Рекомендации «круглого стола» Комитета Государственной Думы по энергетике от 27.01.2017 № 3.25-5/14 на тему: «Перспективы развития вопросов информационной безопасности топливно-энергетического комплекса и законодательные аспекты обеспечения безопасности информационных систем объектов топливно-энергетического комплекса»

15 декабря 2016 года, зал 706, Охотный ряд, д. 1

Энергетическая отрасль является стратегической для экономики, обороноспособности и всей инфраструктуры Российской Федерации.

Начиная с 2015 года Государственной Думы, на фоне усиления санкционного давления, активизации террористической деятельности по всему миру, характеризующейся высокотехнологичной подготовкой, Комитет Государственной Думы по энергетике в своей работе выделил отдельным блоком направление законодательного обеспечения безопасности топливно-энергетического комплекса.

В период с 2015 года по настоящий момент при активном участии Комитета был принят ряд Федеральных законов, направленных на решение ключевых вопросов законодательного обеспечения безопасности объектов топливно-энергетического комплекса:
- на полицию были возложены обязанности по осуществлению контроля за обеспечением безопасности объектов топливно-энергетического комплекса;
- Правительству Российской Федерации (уполномоченным федеральным органам исполнительной власти) предоставлены полномочия по установлению обязательных требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики;
- поддержан «блок поправок» Правительства Российской Федерации по реализации задачи, поставленной Президентом Российской Федерации В.В.Путиным по внедрению риск-ориентированного надзора в области безопасности гидротехнических сооружений, по аналогии с механизмами, что были апробированы в области промышленной безопасности опасных производственных объектов.

Отдельным направлением законодательного обеспечения объектов топливно-энергетического комплекса с 2015 года стало сотрудничество Комитета с Национальным антитеррористическим Комитетом, Советом Безопасности Российской Федерации, Секретариатами Межпарламентской Ассамблеи государств-участников СНГ и Парламентской Ассамблеи ОДКБ.

В тоже время Комитетом отдельно отмечается, что на фоне напряженной геополитической обстановки возникла настоятельная необходимость в усилении мер информационной безопасности объектов топливно-энергетического комплекса России.

Данная тема впервые обсуждается на площадке Комитета Государственной Думы по энергетике в целях законодательного обеспечения противодействия новым вызовам и угрозам безопасности топливно-энергетического комплекса России в рамках специализированного «круглого стола» с рассмотрением вопросов:
- перспективного развития информационной безопасности топливно-энергетического комплекса;
- дистанционного и удаленного мониторинга параметров предприятий топливно-энергетического комплекса;
- Государственной информационной системы ТЭКа;
-«информационных стратегий»;
- импортозамещения;
- «кибербезопасности» объектов топливно-энергетического комплекса;
- законодательного обеспечения безопасности информационных систем объектов топливно-энергетического комплекса.

Участники «круглого стола» отмечают, что затронутые вопросы имеют исключительно важное значение для формирования новой политики в сфере обеспечения информационной безопасности объектов топливно-энергетического комплекса.

Объекты топливно-энергетического комплекса являются неотъемлемой частью жизнедеятельности Российской Федерации, многие из них являются критически важными объектами. В последнее время объекты топливно-энергетического комплекса по всему миру становятся мишенью для дестабилизации ситуации, а также объектами для совершения диверсий, промышленного шпионажа и террористических актов; наблюдается устойчивый рост количества инцидентов по нарушению информационной безопасности, при этом увеличивается как сложность и комплексность угроз, так и их интенсивность.

Важной тенденцией является изменение ландшафта в мире по структуре и характеру поведения источников угроз. Наблюдается устойчивое усложнение иерархии групп нарушителей, повышение их технической оснащенности и уровня маскировки. Типовые нарушители в киберпространстве видоизменяются от отдельных элементов, мотивированных получением славы с хулиганскими побуждениями, до профессиональных киберподразделений, обладающих внушительными ресурсами, в том числе предоставляемыми государствами. Данные преступные группы как правило ставят своей целью дестабилизацию обстановки потенциального противника, информационную борьбу, вывод из строя объектов инфраструктуры, нарушение работоспособности целых секторов экономики и нарушение работы коммуникаций и связи.

При реализации задач обеспечения информационной безопасности объектов критичной инфраструктуры, необходимо учитывать отсутствие повсеместного глубокого понимания проблематики информационной безопасности, полноценного видения угроз информационной безопасности, отсутствие публикаций большей части инцидентов и в силу этого недооценку данных угроз на местах.

При этом отдельно нужно отметить стратегическую важность реализации Доктрины информационной безопасности, определённой в Указе Президента Российской Федерации от 5 декабря 2016 года «Об утверждении Доктрины информационной безопасности Российской Федерации».

В рамках данного Указа Президента Российской Федерации регламентируются важнейшие положения национальных интересов, угроз информационной безопасности, а также сил и средств информационной безопасности, определяющих систему обеспечения информационной безопасности. В рамках пункта 22 Доктрины защита объектов критической информационной инфраструктуры определяется как одна из стратегических целей.

Таким образом, объекты топливно-энергетического комплекса Российской Федерации из числа критической информационной инфраструктуры напрямую попадают под действие национальной Доктрины информационной безопасности.

Осуществляемый в настоящее время в Российской Федерации переход к информационному обществу приводит к тому, что подавляющее большинство систем принятия решений и бизнес-процессов в ключевых отраслях экономики и сфере государственного управления реализуются или планируются к реализации с использованием информационных технологий. В различных информационных системах уже сейчас хранятся и обрабатываются значительные объемы информации, в том числе касающейся вопросов государственной политики и обороны, финансовой и научно-технической сферы, частной жизни граждан.

Одновременно информационные технологии повсеместно внедряются при построении автоматизированных систем управления производственными и технологическими процессами, используемых в топливно-энергетическом, финансовом, транспортном и других секторах критической инфраструктуры Российской Федерации.

Глобализация современных информационно-коммуникационных сетей и информационных систем, вынужденное применение при их построении иностранного оборудования и заимствованного программного обеспечения, имеющего уязвимости, а также существенное увеличение количества автоматизированных систем управления производственными и технологическими процессами в сочетании с интенсивным совершенствованием средств и методов применения информационных и коммуникационных технологий в противоправных целях формируют новые угрозы безопасности Российской Федерации.

Компьютерная атака на критическую информационную инфраструктуру может привести к катастрофическим последствиям, а учитывая, что она является связующим звеном между другими секторами национальной инфраструктуры, неизбежно повлечет ущерб и этих секторов. Переход информационных и коммуникационных технологий на систему цифровых сигналов упростило и частично автоматизировало управление процессами, но в то же время сделало их более уязвимыми перед потенциальными компьютерными атаками. Вредоносная программа, направленная на внесение изменений в бинарный код программы (алгоритм программы, записанный в двоичной системе исчисления), способна вывести из строя любое оборудование, работающее с использованием бинарного кода. При этом равную опасность могут представлять атаки, совершаемые в преступных, террористических и разведывательных целях со стороны отдельных лиц, сообществ, иностранных специальных служб и организаций.

По экспертным оценкам за последние годы, ущерб от вредоносных программ составлял от трехсот миллиардов до одного триллиона долларов, то есть от 0,4% до 1,4% общемирового ежегодного ВВП, и эти показатели имеют тенденцию к неуклонному росту.

При развитии событий по наихудшему сценарию компьютерная атака способна полностью парализовать критическую информационную инфраструктуру государства и вызвать социальную, финансовую и (или) экологическую катастрофу.

Характерными примерами последствий негативного воздействия компьютерных атак на критическую инфраструктуру государства могут послужить остановка центрифуг иранской атомной станции с помощью компьютерного вируса StuxNet в сентябре 2010 г., прекращение работы доменной печи на сталелитейном заводе в Германии в ноябре 2015 г., серийные возгорания на объектах нефтегазовой инфраструктуры Ирана вследствие срабатывания программных закладок в августе-сентябре 2016 г. и многие другие.

Таким образом, стабильность социально-экономического развития Российской Федерации и ее безопасность, по сути, поставлены в прямую зависимость от надежности и безопасности функционирования информационно-телекоммуникационных сетей и информационных систем.

В настоящее время эффективное правовое регулирование в данной сфере затруднено из-за отсутствия системообразующих законодательных актов, устанавливающих порядок отношений в сфере обеспечения безопасности критической информационной инфраструктуры в Российской Федерации.

Участниками «круглого стола» отмечается, что проектом федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации», внесенным в Государственную Думу 6 декабря 2016 года Правительством Российской Федерации, устанавливаются основные принципы обеспечения безопасности критической информационной инфраструктуры, полномочия государственных органов Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами критической информационной инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов.

В соответствии с положениями данного законопроекта безопасность критической информационной инфраструктуры Российской Федерации и ее объектов обеспечивается за счет:
- определения отраслей экономики и областей государственного управления, автоматизация управления и принятия решений в которых достигла такого уровня, при котором успешное осуществление компьютерных атак на информационные ресурсы данных отраслей и областей может привести к ущербу безопасности Российской Федерации;

- определения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
- разработки критериев категорирования объектов критической информационной инфраструктуры, показателей этих критериев и порядка категорирования объектов критической информационной инфраструктуры;
- категорирования объектов критической информационной инфраструктуры в соответствии с указанными критериями, показателями и порядком;
- ведения реестра значимых объектов критической информационной инфраструктуры;
- установления требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры с учетом их категорий;
- создания систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечение их функционирования;
- обеспечения взаимодействия этих систем с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, созданной в соответствии с Указом Президента Российской Федерации от 15 января 2013 г. № 31с;
- осуществления оценки состояния защищенности критической информационной инфраструктуры Российской Федерации;
- осуществления государственного контроля в области безопасности критической информационной инфраструктуры Российской Федерации.

Реализация мероприятий по указанным направлениям сосредоточена на обеспечении комплексности и непрерывности обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Результаты анализа опыта правового регулирования безопасности критической информационной инфраструктуры стран с развитой информационной инфраструктурой, таких как Германия, США, Великобритания, Япония и Южная Корея, а также международных правовых актов в данной области, показывают, что обеспечение безопасности критической информационной инфраструктуры исключительно силами и средствами государства невозможно. Существенная часть объектов критической информационной инфраструктуры в вышеупомянутых странах, как и в Российской Федерации, не находится в собственности государства. Исходя из этого, рассматриваемым законопроектом предусматриваются дополнительные обременения, налагаемые на лиц, владеющих значимыми объектами критической информационной инфраструктуры на праве собственности или ином законном основании, касающиеся категорирования, создания и обеспечения функционирования систем безопасности этих объектов, а также обеспечения их взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Глобализация современных информационно-коммуникационных сетей и информационных систем, вынужденное применение при их построении иностранного оборудования и заимствованного программного обеспечения, имеющего уязвимости, а также существенное увеличение количества автоматизированных систем управления производственными и технологическими процессами в сочетании с ускоренным совершенствованием средств и методов применения информационных и коммуникационных технологий в противоправных целях формируют новые угрозы безопасности для критических информационных систем объектов ТЭКа.

Постоянно расширяющиеся возможности использования информационно-телекоммуникационных сетей на объектах ТЭКа, обусловленные их постоянным совершенствованием, вызывают повышенный интерес к ним со стороны организованной преступности, экстремистских и террористических организаций, иностранных спецслужб. Существующие особенности построения современного информационного пространства (в том числе в информационно-телекоммуникационной сети «Интернет») позволяют обеспечивать анонимность действий и существенно осложняют идентификацию и авторизацию пользователей.

В настоящее время только в электроэнергетике в технологических процессах производства и передачи электроэнергии и тепла повсеместно применяются автоматизированные системы управления. Сложность данных технологических процессов обуславливает усложнение систем и алгоритмов управления объектами – участниками технологических процессов, что повышает уязвимость объектов электроэнергетики (угрозы удаленного управления объектами, нарушение целостности информации, на основе которой принимаются управленческие решения). От корректной работы и алгоритмов АСУ ТП и её составляющих компонентов непосредственно зависит надёжность и безопасность объектов, участвующих в едином технологическом процессе.

Так, к техногенным угрозам энергетической безопасности относится повышение уязвимости объектов ТЭК, связанное с усложнением систем и алгоритмов управления этими объектами. Кроме того, в числе угроз безопасности ТЭК Российской Федерации все еще остаются риски эмбарго (блокирования поставок продукции или предоставления услуг) и отзыва лицензии, так как в основном авторизированные системы управления поставляются иностранными производителями.

В этой связи участники «круглого стола» отмечают важным и своевременным необходимость принятия проекта федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации», внесенного Правительством Российской Федерации в Государственную Думу, для топливно-энергетического комплекса Российской Федерации. В настоящее время требования к средствам защиты информации и информационной безопасности объектов электроэнергетики в целом устанавливаются государственными стандартами и приказами федеральных органов исполнительной власти (в том числе ФСБ России, ФСТЭК России). Вместе с тем, требования к информационной безопасности, устанавливаемые государственными стандартами Российской Федерации, не имеют нормативного, обязывающего характера, модель угроз информационной безопасности автоматизированных систем управления на объектах электроэнергетики отсутствует.

Подпунктом 4 пункта 3 статьи 7 законопроекта установлена обязанность обеспечения беспрепятственного доступа субъектом критической информационной инфраструктуры (при признании объекта электроэнергетики значимым объектом критической информационной инфраструктуры) должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры. Комитет обращает внимание, что техника безопасности при работе с электрооборудованием предусматривает приобретение компетенции в вопросах электробезопасности,

которая закрепляется присвоением персоналу соответствующей группы допуска для обслуживания электроустановок. Для определенной группы устанавливается предельное напряжение и другие параметры доступа к электроустановкам. Персоналу, не имеющему соответствующей группы допуска по электробезопасности, категорически запрещен доступ к электроустановкам. Учитывая особый статус и потенциальную опасность отдельных объектов энергетики, представляется целесообразным дополнительно обсудить данный вопрос.

Согласно подпункту 4 пункта 2 статьи 8 законопроекта система безопасности значимого объекта критической информационной инфраструктуры должна обеспечивать восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемое, в том числе за счет создания и хранения резервных копий необходимой для этого информации. Комитет отмечает, что применительно к объектам ТЭКа в ряде случаев может потребоваться не только наличие резервных копий информации, но и резервного оборудования. Положениями указанной статьи подразумевается создание и последующая эксплуатация системы информационной безопасности. Задачи обеспечения безопасности критической информационной инфраструктуры ТЭК в большей степени относятся к инженерно-техническим, а не к организационно-методологическим проблемам. Если объект критической информационной инфраструктуры эксплуатируется через полностью автоматизированную технологию с применением удаленного телеуправления, то представляется сложным обосновать целесообразность затрат на проведение документарных проверок. В этой связи представляется целесообразным предусмотреть проведение инструментального аудита.

Участники «круглого стола» отмечают, что учитывая важность обеспечения безопасности критической информационной инфраструктуры топливно-энергетического комплекса для страны, статью 14 законопроекта необходимо дополнить пунктом 2, согласно которому субъекты критической информационной инфраструктуры несут ответственность в соответствии с законодательством Российской Федерации в области безопасности критической информационной инфраструктуры Российской Федерации.

Принимая во внимание стратегическое значение энергетической отрасли для экономики, обороноспособности, энергообеспечения и безопасности Российской Федерации, участники «круглого стола» предлагают дополнительно рассмотреть возможность регламентации особого статуса объектов ТЭК, внеся ко второму чтению проекта федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации» корреспондирующие ему изменения в Федеральный закон от 21.07.2011 г. № 256-ФЗ «О безопасности топливно-энергетического комплекса России», тем более что Лабораторией Касперского было внесено предложение рассмотреть изменения в Паспорт безопасности объекта топливно-энергетического комплекса, в связи с внесением правительственного законопроекта № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации», учитывая, что категорирование объектов топливно-энергетического комплекса было завершено в 2015 году.

Участники «круглого стола» отмечают, что принятие законопроекта позволит создать правовую и организационную основу для эффективного функционирования системы безопасности критической информационной инфраструктуры Российской Федерации, направленной в первую очередь на предупреждение возникновения компьютерных инцидентов на ее объектах, а также существенно снизит общественно-политические, финансовые и иные негативные последствия для Российской Федерации в случае проведения против нее компьютерных атак.

Данный законопроект может стать основным нормативно-правовым документом законодательного уровня в рассматриваемой сфере общественных отношений для решения задач, определенных в Доктрине информационной безопасности Российской Федерации.

Участниками «круглого стола» также отмечается, что для целей обеспечения информационной безопасности объектов топливно-энергетического комплекса представляет интерес изучение Системы дистанционного контроля промышленной безопасности опасных производственных объектов, апробированной Ростехнадзором.

Создание информационной системы управления промышленной безопасностью на территории Российской Федерации, включающей систему дистанционного мониторинга и риск-ориентированного надзора на поднадзорных объектах, Ростехнадзор проводит совместно с ЗАО «Российская корпорация средств связи» и Компаниями ПАО «СИБУР», ПАО «Газпром», ПАО «Лукойл».

Основная часть данных ОПО I и II классов опасности уже оснащена автоматизированными системами управления и безопасности технологическими процессами с применением современной микропроцессорной техники.

Требование обязательности контроля технологических параметров закреплены в статье 9 Федерального закона от 21.07.1997 № 116-ФЗ «О промышленной безопасности опасных производственных объектов».

Одновременно, с 1 января 2017 года вступают в силу требования пункта 11 ФНиП «Правила безопасности в нефтяной и газовой промышленности», определяющие обязанность организаций обеспечить дистанционную передачу данных о состоянии ОПО в Ростехнадзор.

В 2015-2016 годах были созданы и реализованы пилотные проекты по внедрению системы дистанционного контроля за состоянием промышленной безопасности (далее – Системы) на морской платформе МЛСП-1 ООО «ЛУКОЙЛ-Нижневолжскнефть» в Каспийском море на базе отечественного программного продукта и на ОПО нефтехимической промышленности ПАО «Сибур» на установке по производству этилбензола и установке газофракционирования ЗАО «Сибур-Химпром» (г.Пермь).

Создаваемая Система позволяет с использованием широкого спектра протоколов информационного взаимодействия получать от автоматизированных систем диспетчерского управления, управления технологическими процессами предприятия информацию о технологических параметрах производства и сигналов, характеризующих состояние промышленной безопасности ОПО, и передавать ее в Ситуационно-аналитический центр Ростехнадзора для аналитической обработки в режиме реального времени, оценки и прогнозирования рисков промышленной безопасности, сигнализации и оповещения соответствующих служб

Ростехнадзора при возникновении угрозы возникновения аварийной ситуации.

Защита передаваемых по каналам связи данных обеспечивается путем их криптозащиты, а также посредством создания защищенных соединений.

Разрабатываемая Система позволяет развивать в Российской Федерации отрасль информационных технологий за счет создания, развития и внедрения отечественных разработок, что соответствует положениям по информационной безопасности Российской Федерации, определенных в Доктрине информационная безопасность Российской Федерации (утверждена Указом Президента Российской Федерации от 05.12.2016 г. № 646).

Кроме того, внедрение Системы дает следующие преимущества для предприятия:

1. Сокращение административного давления на бизнес за счет уменьшения количества проверок и продолжительности (на порядок) их проведения, минимизации роли человеческого фактора при реализации функций надзора за ОПО.

2. Повышение результативности контроля за счет обеспечения возможности принятия превентивных мер для предотвращения аварий на ОПО.

3. Данное решение практически не приводит к дополнительной нагрузке на предприятия: не предполагает задействование дополнительного контрольно-измерительного оборудования на поднадзорном объекте, исключает дублирование функций с автоматизированными системами производственного контроля предприятий.

31 мая 2016 года работа Системы, установленной на морской платформе МЛСП-1 ООО «ЛУКОЙЛ-Нижневолжскнефть», была продемонстрирована Председателю Правительства Российской Федерации Д.А.Медведеву и получила одобрение. Председатель Правительства высказал позицию о необходимости внедрения Системы для ОПО 1 класса опасности.

Ростехнадзор считает необходимым установить на законодательном уровне требования по использованию (применению) «Системы» и передаче информации, так как в соответствии с Федеральным законом от 12.03.2014 № 31-ФЗ «Об информации, информационных технологиях и о защите информации» все случаи обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

Участники «круглого стола» отмечают, что в настоящее время, когда федеральные органы исполнительной власти являются основными носителями информации об объектах топливно-энергетического комплекса, ведущими реестры, содержащие сведения об эксплуатируемом оборудовании на предприятии, информацию об автоматизированных системах управления, рисках и опасностях этих объектов.

В 2016 году Минэнерго России проведена оценка рисков и угроз энергетической безопасности, связанных с использованием систем удаленного мониторинга и диагностики критически важного энергетического оборудования в Российской Федерации. Выделяются следующие виды рисков в части автоматизированных систем управления технологическими процессами и систем мониторинга:
- риск эмбарго (блокирования поставок продукции или предоставления услуг);
- риск отзыва лицензии;
- риски, связанные с информационной безопасностью (уязвимости к кибернетическим атакам, различные программные и аппаратные «закладки», недокументированные возможности и т.п.).

Отмечаем, что процесс сбора, хранения и передачи данных о техническом состоянии энергетического оборудования, используемых системами удаленного мониторинга и диагностики критически важного энергетического оборудования все еще остаётся на недостаточно прозрачном уровне. При этом в числе угроз энергетической безопасности Российской Федерации все еще остаётся использование генерирующими компаниями систем удаленного мониторинга и диагностики оборудования иностранных производителей, система анализа и хранения данных газотурбинного и энергетического оборудования которых расположена за пределами территории Российской Федерации.

Кроме того, в соответствии с постановлением Правительства Российской Федерации от 01.12.2009 г. № 982 «Сети, системы и комплексы вычислительные электронные цифровые» включены в перечень продукции, подлежащей обязательной сертификации. Указанное постановление принято во исполнение Федерального закона Российской Федерации от 27.12.2002 г. № 184-ФЗ «О техническом регулировании».

Федеральным законом от 27.12.2002 г. № 184-ФЗ «О техническом регулировании» не предусмотрено регулирование отношений, связанных с разработкой, принятием, применением и исполнением требований к осуществлению деятельности в области промышленной безопасности, безопасности технологических процессов на опасных производственных объектах, требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики (п. 4 ст. 1 № 184-ФЗ от 27.12.2002 г.).

В этой связи, в целях обеспечения надежности и безопасности объектов электроэнергетики, для мониторинга и управления которыми применяются автоматизированные системы управления, необходимо рассмотрение и принятие проекта постановления Правительства Российской Федерации «Об установлении требований в отношении базовых (обязательных) функций и информационной безопасности при создании и эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики критически важного энергетического оборудования и порядке сертификации систем».

В рамках проекта постановления предлагается принятие комплекса мер по обеспечению информационной безопасности систем удаленного мониторинга и диагностики, прямо или косвенно влияющих на надёжность и безопасность функционирования

критически важного энергетического оборудования.

Предлагаемые проектом постановления требования позволят установить адаптированные к общественным отношениям в сфере электроэнергетики единые правила, применимые для компаний, осуществляющих эксплуатацию, мониторинг и диагностику технического состояния критически важного энергетического оборудования с использованием систем удаленного мониторинга и диагностики, производителей программного обеспечения, входящего в состав систем удаленного мониторинга и диагностики, организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств защиты информации, компаний-заявителей на осуществление сертификации продукции в системе сертификации ФСТЭК России.

Обязательная сертификация позволит не только раскрыть все исходные данные и коды, но и обяжет иностранного производителя создать на территории Российской Федерации центры обработки данных и аналитические центры для российских потребителей услуг. Кроме того, внесение изменений в Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологий и защите информации» в части определения понятий «технологические данные» и «инфраструктура технологических данных» позволит ограничить «оборот» технологических данных (данных, полученных при фактической эксплуатации единиц оборудования) за пределами Российской Федерации и иностранными контрагентами.

В настоящее время обеспечение информационной безопасности организаций топливно-энергетического комплекса осуществляется в соответствии с внутренними нормативными документами каждой компании. Это приводит к тому, что уровень защиты информации в каждой компании разный, так как зависит от компетенции работников, отвечающих за информационную безопасность, и принимаемых руководством компаний рисков информационной безопасности.

Кроме того, имеются трудности при обеспечении информационной безопасности, касающиеся обмена информацией между организациями топливно-энергетического комплекса.

Необходимо также учитывать, что у компаний со 100% долей государства затраты на создание или модернизацию системы защиты информации должны включаться в тариф (устанавливаются регулирующим органом методом экономически обоснованных расходов (затрат) в соответствии с Основами ценообразования в области регулируемых цен (тарифов) в электроэнергетике, утвержденными Постановлением Правительства Российской Федерации от 29.12.2011 № 1178).

Для определения единого подхода к обеспечению информационной безопасности, обоснования затрат на создание системы защиты информации на предприятиях ТЭК представляется необходимым разработать отраслевую нормативную документацию, стандартизирующую подходы к обеспечению информационной и кибербезопасности.

В настоящий момент в Минэнерго России создана межведомственная рабочая группа по разработке проекта документа по созданию системы защиты информации и информационно-телекоммуникационных сетей объектов ТЭК.

По мнению представителей ПАО «Россети», необходима разработка национальных стандартов по защите информации, циркулирующей по беспроводным каналам передачи данных в процессе взаимодействия объектов промышленного интернета с инфраструктурой объектов сетевого комплекса. В первую очередь требуется обеспечить защиту целостности и доступности технологической информации, а также надежную совместную работу всех составляющих энергосистему элементов в едином технологическом процессе. Защита информации в процессе дистанционного и удаленного мониторинга объектов сетевого комплекса, а тем более телеуправления невозможна без применения криптографических алгоритмов и протоколов обеспечения безопасности информации. Необходима разработка отечественных алгоритмов и протоколов, отечественных встраиваемых операционных систем и операционных систем реального времени для применения в специализированных технических устройствах, в устройствах с низким энергопотреблением и обеспечения реагирования на события в рамках заданных временных ограничений при заданном уровне функциональности.

Представляется необходимым актуализировать руководящие документы ФСТЭК России в части Базовой модели угроз, Общих требований по обеспечению безопасности информации, Методике определения актуальных угроз, Рекомендаций по обеспечению информационной безопасности. Для обеспечения противодействия новым вызовам и угрозам безопасности ТЭК России и обеспечения надежности технологических процессов в электроэнергетике при проектировании и строительстве объектов, производстве оборудования и устройств, а в последствии при эксплуатации инфраструктуры электросетевого комплекса различной категории опасности необходимо принять в форме нормативных правовых актов отраслевые, обязательные к применению, требования и стандарты в части:
- набора профилей защиты информации на всех уровнях управления;
- типовой архитектуры системы защиты информации и информационно-телекоммуникационных сетей объектов ТЭК для каждой категории опасности;
- количественного и качественного оснащения системами и средствами защиты информации и информационно-телекоммуникационных сетей объектов ТЭК, персоналом;
- проведения оценки защищенности объектов ТЭК;
- организации эксплуатации и проверки, вновь вводимых средств защиты информации, программного обеспечения АСТУ, системы защиты АСТУ на объектах;
- информированию и обучению персонала основам информационной безопасности.

Для обеспечения возможности фиксации фактов аварий, произошедших в результате компьютерных атак или инцидентов, представители ПАО «Россети» считают необходимым внести изменения в Постановление Правительства Российской Федерации от 28 октября 2009 г. № 846 «Об утверждении Правил расследования причин аварий в электроэнергетике».

Требования по информационной безопасности должны появляться, по мнению представителей ПАО «Россети», на самых ранних этапах жизненного цикла объектов ТЭК. Необходимо актуализировать положения постановления Правительства Российской Федерации от 16 февраля 2008 г. № 87 «О составе разделов проектной документации и требованиях к их содержанию», в части требований к определению угроз безопасности и оценке класса защищенности объекта и включения в проектную документацию

требований по реализации защиты информации, обеспечивающей нейтрализацию указанных угроз, применению программно-технических средств обеспечивающих заданный уровень доверия и отсутствия не декларированных возможностей.

Участники «круглого стола» отмечают недостаточность в настоящее время на российском рынке труда квалифицированных специалистов, владеющих вопросами обеспечения информационной безопасности АСУ ТП, что указывает на необходимость их подготовки через обязательное или рекомендуемое прохождение специализированного обучения по вопросам обеспечения информационной безопасности объектов ТЭК ответственных за обеспечение информационной безопасности АСУ ТП на каждом из объектов ТЭК. Например, по пути обязательного прохождения обучения решил пойти Центральный Банк Российской Федерации, который заявил о подобных планах и в ближайшее время планирует сформировать требования к компетенциям, которыми должны будут обладать ответственные за обеспечение информационной безопасности в организациях банковской сферы, по результатам прохождения ими соответствующего обучения.

По линии МЧС России в настоящий момент ведется работа по внедрению технологий дистанционного и удаленного мониторинга параметров предприятий ТЭК России на основе положений ГОСТ Р 22.1.13-2013 и организация системы реагирования на данные мониторинга.

В ходе реализации положений ГОСТ Р 22.1.13- 2013 «Безопасность в чрезвычайных ситуациях. Мероприятия по гражданской обороне, мероприятия по предупреждению чрезвычайных ситуаций природного и техногенного характера. Структурированная система мониторинга и управления инженерными системами зданий и сооружений. Требования к порядку создания и эксплуатации» в МЧС России прорабатывается вопрос по законодательной проработке внедрения на объектах ТЭК дистанционного и удаленного мониторинга предприятий на базе технологий структурированной системы мониторинга и управления инженерными системами зданий и сооружений (далее – СМИС).

СМИС представляет собой унифицированную систему сбора и передачи данных в Единую государственную систему предупреждения и ликвидации чрезвычайных ситуаций (далее – РСЧС). Для реализации СМИС на объектах ТЭК необходимо разработать стандарты на создание СМИС конкретного вида предприятия.

Перечень и объем данных мониторинга должны быть согласованы в рамках Единой государственной системы предупреждения и действий в чрезвычайных ситуациях и поступать субъектам в федеральные органы исполнительной власти и госкорпорации, являющиеся ответственными за функциональные подсистемы Единой государственной системы предупреждения и действий в чрезвычайных ситуациях.

В целях реализации указанных задач МЧС России отмечает необходимость принятия мер по совершенствованию нормативных правовых документов, устанавливающих правовые основы обеспечения безопасности автоматизированной системы управления (АСУ КВО) и иных объектов критической инфраструктуры Российской Федерации. Данные предложения были сформированы МЧС России при выполнении пункта 13 плана мероприятий второго этапа Основных направлений государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации, утвержденного Поручением Председателя Правительства Российской Федерации от 10 декабря 2013 года № ДМ-П10-8883.

По мнению Ростехнадзора, анализ информационных систем, разработанных МЧС России, в том числе и СМИС, показывает, что показатели, указанные в данных системах, не отражают все вопросы прогнозирования, выявления, анализа и оценки рисков аварий, необходимые для реализации основных положений Стратегии национальной безопасности Российской Федерации, Доктрины энергетической безопасности Российской Федерации, Доктрины информационной безопасности Российской Федерации и внедрению риск-ориентированного подхода в надзорную деятельность с целью снижения риска аварий.

По информации полученной от ПАО «Транснефть», в соответствии с совместным приказом МЧС России, Минсвязи России и Минкультуры России от 25 июля 2006 г. № 422/90/376 «Об утверждении Положения о системах оповещения населения» на объектах ПАО «Транснефть» предусматриваются региональные автоматизированные системы централизованного оповещения о чрезвычайных ситуациях (далее - ЧС). Указанные объекты оснащаются системами автоматического регулирования, блокировок и сигнализации, обеспечивающие как мониторинг, так и контроль состояния отдельных установок и технологических процессов на всех уровнях производства дежурно-диспетчерской службой.

Оснащение объектов ПАО «Транснефть» дополнительной системой мониторинга СМИС приведет к дублированию функционала штатных систем автоматизации, которыми уже оснащены объекты ПАО «Транснефть». В целом автоматизированные системы, установленные на объектах ПАО «Транснефть», совместно с региональной автоматизированной системой централизованного оповещения о ЧС выполняют весь спектр функций, предусмотренных требованиями по разработке СМИС.

Учитывая, что все объекты магистральных нефтепроводов и нефтепродуктопроводов ПАО «Транснефть» функционируют в едином технологическом режиме, контроль состояния объектов в реальном времени осуществляется посредством действующей в ПАО «Транснефть» многоуровневой иерархической АСУ ТП. Согласно действующим регламентам и инструкциям все диспетчерские службы обязаны в оперативном режиме передавать сообщения о возможных ЧС на объектах в местные территориальные органы МЧС России.

Создание на объектах системы СМИС как дублирующей функции штатных систем АСУ ТП, по мнению представителей ПАО «Транснефть», приведет к снижению уровня безопасности данных объектов. Вмешательство специалистов, не имеющих специальной подготовки и допуска к управлению технологическими объектами магистральных нефтепроводов и нефтепродуктопроводов, которое предполагается в соответствии с требованиями п.5.1 ГОСТ Р 22.1.12-2005 в управление технологическим процессом в целом и на отдельных технологических участках, значительно повысит вероятность возникновения аварий и ЧС, а дублирование функции оперативного управления объектами магистральных нефтепроводов и нефтепродуктопроводов приведет к необоснованным и дополнительным финансовым затратам операторов магистрального трубопроводного транспорта Российской Федерации, росту капитальных и эксплуатационных затрат и соответственно росту

тарифов на транспортировку.

Участники «круглого стола» отмечают, что тема использования СМИСа в качестве системы дистанционного мониторинга объектов ТЭКа, активно дискутируемая энергетическим сообществом, ввиду неоднозначного ее восприятия, требует еще более внимательной и глубокой проработки на уровне секций экспертного Совета при Комитете Государственной Думы по энергетике.

Участники «круглого стола» отмечают, что в соответствии со ст. 11 Федерального закона от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»: «В целях обеспечения безопасности объектов топливно-энергетического комплекса субъекты топливно-энергетического комплекса создают на этих объектах системы защиты информации и информационно-телекоммуникационных сетей от неправомерных доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий и обеспечивают функционирование таких систем».

Создание таких систем предусматривает планирование и реализацию комплекса технических и организационных мер, обеспечивающих, в том числе, антитеррористическую защищенность объектов топливно-энергетического комплекса.

Информация о системах защиты информации и информационно-телекоммуникационных сетей является информацией, доступ к которой ограничен соответствующими федеральными законами. Указанная информация вносится в паспорта безопасности объектов топливно-энергетического комплекса.

В пункте 29 проекта указанных требований определено, что обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления производственными и технологическими процессами осуществляется персоналом объекта топливно-энергетического комплекса, ответственным за эксплуатацию системы и сотрудниками Департамента безопасности в соответствии с эксплуатационной документацией на систему защиты и организационно распорядительными документами по защите информации.

Необходимо отметить, что постановление Правительства Российской Федерации, утверждающие указанные требования до настоящего времени не принято.

Так, например, к основным, применяемым в Группе «Интер РАО» мерам защиты, относятся обеспечение предотвращения несанкционированных подключений систем АСУ ТП к сетям общего пользования (сети «Интернет»), устройствам беспроводной передачи данных, использования личных съемных носителей информации, исключения несанкционированного физического доступа к объектам АСУ ТП. Особое внимание уделяется системам удаленного мониторинга и обновления программного обеспечения систем управления энергетическим оборудованием иностранного производства.

Однако значительные сложности при построении систем защиты АСУ ТП возникают вследствие отсутствия типовой модели угроз, определяющей на государственном уровне методику определения угроз, нейтрализация которых должна быть обязательной при выборе основных и компенсирующих защитных мер (применение в этих целях существующей базы данных угроз ФСТЭК не позволяет полностью решить проблему). По мнению группы «Интер РАО» представляется необходимым скорейшую разработку, в рамках законотворческой деятельности и во исполнение пункта 1 статьи 11 Федерального закона от 21.07.2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» и положений приказа ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» базовой модели угроз информационной безопасности систем АСУ ТП, устройств релейной защиты и автоматики (РЗА) и устройств противоаварийной автоматики (ПА) объектов электрогенерации, управляемых и/или служащих источниками оперативной информации для Системного Оператора электроэнергетической системы Российской Федерации (ПАО «СО ЕЭС»).

По экспертной оценке Группы «Интер РАО», вышеуказанная базовая модель угроз безопасности АСУ ТП должна базироваться на перечне инцидентов и аварийных ситуаций, определенных п. 4 «Правил расследования причин аварий в электроэнергетике» от 28.10.2009 г., с учетом изменений, принятых Постановлением Правительства Российской Федерации № 525 от 10.06.2016 г.

Большой интерес обеспечения информационной безопасности представляет опыт Государственной корпорации «Росатом», являющейся на данное время передовой компанией в части обеспечения информационной безопасности топливно-энергетического комплекса России.

Одним из примеров создания в Госкорпорации «Росатом» территориально распределенной защищенной системы, имеющей отношение к энергетике, является автоматизированная система управления энергоэффективностью, основная задача которой – автоматизация управления энергосбережением на всех уровнях административно-территориальной иерархии: от дирекций и дивизионов Госкорпорации «Росатом» до организаций, включая их филиалы.

В АСУЭ обрабатывается служебная информация ограниченного распространения (служебная тайна), информация, составляющая коммерческую тайну, а также персональные данные. В качестве «транспорта» используются открытые каналы информационно-телекоммуникационной сети «Интернет», для защиты конфиденциальности и целостности данных применяются сертифицированные средства криптографической защиты информации, сертифицированные Федеральной службы безопасности России. Защита информации внутри системы реализована на прикладном уровне, соответствующее программное обеспечение сертифицировано в системе сертификации ФСТЭК России.

Значительно более жесткий подход применяется в атомной отрасли для защиты автоматизированных систем управления технологическими процессами (АСУ ТП) реакторных установок атомных электростанций.

Помимо использования для таких АСУ ТП ГК «Росатом» используется эшелонированная система физической защиты и система гарантированного жизнеобеспечения и непрерывного энергоснабжения.

Известно, что программируемые контроллеры большинства производителей оборудования допускают дистанционное конфигурирование и администрирование в случае наличия канала связи между потребителем и сервисным подразделением производителя. При этом в ряде случаев договоры технической поддержки оборудования предусматривают его подключение к сети общего пользования для удаленной первоначальной настройки и конфигурирования, а также диагностики в случае возникновения проблем. Этот вариант создает канал для проведения атак по сети с целью воздействия на АСУ ТП, в состав которой входят такие программируемые контроллеры. При достаточно высокой квалификации атакующей стороны возможна дезорганизация работы системы с широким спектром возможных негативных последствий.

Изоляция АСУ ТП от внешних сетей не гарантирует защиту от попадания в систему вредоносного кода. Уже упомянутый и наиболее показательный пример – проникновение вируса «Stuxnet» в АСУ ТП центрифужного блока обогатительного завода в Иране. Вирус был занесен через флэш-накопитель во внутреннюю сеть завода, откуда и распространился на компьютеры АСУ ТП. В результате активности вируса часть центрифуг была за короткое время выведена из строя.

Другой вариант проникновения вредоносного кода в программируемые контроллеры – при внесении обновлений программного обеспечения. Известны случаи, когда занесение вредоносного кода осуществлялось первоначально в среду разработки производителя программного обеспечения, в результате чего изготавливаемые с соблюдением технологии новые версии программного обеспечения оказывались зараженными вредоносным кодом. Доставленные по доверенному каналу обновления затем устанавливались у конечных потребителей, делая их системы уязвимыми для воздействия извне.

Одним из возможных решений для данной проблемы является использование аппаратных решений, исключающих перепрограммирование контроллеров при отсутствии физического доступа к ним. Это, например, может быть встроенный в плату контроллера переключатель, блокирующий в одном из положений возможность его перепрошивки. Использование контроллеров собственной разработки со встроенными механизмами защиты резко повышает защищенность АСУ ТП при атаках, нацеленных на контроллеры. При этом предпочтительнее использовать процессоры отечественной разработки.

Также одной из наиболее серьезных угроз для АСУ ТП и территориально распределенных автоматизированных систем является проблема устойчивости сети связи. Не секрет, что в российском сегменте сети «Интернет» значительная часть коммутационного оборудования – импортного производства. Маршрутизаторы даже доминирующих мировых брендов имеют значительное количество (обычно – до нескольких десятков) известных уязвимостей, некоторые из которых обеспечивают возможность удаленного администрирования. При массированной атаке с использованием подобных уязвимостей возможна полная дезорганизация работы глобальной сети в определенных районах, при этом функциональность таких устройств может кардинально изменяться. Разумеется, при этом работа территориально распределенных информационных систем может быть нарушена на длительный срок, как и целостность, и достоверность хранящихся в них данных. Временные и материальные затраты на восстановление их работоспособности могут оказаться весьма значительными. Похоже, что в текущей ситуации для критически важных объектов и мощных энергоустановок необходимо предусматривать возможность перехода на ручное управление объектами управления, пусть даже с некоторым снижением оперативности и функциональности такого управления.

Следует учитывать, что к настоящему времени выявлены десятки тысяч уязвимостей, как программного обеспечения средств вычислительной техники, так и коммуникационного оборудования большинства крупных мировых производителей, что делает потенциально уязвимыми любые создаваемые на их базе сети связи и распределенные вычислительные сети. Существенно и то, что в рамках санкционной политики групп государств легитимность использования таких средств в Российской Федерации в любой момент может оказаться под вопросом на неопределенный срок.

Таким образом, создание устойчивых к злонамеренным внешним воздействиям компонентов АСУ ТП, базирующихся на использовании элементной базы, вычислительных средств и коммуникационного оборудования отечественной разработки и производства, является на ближайшие десятилетия, по сути, единственной альтернативой системам, предусматривающим наличие режима ручного управления, для критически важных объектов энергетики и энергораспределения.

Учитывая вышеизложенное, можно сделать вывод, что проблема импортозамещения электронных компонентов и изделий в сфере вычислительной техники и связи, а также встроенного и общесистемного программного обеспечения для них является одной из наиболее важных и неотложных задач в масштабе государства. Решение ее на уровне отдельных отраслей возможно лишь фрагментарно, причем такой подход заведомо будет более затратным по ресурсам и времени по сравнению с глобальным подходом.

В ходе «круглого стола» представители акционерного общества «Системный оператор Единой энергетической системы» акцентировали внимание участников на необходимость обеспечения надежного непрерывного управления электроэнергетическим режимом Единой энергетической системы России, которая предъявляет чрезвычайно высокие требования к надежности и отказоустойчивости приложений, вычислительных средств и сетей связи, используемых в оперативно-диспетчерском управлении в электроэнергетике и составляющих основу информационно-технологической инфраструктуры электроэнергетики (далее – ИТ-инфраструктура).

Наряду с получаемыми преимуществами от развития информационных технологий электроэнергетика подвергается новым рискам, связанным с безопасностью хранимой, обрабатываемой и передаваемой информации, критичной с точки зрения возможных последствий, как для отрасли, так и для государства в целом.

В силу этого создание и эксплуатация информационных систем должны осуществляться с учетом необходимости обеспечения информационной безопасности энергосистемы и входящих в нее объектов.

Необходимо исключить случаи раскрытия (опубликования) детализированной технологической информации об энергосистеме, входящих в нее объектах, параметрах и результатах их функционирования, свободный неконтролируемый доступ к которой связан с рисками для энергетической безопасности Российской Федерации. Указанный подход должен учитываться при установлении Правительством Российской Федерации обязательных стандартов раскрытия информации субъектами

электроэнергетики и определении состава сведений, включаемых в различные информационные системы.

Федеральным законом от 3 декабря 2011 г. № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса» было утверждено создание правовых и организационных основ для создания Государственной информационной системы топливно-энергетического комплекса (ГИС ТЭК) – федеральной государственной информационной системы, содержащей информацию о состоянии и прогнозе развития топливно-энергетического комплекса. В период с 2012-2014 гг. по указанной системе был утвержден ряд нормативных правовых актов, регулирующих основные этапы создания и внедрения ГИС ТЭК.

Основные работы по созданию и внедрению ГИС ТЭК реализуются на базе ФГБУ «Российское энергетическое агентство» Министерства энергетики Российской Федерации в соответствии с выделенной из средств федерального бюджета субсидией.

Контроль за ходом реализации работ на регулярной основе осуществляет образованная Минэнерго России комиссия по созданию и вводу в эксплуатацию ГИС ТЭК, в состав которой вошли представители Аппарата Правительства Российской Федерации, федеральных органов исполнительной власти и заинтересованных организаций.

Исходя из доклада специалистов Счетной палаты Российской Федерации и Министерства финансов Российской Федерации, представленном на одном из заседаний Комитета Государственной Думы по энергетике, проектом федерального закона «О федеральном бюджете на 2017 год и на плановый период 2018 и 2019 годов» в 2017 году предусмотрены бюджетные ассигнования для целей обеспечения функционирования Государственной информационной системы топливно-энергетического комплекса. При этом работы по созданию указанной системы, по оценке экспертов, на сегодняшний день не завершены. ГИС ТЭК в промышленную эксплуатацию не введена, находится на стадии завершения опытной эксплуатации.

Отдельным направлением работы по обеспечению, в том числе и информационной безопасности объектов топливно-энергетического комплекса России, является совместная работа Комитета Государственной Думы по энергетике с Межпарламентской Ассамблей государств – участников СНГ.

В настоящий момент Межпарламентской Ассамблеей государств – участников СНГ проводится работа по сближения законодательства государств-участников СНГ в сфере обеспечения информационной безопасности. Так, в соответствии с Межгосударственной программой совместных мер борьбы с преступностью на 2014-2018 годы, утвержденной решением Совета глав государств СНГ 25 октября 2013 г., МПА СНГ подготовлен проект «Стратегии информационной безопасности государств – участников Содружества Независимых Государств», направленный на международное сотрудничество по сближению государственных политик государств – участников СНГ в области обеспечения информационной безопасности, приняты модельные законы «О критически важных объектах информационно-коммуникационной инфраструктуры» (постановление МПА СНГ от 28.11.2014 № 41-14) (опубликован в «Информационный бюллетень МПА СНГ» 2015, № 62, ч. 2, с. 58,) и «Об информации, информатизации и обеспечению информационной безопасности» (постановление МПА СНГ от 28.11.2014 № 41-15) (опубликован в «Информационный бюллетень МПА СНГ» 2015, № 62, ч. 2, с. 98).

В то же время, в процессе насыщения информационными системами контуров управления критически важными объектами инфраструктуры государств возникает необходимость систематизации и унификации правовых режимов таких объектов, и, тем более, объектов топливно-энергетического комплекса, для обеспечения общих целей национальной безопасности.

На основании вышеизложенного, Комитет р е к о м е н д у е т:

Правительству Российской Федерации:
- рассмотреть возможность на законодательном уровне в обязательном порядке министерствам и ведомствам, в той или иной мере курирующих вопросы топливно-энергетического комплекса, согласовывать собственные отраслевые стандарты информационной безопасности в соответствии с отраслевыми приказами регуляторов. Данная работа определит и инициирует конкретную практическую реализацию мер информационной безопасности, определенных как в Доктрине информационной безопасности, так и в проекте федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации»;
- предусмотреть на законодательном уровне или соответствующим приказом создание Ситуационного центра топливно-энергетического комплекса, в рамках государственной информационной системы топливно-энергетического комплекса, определенной Федеральным законом от 3 декабря 2011 г. № 382-ФЗ «О государственной информационной системе топливно-энергетического комплекса»;
- в рамках указанного Ситуационного центра предлагается рассмотреть определение специализированной функции централизованного мониторинга информационной безопасности, в соответствии пунктом 4 статьи 6, и пунктами 19 и 20 статьи 10 20 Федерального закона от 3 декабря 2011 года №382-ФЗ «О государственной информационной системе топливно-энергетического комплекса»;
- предусмотреть единый подход с определением критериев по выбору импортозамещающих средств в рамках концепции построения Ситуационного центра, с приоритетом инновационного и перспективного решения информационной безопасности, для реализации стратегических целей, определенных пунктом 25 и пунктом 26 Доктрины информационной безопасности: ликвидации зависимости от зарубежных информационных технологий, повышение конкурентоспособности российских компаний в отрасли защиты информации и информационных технологий и поддержка инновационного и ускоренного развития системы информационной безопасности;
- предусмотреть однозначное и прозрачное взаимодействие указанного Ситуационного центра с инфраструктурой ГосСОПКА, определенной в Указе Президента Российской Федерации от 15 января 2013 года № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)»;
- проработать вопрос о необходимости внесения в законодательство Российской Федерации изменений, предусматривающих установление обязательных требований к обеспечению безопасности информационных систем объектов топливно-энергетического комплекса в зависимости от присвоенной объекту категории опасности;
- в рамках программ импортозамещения на законодательном уровне рассмотреть возможность создания условий, мотивирующих

отечественные компании к разработке собственного системного и прикладного программного обеспечения для АСУ ТП, а также к созданию отечественной компонентной базы, организации сборочного производства на территории Российской Федерации. При этом необходимо иметь в виду, что «сборка» на территории Российской Федерации иностранного оборудования в отечественные корпуса не может считаться «импортозамещением»;
- рассмотреть возможность законодательного регламентирования требования по обеспечению защиты информации АСУ ТП объектов топливно-энергетического комплекса Российской Федерации.

2. Министерству энергетики Российской Федерации:
- продолжить работу по разработке отраслевой нормативной документации, стандартизирующей подходы к обеспечению информационной и кибербезопасности на предприятиях топливно-энергетического комплекса Российской Федерации, принимая во внимание материалы, разрабатываемые в рамках Российского национального комитета Международного Совета по большим электрическим системам высокого напряжения (РНК СИГРЭ), результаты реализации проектов по информационному обмену между организациями топливно-энергетического комплекса.

3. Государственной Думе Федерального Собрания Российской Федерации:
- ускорить работу над проектом федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации», внесенным Правительством Российской Федерации, дополнив необходимые изменения ко второму чтению, с учетом обсуждения на «круглом столе» и итоговых рекомендаций, учитывающие специфику и стратегическое значение топливно-энергетического комплекса Российской Федерации, изменения, предусматривающие установление обязательных требований к обеспечению безопасности информационных систем объектов топливно-энергетического комплекса, в зависимости от присвоенной объекту категории опасности, и учитывающие многоплановость структуры собственности объектов топливно-энергетического комплекса России.

4. Комитету Государственной Думы по энергетике:
- на уровне профильных Секций Экспертного Совета при Комитете Государственной Думы по энергетике проработать предложения по использованию СМИСа, в качестве системы дистанционного мониторинга объектов ТЭКа, использованию новых подходов в надзоре, дистанционного контроля, как одного из мероприятий по контролю, исследования правового обеспечения новых подходов в надзоре;

5. Субъектам топливно-энергетического комплекса Российской Федерации:
- предоставить предложения и замечания к проекту федерального закона № 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации» до его рассмотрения Государственной Думой в первом чтении;
- рассмотреть вопрос о постепенной замене АТС, обеспечивающих производственную деятельность, импортного производства на отечественную продукцию.

6. ФСБ России:
- в рамках функционирования ГосСОПКА организовать информирование, в том числе через Минэнерго России, субъектов топливно-энергетического комплекса Российской Федерации об опасности использования АТС и оборудования связи различных зарубежных производителей.

Председатель Комитета П.Н.Завальный

информационная безопасность, безопасность критической информационной инфраструктуры