



**Некоммерческое партнерство
«НАУЧНО-ТЕХНИЧЕСКИЙ СОВЕТ
Единой энергетической системы»**
109044, Россия, Воронцовский пер., 2, стр.1
Тел. (495) 912-10-78, 912-57-99, факс. 632-72-85
www.nts-ees.ru

ОТЧЕТ

**заседания секции «Автоматизированный учет электроэнергии
и управление электропотреблением»**

НП «НТС ЕЭС»»

по теме:

Кибербезопасность РЗА и АСУТП

Москва, 2017 г.



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»,
д.т.н. профессор

Н.Д. Роголев

«06» октября 2017 г.

ПРОТОКОЛ

**заседания секции «Автоматизированный учет электроэнергии и управление
электропотреблением» НТС ЕЭС**

по теме

«Кибербезопасность РЗА и АСУТП»

28.09.2017 г.

№ 7

г. Москва

Присутствовали: 15 человек (список прилагается)

На заседании выступили:

С вступительным словом о работе секции председатель секции «Автоматизированный учет электроэнергии и управление электропотреблением» А. В. Покатилов. Сообщил о состоявшейся 4-5 октября 2017 года в рамках российской энергетической недели 2017 2-ой отраслевой инновационной конференции, Строительство цифровой экономики является на сегодняшний день одной из основных стратегических задач, поставленных Президентом и Правительством Российской Федерации. Данные и создаваемую на их основе информацию следует рассматривать как самостоятельный фактор производства, позволяющий влиять на его эффективность, производительность труда, надежность и безопасность энергоснабжения. Цифровизации сейчас предается первостепенное значение, считается, что с помощью таких методов можно «оживить» экономику России. Следовательно, возникают вопросы и обеспечения безопасности информационных сетей.

С основным докладом «Кибербезопасность РЗА и АСУТП», выступил Генгринович Евгений Леонидович, АО «ИнфоТекс» (Приложение 1).

Евгений Леонидович добавил к вступительному слову, что он входит в рабочую группу Наталья Касперская, которая по программе «Цифровая экономика» отвечает за направление «Информационная безопасность». К началу октября в рамках программы готовится расширенная программа по мероприятиям нормативно-технического регулирования и по стандартизации, связанных с тем, чтобы поддержать работу по постановлению правительства, подписанному Медведевым в августе 2017 года. Задача всех рабочих групп – сформировать программу, которая сможет попасть в бюджет уже начиная с 2018 года для того, что бы обеспечить ее финансирование. Поэтому вопросы информационной безопасности сейчас крайне актуальны, мы находимся на том этапе, когда еще можем повлиять на ряд моментов с точки зрения отрасли.

Сегодняшняя встреча обусловлена тем, что в июле 2017 года был подписан Федеральный закон 187 о безопасности критической информационной инфраструктуры. Есть поручение Президента о выпуске ряда Постановлений Правительства по определению критериев, механизмов и процедур реализации Федерального закона. Первые законодательные акты уже принимаются - принято Постановление Правительства по критериям ранжирования компаний, которые занимаются эксплуатацией критической информационной инфраструктуры. Определен федеральный орган исполнительной власти (ФОИВ), ответственный за реализацию этого закона. Активно ведется подготовка других документов.

Критическая информационная инфраструктура широкое понятие, мы ограничим этот круг инфраструктурой электроэнергетики. Кибератаки на энергообъекты по всему миру связаны с тем, чтобы нанести ущерб третьей стороне, так как сегодня электроэнергия играет серьезную роль в любом производственном процессе, в любой системе контроля, в медицинских центрах и так далее. Сейчас на энергетических объектах идет интеграция с IT, технический процесс выработки, передачи и распределения электроэнергии превращается в мультифункциональный процесс, на каждом этапе которого необходимо решать как сложные технологические задачи, так и формировать сложные алгоритмы со стороны IT. Это касается и измерительных приборов, и заправок для электротранспорта, и энергосервисных контрактов. С точки зрения ранжирования процессов (из опыта испанской компании магистральных сетей) все задачи делятся на три части: задачи критичные для исполняемого процесса, задачи критичные для бизнеса и задачи, которые обеспечивают большую эффективность бизнеса (более высокую маржинальность). Государство во всем мире регулирует только задачи критичные для самого процесса (опасность для людей, предотвращение техногенных катастроф). Две другие задачи – задачи бизнеса, заключающиеся в зарабатывании денег. Но, в связи с тем, что идет

модернизация систем и подходов, наблюдается интеграция задачи бизнеса в непосредственный технологический процесс.

Интересные исследования год назад провел казанский «Университет Иннополис», опросив более 100 руководителей и ведущих специалистов отделов ИБ крупнейших компаний России, выявила следующую статистику: большая часть специалистов ИБ проблему видят не во внешних факторах, а во внутренних, в собственных сотрудниках. Фактически, во многих даже крупных российских компаниях не выстроены процессы информационной безопасности контроля и разграничения доступа. В модели нарушителя одной из крупных российской компаний внутренний нарушитель выведен из списка, и сделано допущение, что т.к. персонал набирается отделом кадров и проходит определенные проверки при наборе, он не может повлиять на работу информационной системы. Такие допущения могут привести к не корректной работе модели нарушителей.

Говоря о понятии «киберинциденты» мы представляем некоего злоумышленника, внутреннего или внешнего, на самом же деле, при современном уровне развития микропроцессорной техники и интеграции ИТ в процессы, киберинциденты чаще возникают из-за человеческого фактора (ошибок персонала), из-за переконфигурации тех или иных устройств, выхода из строя микропроцессорной техники. Конечно, злонамеренные воздействия так же имеют место быть. Необходимо выстроить внутренние процессы, которые обеспечивали бы, защиту от киберинцидентов, многократные проверки и возможность контроля того, что происходит на объектах с точки зрения информационной среды.

На сегодняшний день согласно мировой статистике из 100 инцидентов, только два классифицируются как кибератаки. При этом существует довольно большая серая зона, которая возникает из-за отсутствия инструментов контроля ситуации на объекте информационной составляющей. Закономерно, что информационная безопасность сначала развивалась в ИТ, в первую очередь в финансово-банковских системах, там она доведена до высокого уровня. Но там решилась немного другие задачи, а когда эти задачи начали менять вектор и переходить в область критической информационной инфраструктуры, выяснилось, что копирование методов и средств задачу не решает. Причина в том, что другая среда, другие сроки эксплуатации оборудования, установка патчей – нетривиальный процесс. В любой технологической среде сам процесс отточен до мелочей, с информационной точки зрения - поставленные процессы просто отсутствуют. Актуальность вопроса информационной безопасности объясняется так же следующими изменениями: ранее в технологических процессах был задействован только персонал подстанции, сейчас же можно загрузить конфигурацию в контроллер терминала РЗА

находясь в другом городе, можно ретранслировать данные надзорным органам, часто привлекают аутсорсинговые компании и так далее. Поэтому надо понимать, что данные изменения влекут за собой определенные последствия.

Далее докладчик рассказал о моделировании процессов в электроэнергетике. Международная квалификация позволяет разделить процессы на несколько уровней от бизнеса до объекта и уровней компонентов. Для каждого уровня решения будут отличаться, однако безопасность создает только совокупность решений. При этом надо понимать, что процесс обеспечения безопасности постоянный, требующий регулярного анализа и исследования векторов атак, и соответственно, корректировки методов защиты. Так же сама система безопасности при внедрении должна быть проанализирована как новый потенциальный источник атаки. Еще одна проблема это разность пониманий и разность приоритетов у ИТ, ИБ и технологов. Если выполнять требования ИБ по полному ограничению рисков, то и сам технологический процесс придется останавливать, что невозможно. Поэтому в первую очередь нужно обеспечить выполнение и реализацию самого технологического процесса, и при этом обеспечить требования безопасности, что возможно, если уделить внимание данной задаче.

Существует ряд типовых проблем информационной безопасности:

- ИТ в промышленности не всегда управляется должным образом, то есть процессы отлажены, а информационное обеспечение не регламентировано.
- Сети SCADA уязвимы, потому что не проводился анализ векторов атак при переходе от изолированных сетей к иерархическим сетям с точки зрения безопасности.
- Сближение ИТ и ОТ, потому что многие контроллеры содержат программное обеспечение, много измерительных приборов содержит алгоритмику.
- Разрыв в психологии между специалистами по безопасности и специалистами АСУТП.
- Широкое поле для атак – удаленный доступ, внутренние угрозы, более 40000 промышленных компонентов уже доступны при помощи публичных сетей (shodan.io).

На сегодняшний день не только защита от хакеров является важным моментом, но и возможность обеспечить нормальную эксплуатацию оборудования и систем управления. За счет контроля информационной среды можно выявлять большое количество технологических и информационных параметров. Не уделяя должного внимания отслеживанию этих параметров, мы узнаем о выходе за установленные нормы показателей по факту этого свершения. А контроль информационной среды позволяет

выявить ситуации, когда возникло какое-либо отклонение от стандартной жизнедеятельности системы. Три базовых направления – оперативное управление, локальная сеть и информационная безопасность, по каждому из этих направлений можно получать дополнительную информацию и имея сетку анализа, основываясь на полученных данных принимать обоснованные решения. Помимо регламентации требований, то чем всегда оперирует информационная безопасность, подобного рода мероприятия могут так же влиять на ROI (окупаемость инвестиций), оптимизировать информационный процесс, обеспечивать объем ремонтов и непрерывность бизнеса.

Определение из документа NIST 1800-7B (DRAFT) SITUATIONAL AWARENESS (SA) для отрасли электроэнергетики звучит так, SA - это «контроль событий во времени и пространстве, осознание их смысла и оценка их влияния на ближайшее будущее». Цель – знать, что происходит вокруг вас, и как это может повлиять на вашу деятельность.

Фактически мы не боремся с атакующими факторами, а обеспечиваем киберустойчивость. Она обеспечивается за счет того, что мы пытаемся понять, что происходит на этапе, когда еще нет каких-либо внешних проявлений. Известно, что средства атаки развиваются вместе со средствами защиты, поэтому идти по пути заблаговременного вычисления кто и откуда может тебя атаковать не совсем верна. Мы же подходим с другой стороны, самое важное это сам процесс – он описан, есть понимание как он должен работать, есть эксперты, которые могут определить какие режимы нормальные, а какие не нормальные. Соответственно, запускается циклический контроль, постоянная оценка текущей ситуации с определенной периодичностью. Как только появились отклонения, вирус или ошибка персонала или неисправность какого-либо оборудования, это уже факт, который необходимо изучить, расследовать и принять какие-то меры. Статистика успешных атак, которая была собрана в мире, говорит о том, что инкубационный период компьютерной атаки занимает от года до трех. Что такое инкубационный период? Это период, в процессе которого, вредоносное ПО изучает конфигурации и ищет уязвимые места для того, чтобы нанести максимальный ущерб атакуемому объекту. Помимо технологических стандартов на западе существуют организационные стандарты, серия ISO/IEC 27001 – говорит о том, как управлять безопасностью. Россия в этом плане отстает примерно лет на 6, мы используем стандарт 2006 года, а зарубежом уже используется стандарт 2013 года. Стандарты в свою очередь являются ответом на изменения/развитие инфраструктуры. На основании этих стандартов все электроэнергетические компании Евросоюза должны пройти аттестацию по требованиям ISO/ IES TR 27109: 2013 до 30.01.2018 года. Это жесткое требование будет на первом этапе распространяться на развитые страны (Германия, Франция, Нидерланды,

Испания), Восточная Европа немного отстает, но система организации управления безопасностью должна быть доведена до определенного уровня и должна соответствовать тем технологиям, которые внедряют на объектах.

В России самым актуальным документом в области кибербезопасности является ФЗ №187 «О безопасности критической информационной инфраструктуры РФ» от 26.07.17, а так же ФЗ №193 «О внесении изменений в отдельные акты РФ в связи с принятием ФЗ-187». Эти ФЗ определяют новый подход к защите критической инфраструктуры, определяют персональную ответственность вплоть до уголовной для руководства компаний, которые отвечают за эксплуатацию инфраструктуры, в случае если технически эта безопасность будет обеспечена не должным образом, либо будет вестись не соответствующим образом организационно. В ФЗ определены критерии отнесения к разным группам, что будет обязывать на законодательном уровне всем заняться информационной безопасностью. Первый драфт 187-ФЗ был внесён в Госдуму еще в 2012 году от имени ФСБ, но за все эти годы, не одно из отраслевых министерств не проявило желание принять участие в его рассмотрении. В результате, пока не вышли Постановления Правительства, было не понятно как предполагается этот ФЗ исполнять технически и за какие средства, сейчас там прописано, что компании должны это обеспечивать в рамках текущей эксплуатационной деятельности. Сейчас в рамках цифровой экономики формируется перечень того, что мы должны сделать в ближайшие пять лет до 2023 года и, имеет смысл, что в увязке с этим Законом, отраслям более активно поучаствовать в формировании более комфортной ситуации.

Так же, докладчик отметил, что введена в работу ГосСОПКА (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак). Все компании, которые будут отнесены к критической инфраструктуре, а энергетика процентов на 80 будет к ней отнесена, будут предоставлять данные в ГосСОПКУ по защищенным каналам с уровнем самих объектов. В этой связи возникает ряд вопросов технического и организационного обеспечения. Все что связано со средствами защиты информации в Российской Федерации имеет ограничения в работе еще больше чем с метрологическим обеспечением оборудования, идет наслаивание требований организационных и технических регламентов. В энергетике существует Постановление Правительства по расследованию системных аварий. Согласно этому Постановлению выпускаются приказы по расследованию аварий внутри компаний. На сегодняшний день в перечне причин аварий вариант киберинцидента просто отсутствует. Из чего следует, что расценить аварию как киберинцидент не предоставляется возможным, по этой же причине в комиссии отсутствуют профильные специалисты. Изменить эту ситуацию можно путем

корректировки Постановления Правительства, добавив такую причину аварии, как киберинцидент и при анализе ситуаций проводился информационный SA анализ.

На этом Евгений Леонидович закончил первую ознакомительную часть своего доклада и участники заседания секции задали свои вопросы и высказали свои мнения по поводу освещенной темы. В обсуждении приняли участие представители ФГУП «ВНИИМС», ПАО «Мосэнерго» и т.д.

Виктор Федорович Чернецов сообщил о том, что в энергетике есть нормативные документы, которые требуют обязательного расследования всех аварийных инцидентов и несчастных случаев. В них есть определенная классификация и при анализе любого инцидента будь то, отказ по вине первичного оборудования, по вине сбоя релейной защиты или АСУ ТП, везде в конечном итоге – мы приходим к человеческому фактору. Так было на Саяно-Шушенской ГЭС и ледяной дождь в Москве (это не только погодные условия, сколько поросли льда, которые не должны образовываться, это просто халатность персонала). В отношении кибербезопасности – как правильно отметил докладчик, сейчас пока ни в каких инструкциях данный вопрос не прописан. Надо внести соответствующие корректировки и анализ на эту тему, начав работу в этом направлении. Раз есть фактор вмешательства, то точно нужны и технические средства и организационные мероприятия для того, чтобы этого не допустить. Другой вопрос, что если это не будет работать в полуавтоматическом (а лучше в автоматическом режиме, то это могут быть деньги на ветер).

Участие в дискуссии принял Владислав Анатольевич Бедин. Отметив, что кибербезопасность состоит из технической и организационной части, он поинтересовался есть ли какая-то дорожная карта или алгоритм действий? Присоседился к вопросу и Александр Васильевич Покатилов, высказав свое сложившееся впечатление, что для безопасности надо ото всего отключиться, в интернет не выходить и так далее. Вопрос к докладчику, какие именно действия надо предпринять, чтобы обеспечить кибербезопасность на предприятии.

Евгений Леонидович дал ответы на озвученные вопросы – не существует универсального рецепта, который бы обеспечивал безопасность. Безопасность это процесс, некая цель, к которой надо идти. Завтра поменялась какая-то технология или какое-то решение, следовательно, на безопасность надо смотреть уже с другой стороны. Необходимо постоянное развитие. В принципе, первая часть доклада как раз подразумевала рассмотрение кибербезопасности с разных аспектов, с функциональной безопасности, с текущего состояния информационных потоков и так далее. В России с учетом того, что вышел очень жесткий закон, и нет сформированных Постановлений

Правительства, а дальше под Постановления Правительства, скорее всего, будут формироваться какие-то СТО компаний, ведомственные требования и т.д. Поэтому сейчас сказать, что надо делать только так или по-другому, будет неправильно.

Владислав Анатольевич привел пример Федеральной Сетевой Компании (ПАО «ФСК ЕЭС»), где проблема решается следующим образом, ограждаются ото всего, никуда не пускают никого, то есть они просто не пускают никого в свои сети. На что Евгений Леонидович отметил, что на сегодняшний день, изоляция как таковая микропроцессорного оборудования это уже устаревшее решение, которое не исключает опасности.

Александр Васильевич обратил внимание, что в докладе много информации о западном опыте и поинтересовался, как обстоят дела в Китае. Евгений Леонидович ответил, что в Китае кибербезопасность развита очень хорошо, они пытаются идти в ногу с Америкой и наравне со многими другими странами уже имеют свои кибервойска.

Продолжая доклад, Евгений Леонидович отметил, что в отношении информационной безопасности чаще всего информация не открытая, поэтому доклад будет основан на продукции компании, которую он сейчас представляет. На их примере будет показано, какие инструменты могут быть использованы для защиты критической инфраструктуры.

Сеть делится на несколько сегментов, IT это уровень, где работают ERP, MES системы, и два уровня это непосредственно уровень системы АСУ, ТИ и уровень исполнительных устройств ПЛК, которые установлены на объекте. Соответственно инструменты для уровней различаются, вектора атак могут идти как снизу вверх, так и сверху вниз. Сейчас работы идут с различного вида шифраторами, которые обеспечивают по ГОСТу зашифрованный канал для передачи данных, содержание которых является важным для компании или для какого-либо процесса. Второй момент это анализ сетевых инцидентов и нестандартного поведения. И третье, база опыта компании по выявленным различным сигнатурам атак, поиск вирусов. На уровне АСУ ТИ это тоже шифраторы, которые позволяют обеспечить зашифрованный канал и взаимодействие с такими системами как ГосСОПКА, и появляется встраиваемая линейка решений. Что такое шифрация? Шифрация - прежде всего время, которое вам необходимо на изменение информации по определенному алгоритму, чтобы она была недоступна другим. Когда мы говорим о быстрых процессах или объектах, таких как цифровая подстанция, которые работают по протоколу 61050 – времени нет, его физически не хватает. Тем не менее, достоверность данных очень важна, мало того просто необходима. Разработанное решение встраивается в оборудование других производителей. Оно позволяет взаимодействовать с контроллером, получать информацию, вставляя туда что-то типа

электронной подписи, которая фиксирует соответствие этой информации на самом устройстве и на уровне системы, которая эту информацию использует. Так как она стоит не в разрез, то время на ее работу практически минимальное и процесс не останавливается. Соответственно, если брать полевой уровень, то здесь шифрование канала, используется промышленный межсетевой экран с обеспечением ГОСТ VPN канала. При этом надо понимать, что сам по себе алгоритм шифрования не содержит какой-то логики, они известны, они описаны. Основной вопрос в этих системах это вопрос с ключами. Как счетчик, например, требует поверки раз в три года, так алгоритм требует полной замены всех ключей раз в год или раз в три года, это все регулируется и так же, как и коррекция времени работает эффективно только при наличии комплекса, а не отдельной железки установленной на объекте.

Сейчас в России есть порядка 3-4 производителей, которые специализируются на системе комплексной защиты информации и криптографии, одна из этих компаний Infotecs. Преимущество компании состоит в комплексной системе управления ключами (изначально разрабатывалась для ЦБ, так же используется для системы Visa в России). Есть много зарубежных аналогов, которые предлагают подобные линейки, но они используют VPN не в соответствии с ГОСТ (не российские). Есть два вопроса – соответствие российскому законодательству по протоколу, второе – по стойкости ключа, с точки зрения управления ключами. По смыслу можно провести аналогию с синхронизацией времени. Сейчас появились требования по межсетевым экранам типа Д, хотя в России на сегодня сетевой экран такого типа отсутствует, их просто нет. Аналогию, опять же, можно провести с требованиями по коммерческому учету на оптовом рынке, когда появились требования, оборудования, им удовлетворяющего еще не было. Требования по типу Д очень жесткие, и сейчас компания Infotecs работает над доведением своего устройства до соответствия им. Требования к корпусу, к эксплуатационным характеристикам меняются в зависимости от модели нарушителя.

Евгений Леонидович подробнее рассказал по поводу встраиваемых средств защиты. Встраиваемые средства защиты ставятся непосредственно на уровень объекта. Сам модуль встраивается внутрь как релейного терминала, так и контроллера АСУ ТП и фактически обеспечивает передачу данных и на верхнем уровне выполняются две функции: управление ключами и расшифровка для обеспечения работы всех приложений.

Докладчику был задан вопрос: поставлен счетчик, в котором поставлено устройство, с криптографической защитой. Для того, чтобы попасть на прибор, раньше можно было подойти и накинуть оптопорт, набрал 1111, сейчас же при использовании криптографического оборудования такое невозможно, необходимо будет каждое ПО

сертифицировать и управлять ключом, все ли верно? Евгений Леонидович пояснил, что это не так. Верно то, что взять любой попавшийся ноутбук, и подойти к прибору будет нельзя, будут определены ноутбуки, которые используются для конфигурации и настройки тех или иных устройств. Эти ноутбуки будут идентифицированы как ноутбук, который имеет право доступа на данный прибор. Когда подойдешь к счётчику с этим ноутбуком - все будет нормально, а вот с другими ноутбуками подойти не получится. Ключи на ноутбуках могут выдаваться на час, два или сутки, с целью предотвращения опасности, в случае кражи ноутбука.

В своей презентации Евгений Леонидович продемонстрировал сам криптомодуль, отметив его небольшие размеры. Модуль является пассивным, если к нему обращаются, то он отвечает. Существует ГОСТ на алгоритмы, модули обеспечивают хранение ключей и сертификатов, могут быть установлены прямо внутри контроллера. Так же, был продемонстрирован высокопроизводительный криптосервер.

Далее докладчик коснулся стандартизации. При ТК26 «Криптографические механизмы для М2М и промышленных систем» создана рабочая группа №4, задачей которой является стандартизация использования национальных криптографических механизмов в стандартах МЭК 60870-5-101/103/104. Были проведены консультации с рядом представителей отрасли, и общим мнением стало то, что наиболее важно на первом этапе получить данную возможность в 104 протоколе, так как этот протокол используется для магистральной ретрансляции данных по технологическим объектам в электроэнергетике. Стандарт 60870 по своей сути это международный стандарт, в нем есть раздел связанный с криптографией. Методы криптографии, которые там заложены - формально не соответствуют требованиям законодательства, которое на сегодня действует в Российской Федерации. Что такое криптография внутри алгоритма? Это когда устройство работает в 104 протоколе, и он сразу без всяких модулей накладывает дополнительные криптографические элементы на передаваемую информацию. Для того, чтобы реализовать это в соответствии с российским законодательством предложен протокол защищенного обмена для промышленных систем, сейчас активное участие в обсуждении проекта принимают представители Системного оператора ЕЭС и НТЦ ФСК ЕЭС. Базовые принципы предложенного решения – минимальные задержки обработки, минимальное увеличение объема информации при криптографии, предварительно распределенные ключи, проверка их стойкости и так далее. Во всем мире только часть информации подлежит защите, ее необязательно защищать всю. Так же, это касается только определенного типа объектов, не всех. Поэтому, если объект не попадает под определенные критерии или там нет информации, которую надо защищать, изменение

стандартизации не будет влиять на базовую часть 104 протокола. Но если объект попадает под какой-либо критерий или содержит часть информации, которую надо защищать, то есть два выхода. Первый выход - покупать дорогое устройство, формировать защищенный канал и тратить деньги на то, чтобы его полностью формировать с нуля. Второй - многие зарубежные производители выпускают оборудование, на котором предусмотрено модульное наращивание и к этому оборудованию будут выпускаться модули, которые будут поддерживать программно-реализуемые компоненты. Или же возможен «upgrade» прошивки, которая уже стоит. То есть, наличие такого стандарта (а при его выходе его должны будут поддержать производители) для отрасли это существенное снижение затрат на выполнение обязательных требований регулятора по обеспечению безопасности. Другой вопрос, если производители не включатся на этапе разработки стандарта, а после его выхода будут вносить изменения в программное обеспечение и какое-то время их еще реализовывать, то на рынке получится некий разрыв. Евгений Леонидович отметил, что в случае заинтересованности темой стоит принять участие в работе созданной группы.

Докладчик рассказал о НИОКР и НИР, которые сейчас проводятся разными службами, в том числе и Минэнерго. Минэнерго проводит разработку научно-обоснованной концептуальной онтологической модели и семантического описания ЕЭС России. Онтологическая модель это описание процесса и объекта и взаимосвязи между ними, после этого формирование какой-либо прикладной области. По инициативе Минэнерго после выхода 187 ФЗ сейчас идет проработка модели рисков для данной модели и для объектов электроэнергетики. Цель – защитить саму модель, т.к. для любого хакера это является источником очень ценной информации. Модель рисков в онтологической модели с точки зрения организационного управления информационной безопасностью обеспечит более высокий уровень управляемости безопасностью объектов, чем есть сейчас.

Безопасности не бывает без модели угроз и модели нарушителя, то есть для начала определяется от чего мы защищаемся и какие проблемы хотим решить. На основании либо модели угроз, либо каких-либо стандартов строится метрика рисков (что в каком случае от чего зависит) и на основании этой метрики производится оценка текущего состояния. Алгоритмы оценки критичности рисков транспонируются по уровням, например: безопасность, комплаенс, производительность, бренд и финансы.

Говоря об онтологической модели и ее месте в области работы с рисками по ИБ, Евгений Леонидович отметил, что есть ряд технических задач, таких как оценка киберугроз, управление событиями, управление уязвимостями и есть система принятия решений по показателям бизнеса. И здесь есть проблема в части различий в методах,

терминологии и технологии, т.е. специалист по безопасности не всегда четко может объяснить проблему с точки зрения бизнеса. Хорошо описанная онтологическая модель это как раз тот инструмент, который в состоянии транслировать информацию и представить ее в том виде, который будет понятен руководству.

Евгений Леонидович поделился информацией о западном опыте построения решений на примере онтологических моделей компании TENNET (магистральная сетевая компания Германии и частично Нидерландов) и компании Siemens.

На сегодняшний день в России ряд объектов Россетей уже включен в онтологическую модель, ведутся пилотные проекты, есть реальные внедрения, идет подготовка в этой области к ЧМ-2018. Кибербезопасность в нашей стране стоит воспринимать не как далекое будущее, а как реальное настоящее.

В обсуждении и дискуссии приняли участие:

Представители Ассоциация «НП Совет рынка», ФГУП «ВНИИМС», ООО «Ситиэнерго», АО «Инфотекс», ПАО «Мосэнерго».

Часть вопросов участники заседания секции задали по ходу доклада, учитывая большой объем презентации. После окончания презентации обсуждали следующие вопросы:

- Вопрос по поводу нормативной документации, законов/подзаконных Акты или их проектов.

Ответ – Назначен ФОИВ, организующий всю эту работу. Существует проект Постановление Правительства «Об утверждении показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, а также порядка и сроков осуществления их категорирования».

- Правильное ли понимание сложилось, что сейчас первым делом определяют различные категории объектов, к разным категориям будут разные требования.

Ответ – Все верно, Законом предусмотрен перечень критериев, каждый должен их прочитать, и отнести себя к тому или иному критерию. Однако предусмотрено и то, что ответственный ФОИВ запросит доказательства соответствия выбранному критерию и/или порекомендует выбрать другой критерий. В первом случае идет проверка аналогичная защите тарифа. Прозвучало мнение участников заседания о том, что все будут причислять себя к наиболее простым критериям. Докладчик ответил, что тогда, в случае совершения киберинцидента, будет проводиться расследование, и обнаружится недобросовестный выбор критерия, который будет

наказываться. Евгений Леонидович отметил, что пока 187 ФЗ написан как «дубинка» (там прописано, что руководители предприятий несут ответственность за любые информационные инциденты на предприятии), но после выхода разъясняющих Постановлений Правительства должны появиться так же «пряники».

- Участник секции провел аналогию с ситуацией по промышленной безопасности особо опасных объектов. Была рассмотрена эволюцию применения этого закона. Сначала объекты в целом относили к особо опасным, потом сказали, что у государства нет денег и стали относить отдельные зоны объектов к особо опасным, в любом случае, если нет денег на реализацию – найдутся механизмы к упрощению применения тех или иных требований, которые прописаны в законе.

Ответ – промышленная безопасность это система обеспечивающая безопасность жизни людей, защиту от взрывов. Закону о промышленной безопасности не было уделено должное внимание со стороны отрасли, поэтому он был принят в таком виде. Надо понимать, что если не заниматься информационной безопасностью, то она начнёт влиять на функциональную безопасность.

Докладчик сообщил о своем участии в группе безопасности релейной защиты и АСУ ТП СИГРЭ, делали разбор простого кейса. В Постановлении Правительства по разбору аварий сказано, что взрыв на трансформаторе 110 кВ и выше это серьезная системная авария, которую необходимо рассматривать. Далее, берем учебник и читаем, в результате чего может произойти взрыв трансформатора – проблемы с обмотками и т.д. Одна из возможных причин это перенапряжение, подаваемое на обмотку в течение определенного времени. Сегодня РПН чаще всего управляют уже автоматизированные устройства, контроллеры и так далее. Если стоит одно значение, а по каким-то причинам (ошибка персонала или зло намерение) в течение какого-то времени будет подаваться перенапряжение трансформатор выйдет из строя. В заключении, если никто не будет проверять что было на контроллере, скорее всего, будет заводской брак или ошибка персонала. То есть причины будут отнесены к физическим проблемам, а не к тому, что это было вызвано целенаправленным действием.

- Может ли система информационной безопасности в перспективе выстроить рейтинг персонала по его значимости в технологических процессах и рекомендации к оптимизации, чтобы эти высокопрофессиональные люди не попадали под эту угрозу?

Ответ – На одном из слайдов прозвучал термин «киберустойчивость», он предполагает защиту от «дурака» и становится понятнее, что мы делаем, и от чего мы защищаемся. Системы по профилированию персонала есть, их два типа. Защита конечных устройств - на основе технологии машинного обучения, далее информация попадает под некий набор правил, и люди проверяют, что правила соответствуют политике компании. После того, как политике компании соответствует, любое изменение на компьютере (запуск новой программы) будет проанализировано. Оно либо будет разрешено оператором, либо (когда была, например, скачана программа или картинка из интернета) это будет отмечено как аварийная ситуация, система это отследит, будет несоответствие тому набору правил, и компьютер будет изолирован. Это один из типов систем, которые могут быть использованы для решения поставленной задачи. Второй тип, это системы, в которых есть требования, и есть инструмент для проверки этих требований. Системы уже полностью безагентские (в отличие от первого типа), получают информацию из базы и выстраивает оценку происходящего с точки зрения нормальной ситуации (требования – это некий набор правил что принимать за норму). Эти правила прописываются аналитиком и все, что от этих правил отклоняется, это инцидент, который нужно рассматривать.

- Прозвучал вопрос о сроках реализации, предусмотренных законом.

Ответ – Закон вступает в силу с первого января 2018 года. Далее будут разрабатываться программы, они будут согласовываться с региональными ФОИВами, будет вестись контроль их выполнения.

С отдельным мнением по теме заседания выступил Осика Лев

Константинович, Фонд «Энергия без границ», член секции:

Во всем новом должен быть здравый смысл. Стоит сказать, что абсолютизировать информацию не стоит, но и недооценивать, тоже не стоит. Технологическая система на любом уровне не может существовать без обмена информации. Невозможно оценивать любое новое направление (а кибербезопасность это новая область) в отрыве от исторического подхода. А история здесь даже не в том, что информация меняется, она может быть аналоговой, цифровой, информация это любое изменение. По жизни в технологических системах происходил отрыв различных областей от единой системы производства. Например, надежность, сколько было создано ГОСТов в области надежности, сколько было специалистов в области надежности и так далее. Всегда любой

инженер не может не создавать, не эксплуатировать систему не обращая внимания на этот показатель, он просто не говорит, что это надежность (он «чувствует», его учили, как делать так, чтобы система работала безотказно, бесперебойно с теми параметрами, которые в ней заложены). Точно так же информация, ее нельзя отрывать от технологической системы. Сейчас мы работаем на электростанциях, на подстанциях, в электрических сетях, мы ежедневно пользуемся информацией, и по жизни обеспечиваем, как можем, информационную безопасность. Задача любого инженера сделать так, чтобы и информационно, в том числе, выполняла ту функцию, для которой была создана. Кибербезопасность воспринимается сейчас излишне обособленной. Кибербезопасность направлена на цифровую форму, на микропроцессорные или вычислительные устройства, но все-таки, она связана с новыми цифровыми носителями, которыми мы обмениваемся. Это все равно часть той большой системы, в которой мы как инженеры все работаем, проектируем, эксплуатируем и так далее. Здесь есть предмет работы, она конечно необходима, но ее стоит ограничить, и не приравнивать к другим видам безопасности. Правильно было сказано, что у нас есть закон о промышленной безопасности и он определен. Во первых безопасность это состояние защищенности. По жизни и по физике есть понятие безопасность, есть химическая безопасность, ядерная безопасность, экологическая безопасность, информация – является тем фактором, который обеспечивает все реальные безопасности. Говорить о безопасности фактора, наверно можно, но это с точки зрения терминологии не совсем логично. Помимо информационной безопасности есть человеческий фактор, мы же не будем говорить о безопасности человеческого фактора, а речь идет и об этом. Получается вопрос с терминологией еще надо продумывать. Можно только приветствовать, что с появлением всех этих многочисленных информационных технологий появилась необходимость их как-то упорядочить, просто определить это надо немного по другому, не нравится сам термин кибербезопасность. Информация, в том виде, о котором мы говорим, как информационная безопасность это часть технологической системы. Как правило, все действия направлены на предотвращение внешнего вмешательства. Все законопроекты выпускаются правительством по той причине, о которой бояться говорить, это терроризм. Бояться, что кто-то не санкционировано влезет со злым умыслом и произойдет взрыв. Государство не стало бы обращать внимание на все остальное, если бы именно эта часть не была доминантой. Доминантой является борьба с противником, противник может войти и ударить, поэтому государство говорит, он может ударить сюда, пожалуйста, защитите. И речь идет о внешнем периметре, а не о внутреннем. Возможно, это мнение ошибочно, но чувствуется, что государство бы не стало вводить все это, если бы не та ситуация, в

которую мы попали в мире. Были высказаны опасения, что вместе с кибербезопасностью придут киберохранники, а вот грань между охраной и рэкетом всегда очень тонкая. Нужно понимать, что кибербезопасность это бизнес. Бизнес, которому дало старт государство.

Заслушав выступление, обсуждения и дискуссии секция «Автоматизированный учет электроэнергии и управление электропотреблением» НТС ЕЭС отметила:


- Глубину проработки вопроса докладчиком и объем знаний в озвученной теме. Изначально была масса вопросов, но по мере того, как шла презентация, они снимались.
- Есть понимание, что информационной безопасностью необходимо заниматься. Идет развитие технологии цифровых подстанций, в которых значимость кибербезопасности очень велика. Любой брак в информационном формате в цифровой технологии может привести к невероятным последствиям.
- Необходимо привлечь внимание отрасли к законопроектам и Постановлением Правительства в области информационной безопасности.
- От того, что решит рабочая группа №4 при ТК26 «Криптографические механизмы для М2М и промышленных систем» и что будет принято в рамках процедуры Росстандарта, впоследствии, зависят настройки того оборудования, которое будут использовать/ предлагать на рынке.

Секция «Автоматизированный учет электроэнергии и управление электропотреблением» НТС ЕЭС решила:

1. Представителям отрасли и производителям устройств АСУ ТП, которые работают и активно используют 104 протокол рекомендовать присоединиться к рабочей группе №4 при ТК26 «Криптографические механизмы для М2М и промышленных систем».
2. Разослать членам секции проект Постановления Правительства «Об утверждении показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, а также порядка и сроков осуществления их категорирования».

3. Рекомендовать членам секции выполнять мониторинг проектов Постановлений Правительства и других выпускаемых нормативных документов в области информационной безопасности.


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


В. В. Молодюк

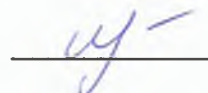
Ученый секретарь научно-
технической коллегии
НП «НТС ЕЭС», к.т.н.


Я.Ш. Исамухамедов

Председатель секции
«Автоматизированный учет
электроэнергии и управление
электропотреблением»,
НП «НТС ЕЭС», к.т.н.


А.В. Покатилов

Ученый секретарь секции
«Автоматизированный учет
электроэнергии и управление
электропотреблением»,
НП «НТС ЕЭС»


Е.Ю. Евенок

Список участников заседания секции «Автоматизированный учет электроэнергии и управление электропотреблением» НТС ЕЭС, состоявшегося 28 сентября 2017 года

1. Покатилов Александр Васильевич, ПАО «Мосэнерго», руководитель секции.
2. Евенок Екатерина Юрьевна, ПАО «Мосэнерго», ученый секретарь секции.
3. Бедин Владислав Анатольевич, член секции.
4. Быков Дмитрий Сергеевич, ПАО «Мосэнерго», член секции.
5. Гаврилов Владимир Вячеславович, ПАО «Мосэнерго», приглашенный.
6. Генгринович Евгений Леонидович, АО «Инфотекс», член секции.
7. Двужилов Андрей Александрович, ПАО «Мосэнерго», приглашенный.
8. Карамянц Илья Андреевич, ПАО «Мосэнерго», приглашенный.
9. Кишкурно Эдуард Антонович, Ассоциация «НП «Совет рынка», член секции.
10. Козленок Сергей Александрович, ПАО «Мосэнерго», приглашенный.
11. Муртазалиева Фариза Хабибовна, ПАО «Мосэнерго», член секции.
12. Осика Лев Константинович, Фонд «Энергия без границ», член секции
13. Панов Сергей Анатольевич, ПАО «Мосэнерго», приглашенный.
14. Ромашина Татьяна Васильевна, ПАО «Мосэнерго», член секции.
15. Тацин Антон Вячеславович, ООО «Ситиэнерго», член секции.
16. Чернецов Виктор Федорович, ФГУП «ВНИИМС», член секции.