказа недостаточно. У КО накоплен достаточный опыт выездных проверок, поэтому исполнителям заказа необходим список операций, соответствующих программе испытаний, после чего будет дан ответ, может ли исполнитель выполнить заказ. Необходимо, чтобы программа испытаний была одинакова для всех субъектов ОРЭМ.

Отмечено, что дистанционные проверки и онлайн мониторинг АИИС КУЭ - естественный шаг в развитии коммерческого учета на ОРЭМ, но как любой новый шаг, он порождает новую систему взаимодействия КО и субъектов ОРЭМ. Новая система требует определить технологические, организационные, методические и юридические аспекты. Сегодня достаточно инструментов для организации безопасных дистанционных проверок и онлайн мониторинга АИИС КУЭ на ОРЭМ, а в дальнейшем можно предположить развитие системы на новый уровень, например переход на сбор коммерческой информации непосредственно КО, с предоставлением этой информации субъектам ОРЭМ.

Предлагается включить в план разработки регламентов оптового рынка, разработку необходимых документов, которые бы обеспечили поэтапный переход к системе удаленного мониторинга и дистанционных проверок АИИС КУЭ субъектов ОРЭМ.

Заслушав выступления и обсуждения в дискуссии, секция Автоматизированный учет электроэнергии и управление электропотреблением НП "НТС ЕЭС" приняла **следующие решения:**

1. Дистанционный доступ к системе коммерческого учета субъектов ОРЭМ с уровня коммерческого оператора технически возможен для большинства используемых на ОРЭМ систем коммерческого учета.
2. Для решения задачи контроля достоверности результатов измерений, передаваемых субъектами ОРЭМ коммерческому оператору необходим дистанционный доступ к счетчикам электрической энергии или УСПД.
3. Дистанционный доступ может применяться как с целью проведения испытаний и проверок систем коммерческого учета субъектов ОРЭМ, так и для непрерывного дистанционного мониторинга систем при их эксплуатации.
4. Сегодня достаточно инструментов необходимых для решения задачи организации безопасных дистанционных проверок и онлайн мониторинга АИИС КУЭ на ОРЭМ.
5. Организация безопасного канала связи для проведения дистанционных проверок и онлайн мониторинга АИИС КУЭ на ОРЭМ потребует дополнительных финансовых затрат, как со стороны субъектов ОРЭМ, так и КО.
6. Для внедрения дистанционного доступа необходимо разработать изменения регламентов оптового рынка, а также иных необходимых документов, которые бы обеспечили поэтапный переход к системе удаленного мониторинга и дистанционных проверок АИИС КУЭ субъектов ОРЭМ.

Заместитель Председателя научно-технической коллегии НП "НТС ЕЭС", д.т.н. _____ В.В. Молодюк

Председатель секции "Автоматизированный учет электроэнергии и управление электропотреблением", к.т.н. _____ А.В. Покатилов

Ученый секретарь научно-технической коллегии НП "НТС ЕЭС", к.т.н. _____ Я.Ш. Исамухамедов

Ученый секретарь секции _____ С.Ю. Чистякова