ГОСУДАРСТВЕННАЯ ДУМА ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ СЕДЬМОГО СОЗЫВА

КОМИТЕТ ПО ЭКОНОМИЧЕСКОЙ ПОЛИТИКЕ, ПРОМЫШЛЕННОСТИ, ИННОВАЦИОННОМУ РАЗВИТИЮ И ПРЕДПРИНИМАТЕЛЬСТВУ

П Р О Т О К О Л

Расширенное заседание Экспертного совета по энергетическому машиностроению, электротехнической и кабельной промышленности при Комитете Государственной Думы по экономической политике, промышленности, инновационному развитию и предпринимательству и Комиссии по вопросам развития и внедрения технологий в области энергетической эффективности и энергосбережения Союза машиностроителей России

г. Москва

от 5 марта 2020 г.

Время проведения: 10:00 - 11:30

Место проведения: Георгиевский пер., д.2, каб. 15-44 а.

Повестка заседания:

«Энергетическая безопасность в соответствии с целями и задачами, указанными в Доктрине энергетической безопасности РФ»

Со вступительным словом к участникам заседания обратился Председатель Экспертного совета, член Комитета Государственной Думы по экономической политике, промышленности, инновационному развитию и предпринимательству **А.Н. Козловский:**

О Доктрине энергетической безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 13 мая 2019 г. № 216, как основополагающем документе стратегического планирования развития энергетических отраслей и обеспечивающих их работу отраслей промышленности в целях обеспечения национальной безопасности Российской Федерации.

О ситуации с необходимостью обеспечения энергетической безопасности, которую в полной мере можно реализовать только опираясь на отечественного надёжного производителя оборудования и комплектующих для обеспечения отрасли работой. Важность опоры на отечественного производителя особенно возросла в последнее время, когда технологии и цифровизация стали все шире проникать во все сферы экономики, а проект энергетической стратегии Российской Федерации, который сейчас широко обсуждается экспертным и профессиональным сообществом, подразумевает цифровую трансформацию и интеллектуализацию отраслей топливно-энергетического комплекса, в результате которой на качественно новый уровень поднимается оперативное управление в сфере энергетики.

Об опыте мировых компаний, которые конкурируют с отечественным производителем на российском рынке. О тендерах, где сегодня наблюдается настоящая экспансия дешевого китайского оборудования. О мощной поддержке китайских производителей своим правительством, что позволяет декларировать более низкие цены. О мерах поддержки, которые в Китае существуют для местных производителей, позволяющих им выходить на зарубежные рынки.

О том, что и Правительство, и производители России стремятся отстаивать рынки для отечественных производителей, но существуют ряд нормативных актов, требования которых затрудняют поддержку этих производителей, а в ряде случаев размывают это понятие *в пользу финишных сборочных производств зарубежных компаний, использующих зарубежную нелокализованную интеллектуальную собственность*.

О том, что модернизация производства и расширение производственной линейки выпускаемой продукции, которую проводят ведущие отечественные производители, дает результаты, но необходимо делать больше, если стоит задача обеспечить энергетическую безопасность страны в условиях любых глобальных непредвиденных кризисов подобных тем, с которыми мы сталкиваемся в настоящее время.

Рябин Т.В. (АО «НТЦ ФСК ЕЭС»):

О целях и задачах Комиссии, в том числе работе с правовыми и нормативными актами, разрешении вопросов внедрения энергоэффективных технологий, создании экспертизы в части технологий, проработке финансирования будущих проектов, подготовке кадров и работе с вузами.

О создании на базе Научного-технического центра «Россети - ФСК ЕЭС» производства элементов силовой электроники, которая на сегодняшний день практически не производится без участия иностранных производителей.

Фурашов А.В. («Национальный совет по энергетической безопасности и защите критической инфраструктуры»):

О «Национальном совете по энергетической безопасности и защите критической инфраструктуры», который создан с целью обеспечения цифрового суверенитета нашей страны в рамках Доктрины по энергетической безопасности Российской Федерации. В совет вошли ведущие специалисты отрасли: доктора наук, кандидаты технических наук, которые готовы поделиться своим опытом в этом вопросе.

Далее доклад на тему: "Угроза энергетической безопасности и критической инфраструктуры Российской Федерации":

О последствиях крупнейшей в энергетике аварии, которая произошла 24 мая 2005 года на подстанции "Чагино" (на тот момент принадлежала «Мосэнерго»), а именно пожаре на автотрансформаторе, в результате которого запустился процесс веерных отключений, были обесточены сотни электроподстанций, напряжением 35 кВ и выше, в том числе и кольцо 500 кВ, остановлено 12 электростанций, и возможности инициации аналогичной аварии целенаправленным внешним воздействием.

О единой энергосистеме Российской Федерации в составе: генерация электроэнергии 600 электростанций совокупной установленной мощностью 240 МВт, системообразующие подстанции - 330-750 кВ более 200, подстанций 220 кВ около 500, которые находятся в ведомстве различных компаний, в том числе ПАО «ФСК ЕЭС», генерирующих компаний оптового рынка электроэнергии для выдачи мощности – различных ОАО ОГК, Госкорпорации «Росатом», ПАО «РусГидро», а также являющихся крупными потребителями электроэнергии предприятий различных отраслей промышленности.

О важности аппаратуры вторичной коммутации, которая является интеллектуальной составляющей любого объекта критической инфраструктуры, потому что именно

автоматические и автоматизированные системы, средства АСУТП, релейная защита и противоаварийная автоматика, обеспечивают цифровой интеллект любого электроэнергетического объекта. Именно эти системы и устройства, а не административный и оперативный персонал сегодня реализуют управление энергообъектами. В то же время эти устройства и системы обеспечивая до 90% интеллекта энергообъекта составляют в его стоимости лишь около 10 %.

О явно спровоцированных извне ситуациях и «странности поведения» оборудования систем управления и контроля импортных производителей в различных условиях, по ситуациям:

1) Венесуэла, март 2019 года, ГЭС "Эль-Гури", обеспечивающая более 70% потребности страны в электроэнергии. Комплексная модернизация, которая проходила в 2005-2007 годах на этой ГЭС, проводилась одной из крупнейших транснациональных компаний. Если в феврале 2019 года начинаются протестные выступления против режима Президента Мадуро, то уже в марте 2019 года в стране происходит тройной блэкаут, вызванный в том числе аварией на вышеназванном объекте. При этом специалисты, которые смотрели более пристально на эту аварию, отметили, что это был самый долгосрочный блэкаут в истории мировой энергетики, и неполадки с оборудованием одного из ведущих мировых производителей.

2) Ливия, март 2011 года. 19 марта начинается военная операция с красивым названием "Рассвет Одиссея". Перед началом этой военной операции вся критическая инфраструктура была отключена от электричества и, этим, по сути, были выведены из строя системы ПВО. Причина – перебои в работе оборудования еще одной транснациональной компании.

3) Иран, 2010 год. Атомная стация в городе Бушер и центр по обогащению ураном оснащенные оборудованием компании "Сименс" были атакованы вирусом Stuxnet. В ходе технического анализа удалось выявить несанкционированные воздействия на алгоритмы по управлению частотно регулируемыми проводами. Данная ситуация была прокомментирована как «успешная совместная операция спецслужб Израиля и США». Позднее, через несколько месяцев это подтвердил и заместитель Министра обороны Израиля в одном из интервью ведущих изданий.

Отдельно отмечено, что отечественные производители за последние годы заняли значительную долю рынка в реализации соответствующих программ и оборудования, при этом большая часть электросетевого хозяйства страны была модернизирована именно в 2000-е годы – с 2000-го по 2012 год на основные транзитные линии, на подстанции 330-

750 кВ, а также на большинство подстанций, через которые осуществляется выдача мощности, например, на Калининской АЭС, Нововоронежской АЭС и других, было поставлено зарубежное оборудование. При этом системы релейной защиты и автоматики крупнейших энергосистем Европы, Америки, Китая и прочих выполнены преимущественно на решениях собственного производства.

Наумов В.А. (Заместитель председателя правления Национального совета по энергетической безопасности и защите критической инфраструктуры):

О понятиях информационной безопасности, информационном суверенитете и энергобезопасности. О том, что особенностью цифрового решения является необходимость регулярного доступа поставщиков оборудования или их представителей для сопровождения эксплуатации, обновления программного обеспечения и других процедур, все это создает совершенно особую уязвимость, и защита традиционными средствами информационной безопасности в настоящий момент представляется неэффективной.

О том, что в современном цифровом мире в условиях политической конкуренции, санкционного давления на первый план выдвигается проблема обеспечения независимости критической инфраструктуры страны от внешних воздействий. Поэтому такое понимание цифрового суверенитета включает в себя информационную физическую безопасность. При этом главным базовым компонентом является предотвращение возможности использования легально полученной информации для целенаправленных физических, кибернетических и иных форм воздействия на объект. Важно также предотвратить использование закладок, скрытых функциональных возможностей и других, основанных на близком доступе к объекту, действий, которые могут привести к получению контроля и инициации аварии с тяжелыми экологическими и социальными последствиями.

О транзите нефти, газа, где так же устанавливаются контролеры управления компрессорами, насосами, и практически везде в настоящий момент управляют всем цифровые решения.

О ситуации с базовыми документами кибербезопасности - Федеральными законами от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» и от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», определяющими требования направлений работы. К сожалению, эти документы, недостаточно учитывают особенности критической инфраструктуры. Так, например, под импортозамещением понимается оборудование,

изготовленное на территории РФ без уточнения требований по объему такой локализации, что является критичным для цифровых технических решений и особенно программного обеспечения. Помимо этого, неясным остается механизм реализации требований по ограничению доступа к информации об объектах критической инфраструктуры при внедрении на них оборудования и ПО зарубежной разработки и производства.

Предложено для обеспечения цифрового суверенитета критической инфраструктуры уточнить понятия импортозамещения, конкретизировать объем информации, доступ к которой ограничивается и ограничить применение продукции и ПО зарубежного происхождения на объектах критической инфраструктуры только случаями полного отсутствия отечественных аналогов, подтвержденного независимой уполномоченной структурой.

О необходимости внимания к организации процесса закупок оборудования и программного обеспечения для объектов критической инфраструктуры. В настоящий момент компании, осуществляющие эксплуатацию таких объектов – компании с государственных участием, которые в работе руководствуются Федеральным законом от 18.11.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц», на основании которого разрабатывается внутреннее положение о закупках. При этом, при оценке и сопоставлении заявок российские лица согласно Постановлению Правительства РФ от 16.09.2016 №925 «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами» и Приказу Министерства Финансов РФ от 04.06.2018 №126н «Об условиях допуска товаров, происходящих из иностранного государства или группы иностранных государств, для целей осуществления закупок товаров для обеспечения государственных и муниципальных нужд» имеют стоимостной приоритет в 15 %. Однако, совершенно очевидно, что иностранный производитель, желающий установить на достаточно важный для него объект критической инфраструктуры свое цифровое оборудование и системы управления, легко пойдет на демпинг в 15 %. При этом предметом поставки могут стать существенные для энергобезопасности объекты, как, например, энергокольцо вокруг Москвы, в настоящий момент уже выполненное на базе иностранного оборудования. Госкомпании являются заложниками отсутствия других инструментов поддержки отечественных производителей. Для обеспечения цифрового суверенитета, необходимо принятие специальных решений, исключающих такой политический мотивируемый демпинг. Например, в виде

применения на критических объектах продукции программного обеспечения зарубежного происхождения только в случаях полного отсутствия российских аналогов.

О сложностях в регулировании информационной безопасности силами ФСТЭК и Приказах ФСТЭК от 14.03.2014 № 31 «Об утверждении «Требований к обеспечению защиты информации в АСУ ТП», от 25.12.2017 № 235 «Об утверждении «Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры РФ и обеспечению их функционирования», от 25.12.2017 N 239 «Об утверждении «Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ», сертификации ФСТЭК, включающей в себя составление заданий на безопасность, обязательные требования на прохождение испытаний, анализе исходного кода и прочему. Полноценный цикл такой сертификации трудоемкий, длительный, дорогостоящий, привязан к конкретной версии программного обеспечения, что существенно ограничивает технологический прогресс и приводит к отставанию наших решений от зарубежных. При этом не достигается, например, защита от закладок в программном обеспечении. Указанные документы и требования не способствуют выработке инструментов и преград от нарушения энергетической безопасности.

О том, что ранее предполагалось при внесении изменений в приказ ФСТЭК от 25.12.2017 № 239 «Об утверждении «Требований по обеспечению безопасности значимых объектов КИИ РФ» в соответствующих разделах будет внесено указание об ограничениях для работников зарубежных организаций, а также организаций, находящихся под прямым или косвенным контролем иностранных физических и (или) юридических лиц, однако в ходе общественных обсуждений это указание из текста проекта изменений к приказу было исключено.

О том, что согласно Постановлению Правительства РФ №719 от 17.07.2015 «О критериях отнесения промышленной продукции к промышленной продукции, не имеющей аналогов, произведенных в Российской Федерации», Приказу Министерства промышленности и торговли РФ №3788 от 24.09.2018 «Об утверждении Порядка определения степени локализации в отношении генерирующего объекта, функционирующего на основе использования возобновляемых источников энергии» и утвержденным Постановлением Правительства РФ от 03.06.2008 №426 «Правилам квалификации генерирующего объекта, функционирующего на основе использования возобновляемых источников энергии», методики определения того, имеет ли продукция отечественное происхождение, описывают показатели, основанные на расчёте баллов,

которые согласно этой методике учитывают данные о производителях и месте осуществления отдельных технологический операций по изготовлению. При этом не учитываются особенности цифровых устройств, в которых основная функциональность определяется не конструкцией, а интеллектуальной составляющей, алгоритмами и программным кодом. Помимо этого, методика не охватывает полный жизненный цикл оборудования для объектов критической инфраструктуры, например, сопровождение проектирования и пусконаладочные работы. По сути, эти методики сейчас определяют то, что любой иностранный производитель может поставить в РФ блоки комплектующих, на территории РФ осуществить из них финишную сборку изделия, выполнить необходимые заводские проверки и это уже будет считаться отечественным продуктом, что в части цифровых устройств очень далеко от истины. Когда не контролируются алгоритмы, которые заложены в блоках контроллеров, не контролируется само программное обеспечение говорить о независимости от этих решений бессмысленно, особенно на объектах критической инфраструктуры. Поэтому для обеспечения цифрового суверенитета, необходимо требовать локализацию критических для информационной и энергетической безопасности технологий на всём жизненном цикле этой продукции.

О совместном Приказе Министерства промышленности и торговли и Министерства экономики и развития РФ №1032/397 от 17.08.2011 «Об утверждении параметров, в соответствии со значениями которых телекоммуникационному оборудованию, произведенному на территории Российской Федерации, может быть присвоен статус телекоммуникационного оборудования российского происхождения, методики определения значений параметров, в соответствии с которыми телекоммуникационному оборудованию, произведенному на территории Российской Федерации, может быть присвоен статус телекоммуникационного оборудования российского происхождения, порядка присвоения телекоммуникационному оборудованию, произведенному на территории Российской Федерации, статуса телекоммуникационного оборудования российского происхождения и ежегодного подтверждения такого статуса» и том, что в энергетическом секторе существует единственная методика определения страны происхождения вторичных систем и их элементов - «Методика определения страны происхождения вторичных систем и их элементов ПАО «ФСК ЕЭС». К сожалению, указанная бальная система не учитывает весь жизненный цикл оборудования для объектов критической инфраструктуры, а также тот факт, что на сегодняшний день в Российской Федерации отсутствуют либо не имеют необходимых характеристик целый ряд комплектующих изделий, например, микропроцессоры, необходимые для встраиваемых

решений, и ряд других компонентов, и такие изделия приходится закупать у зарубежных производителей.

Лунин К.А. (Заместитель начальника Департамента инновационного развития ПАО "ФСК ЕЭС"):

О поддержке компанией «Россети ФСК ЕЭС» (ПАО «ФСК ЕЭС») государственной политики направленной на импортозамещенияцелях и задачах корпоративного импортозамещения, которые направлены на обеспечение технологической безопасности электросетевого комплекса Российской Федерации и снижение зависимости от иностранной продукции, оборудования, технических устройств, а также услуг и работ иностранных компаний и использование иностранного и программного обеспечения.

О том, что в настоящее время при реализации целевых показателей в закупках 2019 года отечественного основного оборудования ПАО «ФСК ЕЭС» было закуплено 75 % от общего объема закупок. За последние 3 года отечественного оборудования компанией было закуплено больше, чем на 30 миллиардов рублей.

Сказано об оборудовании и комплектующих, которые в настоящее время заместить не представляется возможным по тем или иным причинам, в том числе силовом кабеле сверхвысокого напряжения и комплектующих для микропроцессорной техники и прочих позициях, которые в России не производится.

Подчеркнуто отсутствие в законодательстве четкого определения понятий "отечественный производитель" и "отечественная продукция", что затрудняет реализацию адресных проектов по поддержке развития импортозамещающих производств. При этом приведен пример опыта ПАО «ФСК ЕЭС», в котором в этом направлении существует собственная методика, которая, к сожалению, носит декларативный характер. В настоящее время в большинстве случаев понятие "отечественный производитель" определяется на основе критерия страны происхождения продукции, установленного в статье 58 Таможенного кодекса Таможенного союза, как страна, в которой товары были полностью произведены или подвергнуты достаточной переработке в соответствии с критериями, установленными Таможенным законодательством Таможенного союза. Учитывая отсутствие единой методики определения достаточности переработки и обработки, такое определение не дает возможности однозначного отнесения производителей к отечественным.

Сказано, что для обеспечения методологического единства оценки страны происхождения продукции возможно применять количественный показатель уровня

локализации производства процессов на территории Российской Федерации, представляющий собой долю использования при производстве продукции, изделий и услуг российских предприятий в стоимостном выражении.

Стебенев Н.А. (ПАО «ФСК ЕЭС»):

О проблемах, с которыми столкнулось ПАО «ФСК ЕЭС», изучая вопросы обеспечения информационной безопасности технологической инфраструктуры, в том числе при выполнении требований Федерального закона "О безопасности критической информационной инфраструктуры РФ":

1) Кибербезопасность — это не только работа программных и аппаратных средств информационной безопасности, но и подготовка квалифицированных специалистов, взаимодействие специалистов в области информационной безопасности с подразделениями эксплуатации и разработчиками технологических систем. Поэтому выработка инструментов для противодействия несанкционированным воздействиям на энергосистему должна вестись с непосредственными производителями и разработчиками технологических систем, в т.ч. АСУ ТП. С учетом заданного государством курса на импортозамещение оборудования и программного обеспечения, разработка встроенных средств кибербезопасности в технологических системах требует существенных вложений в научные исследования и производство, при этом - обеспечить конкурентное преимущество перед иностранными производителями является непростой задачей. Для решения этих задач необходимо совместное участие всех заинтересованных сторон – производителей и потребителей технологических систем, а также непосредственное участие государства.

2) Стремительный рост цифровизации опережает развитие нормативных актов, в том числе требований по обеспечению кибербезопасности технологических систем, а существующие процедуры сертификации оборудования для защиты информации несовершенны. Программные и программно-аппаратные комплексы усовершенствуются, меняют версии быстрее, чем производитель получает на них сертификаты соответствия требованиям информационной безопасности, из-за чего в целях обеспечениях кибербезопасности применяются не последние разработки и технологии, а разработанные несколькими годами ранее и прошедшие процедуру сертификации, тогда как злоумышленник всегда применяет наиболее актуальные инструменты и уязвимости.

3) Существуют сложности контроля и подтверждения эффективности применяемых систем кибербезопасности. Так, в идеале любая система, любое оборудование для подтверждения работоспособности требуют проверки реальными

пиковыми нагрузками, но вместе с тем, наиболее опасными инструментами злоумышленника остается использование «уязвимости нулевого дня». Всегда существуют риски, что нагрузочное тестирование и используемые методики, имитирующие атаку злоумышленника на технологическую систему, будут далеки от реальных действий злоумышленника.

В связи с озвученным отмечено, что оценить эффективность мер по обеспечению кибербезопасности возможно при проработке всех этапов и участников процесса, в том числе федеральных органов исполнительной власти, с существенной базой данных, производителей АСУ ТП, производителей систем безопасности и непосредственно эксплуатации технологических систем.

Базылев Е.А. (Директор Ялтинского международного экономического форума):

О том, что в процессе подготовки планируемого Ялтинского международного экономического форума запланировано обсуждение на тему «Цифровой суверенитет в российской энергетике».

Ковалев В.Д. (Президент Ассоциации производителей высоковольтного электротехнического оборудования «ТРАВЭК»):

О том, что на фоне обсуждений цифровизации и кибербезопасности не стоит забывать, что до 70 % электротехнического и энергетического оборудования, которое работает в России, выработало свой ресурс. Об Отсутствии программ направленных на диагностику аппаратов проработавших свыше запланированных производителем сроков, что очень важно для российских электротехнических заводов для возможности подготовки к подобным программам заблаговременно.

Об отсутствии единого центра аттестации оборудования, что сегодня является тормозом в развитии научно-технического прогресса и внедрении инновационных технологий. Сегодня ПАО «Россети» имеют свою аттестацию, ГК «Росэнергоатом» свою, ПАО "Транснефть" свою аттестацию и прочие. В результате все производители должны проходить по одному и тому же виду оборудования в каждой отрасли отдельные аттестации с соотвествующими оплатами в миллионы рублей. Причем, любая аттестация выдается производителю на ограниченный срок с необходимостью в дальнейшем этот процесс запускать по новой. Таким образом процесс аттестации не способствует улучшению качества оборудования, а является дополнительной нагрузкой для специалистов предприятий, а в некоторых ситуациях требуют привлечения дополнительных работников с соответствующими дополнительными затратами. Вместо того чтобы заниматься разработками инновационных видов оборудования, профильные

сотрудники предприятий занимаются корректировкой под различные требования многочисленных протоколов испытаний, проводят дополнительные дорогостоящие исследования и часто процесс затягивается на годы. Есть примеры, когда до трех и более лет идет аттестация оборудования.

О вопросах по энергосбережению. Об эффекте внедрения частотно-регулируемых приводов, с сожалением о том, что по России эти позиции не находят широкого применения.

О современных аморфных трансформаторах с существенной экономией энергозатрат, но при этом большей стоимости аппарата, что так же не способствует применению на территории России этого вида инновации в энергоэффективности.

О кибербезопасности и необходимости обеспечить надёжное функционирование энергетических систем за счет создания дополнительной дублирующей системы управления.

Будигин А.Т. (ФГБУ «РЭА» Минэнерго России):

Об ужасном состоянии электрохозяйств, на примере ТЭЦ в малых городах. О необходимости принятия технического регламента безопасности электростанций и сетей, который остановился в Государственной Думе после второго чтения более 10 лет назад.

О необходимости привлечения к разработке технических решений по кибербезопасности ГК «Ростехнологии», ресурсы которой могут посодействовать в разрешении перечисленных сложностей.

Портасова Н. (Компания "Элара" Республика Чувашия):

О сложностях в реализации программы "ДПМ-штрих" (субсидии на модернизацию генерирующих объектов) согласно которой субсидирование не распространяется ни на позиции силового энергетического оборудования, ни на системы автоматизации, хотя, согласно данным о тепловых станциях, автоматизировано менее 50 % электрохозяйств станций.

О том, что в генерирующих компаниях 70 % которых являются собственники в лице импортных компаний либо частных собственников никакие нормативные акты, направленные на импортозамещение, не имеют значения. О примерах конкурсных процедур 2020 года, которые показывают, что иностранные компании производители как присутствовали по системам автоматизации в этих проектах, так они будут и дальше присутствовать, причём без какой-либо оценки уровня локализации.

О важности внесения изменении в Федеральный закон "О безопасности критической информационной инфраструктуры".

О необходимости привлечения исключительно российского программного обеспечения.

О необходимости дополнения приложений Постановления Правительства № 719 в части систем автоматизации с требованиями к именно российскому программному обеспечению, которое включено в постановление № 2036, по линии Министерства информационной политики и связи.

Кваша Е.М. (Директор Национального центра энергоэффективности):

О государственном докладе, в котором отражены все цифры по состоянию с энергоэффективностью на текущий момент в РФ и предложении о совместной проработки вопросов производителей оборудования.

По итогам заседания решили:

1) Принять к сведению предложения Национального совета по энергетической безопасности и защите критической инфраструктуры в части необходимости совершенствования нормативно-правовой базы по вопросам обеспечения безопасного, надежного и устойчивого функционирования инфраструктуры и объектов энергетики.

2) Принять к сведению риск ориентации организаций ТЭК на импорт технологий вместо развития отечественного научно-технологического потенциала. Отметить важность при создании и внедрении новых современных технических и технологических решений, выполнять разработки преимущественно на базе НИОКР российских компаний. При этом в случае необходимости пилотирования технологий, отсутствующих у российских компаний, привлекать на пилотных проектах зарубежных технологий специалистов отечественных компаний для освоения этих технологий в Российской Федерации.

3) Участниками заседания совместно с уполномоченными представителями компаний, входящих в Экспертный совет по Энергетическому машиностроению, электротехнической и кабельной промышленности направить позицию компаний с предложениями по реализации ограничений допуска импортных производителей программного обеспечения и оборудования систем автоматизации, релейной защиты и автоматики, а так же прочих устройств, влияющих на кибербезопасность инфраструктуры компаний. Предложено к обсуждению:

-необходимость внесения корректировок Федеральных законов от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» и от 26.07.2017 №

187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в части введения в них положений, отражающих:

- определение импортозамещения, как использования продукции и программного обеспечения только российского происхождения, а для локализованного – только при условии локализации стадий жизненного цикла от разработки и производства из исходных материалов и комплектующих до утилизации,

- конкретизацию в виде утвержденного исчерпывающего перечня объема информации, доступ к которой ограничивается для любых операций, связанных с возможностью предоставления ее зарубежным партнерам,

- ограничение применения продукции и программного обеспечения зарубежного происхождения только случаями отсутствия отечественных аналогов;

- необходимость внесения корректировок в Постановление Правительства РФ №719 от 17.07.2015 «О критериях отнесения промышленной продукции к промышленной продукции, не имеющей аналогов, произведенных в Российской Федерации», Приказ Министерства промышленности и торговли РФ №3788 от 24.09.2018 «Об утверждении Порядка определения степени локализации в отношении генерирующего объекта, функционирующего на основе использования возобновляемых источников энергии» утвержденные Постановлением Правительства РФ от 03.06.2008 №426 «Правила квалификации генерирующего объекта, функционирующего на основе использования возобновляемых источников энергии», исключающих возможность поставок продукции иностранного производства через локализацию некритических для энергетической безопасности технологий на всем жизненном цикле этой продукции;

- необходимость внесения корректировок в Приказы ФСТЭК от 14.03.2014 № 31 «Об утверждении «Требований к обеспечению защиты информации в АСУ ТП», от 25.12.2017 № 235 «Об утверждении «Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры РФ и обеспечению их функционирования», от 25.12.2017 N 239 «Об утверждении «Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ» положений, водящих ограничения на осуществление поставок оборудования на объекты критической инфраструктуры и выполнения работ на этих объектах для работников зарубежных организаций, а также организациях, находящихся под прямым или косвенным контролем иностранных физических и (или) юридических лиц, а в случае недостижимости в настоящее время реализации таких ограничений - введение соответствующего целевого

требования с отложенным сроком введения или при условии наличия российских решений, отвечающих всем необходимым требованиям;

- необходимость имплементации в Постановление Правительства РФ от 16.09.2016 №925 «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами» методики определения страны происхождения товара и уровня локализации производства оборудования и материалов на территории России принятой в Постановлении Правительства от 17.07.2015 №719;

- необходимость внесения поправок в Постановление Правительства РФ от 16.09.2016 №925 с выделением групп товаров (в том числе используемых в отрасли электроэнергетики) имеющих отношение к безопасности государства и населения;

- необходимость внесения корректировок в приказе Министерства промышленности и торговли и Министерства экономики и развития РФ №1032/397 от 17.08.2011 «Об утверждении параметров, в соответствии со значениями которых телекоммуникационному оборудованию, произведенному на территории Российской Федерации, может быть присвоен статус телекоммуникационного оборудования российского происхождения, методики определения значений параметров, в соответствии с которыми телекоммуникационному оборудованию, произведенному на территории Российской Федерации, может быть присвоен статус телекоммуникационного оборудования российского происхождения, порядка присвоения телекоммуникационному оборудованию, произведенному на территории Российской Федерации, статуса телекоммуникационного оборудования российского происхождения и ежегодного подтверждения такого статуса», учитывающие технологии всего жизненного цикла продукции, включая ввод и сопровождение эксплуатации на объекте, особенности производства цифровых устройств управления, а также рекомендовать государственным компаниям и компаниям с государственным участием ввести соответствующие положения в их положения о закупках и методики оценки степени локализации применяемой ими продукции;

-необходимость внесения корректировок в Государственную программу "ДПМ-штрих" (субсидии на модернизацию генерирующих объектов) Министерства Энергетики РФ в части дополнений в перечень оборудования, подлежащего субсидированию с соответствующими требованиями к локализации на территории РФ позиций силового энергетического оборудования, АСУ ТП и РЗ и А;

-необходимость внесения соответствующих корректировок в Технический регламент о безопасности электрических и тепловых сетей и электрических станций (в том числе с комбинированной выработкой электрической и тепловой энергии), котельных, энергопринимающих устройств и теплопринимающих установок в части устройств АСУ ТП и РЗ и А.

Председатель Экспертного совета
по энергетическому машиностроению,
электротехнической и кабельной промышленности,
член Комитета Государственной Думы
по экономической политике, промышленности,
инновационному развитию и предпринимательству А.Н. Козловский