Выступление члена Экспертного совета при Комитете Государственной Думы по энергетике Шабалина Сергея Васильевича

Уважаемые организаторы, участники и гости конференции «Кибербезопасность в условиях цифровой трансформации»!

Тема моего доклада «**Безопасность и антитеррористическая защищенность объектов ТЭК в условиях цифровой энергетики**».

Минэнерго России и подведомственные ведомству организации в рамках реализации полномочий в области противодействия терроризму, в пределах компетенции участвуют в работе по обеспечению безопасности и антитеррористической защищенности *(далее – АТЗ)* объектов топливно-энергетического комплекса *(далее – ТЭК)* на базе антитеррористического законодательства Российской Федерации, в том числе Федерального закона от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» и других подзаконных НПА.

Также для Минэнерго России и организаций ТЭК являются актуальными задачи обеспечения защищенности информационных систем. Соответствующая норма закреплена в статье 11 Федерального закона № 256-ФЗ.

Информационные технологии активно внедряются

при построении автоматизированных систем управления производственными и технологическими процессами *(далее – АСУ ПТП)*, 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 наряду с заимствованным программным обеспечением, также и иностранного оборудования, имеющего уязвимости, а также существенное увеличение количества АСУ ПТП в сочетании с интенсивным совершенствованием средств и методов применения информационных и коммуникационных технологий в противоправных целях формируют новые угрозы безопасности Российской Федерации.

Сложность технологических процессов производства и передачи электроэнергии и тепла 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 ПТП и её составляющих компонентов

непосредственно зависит надёжность и безопасность объектов, участвующих в едином технологическом процессе.

Напомню, что в мае и июне 2017 года повторились реальные угрозы одного из видов технологического терроризма, в результате которого возможен массовый вывод из строя объектов критической инфраструктуры. Очередные вредоносные программы WannaCry, Petya блокировали работу крупнейших компаний России, Украины и других европейских стран. Атаке подверглись компьютеры энергетических предприятий, банков, правительственных организаций, метро и даже Чернобыльской АЭС.

Данное негативное проявление кибертерроризма еще раз актуализировало необходимость повышения безопасности критической информационной инфраструктуры России, в том числе управляющих информационных систем объектов ТЭК, включая активизацию проводимого в настоящее время импортозамещения программного обеспечения, используемого на этих объектах.

Кроме того, в числе угроз безопасности ТЭК Российской Федерации все еще остаются риски эмбарго (блокирования поставок продукции или предоставления услуг), а также отзыва лицензии, так как в основном авторизированные системы управления поставляются иностранными производителями.

В последнее время всё чаще стали проявляться риски, связанные с информационной безопасностью (уязвимости к кибернетическим атакам, различные программные и аппаратные «закладки», недокументированные возможности и т.п.).

Отмечу, 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.

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 ПТП, в состав которой входят такие программируемые контроллеры. При достаточно высокой квалификации атакующей стороны возможна дезорганизация работы системы с широким спектром возможных негативных последствий.

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 ПТП при атаках, нацеленных на контроллеры. При этом предпочтительнее использовать процессоры отечественной разработки.

Создание устойчивых к злонамеренным внешним воздействиям компонентов АСУ ПТП, 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.

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 рамках действующего законодательства в сфере закупок, субъекты критической информационной инфраструктуры зачастую вынуждены приобретать самую дешевую продукцию, без учета того, где и кем эта продукция была произведена, какое у неё качество, срок службы и условия эксплуатации, есть ли гарантийное и пост гарантийное обслуживание, какой уровень локализации.

При этом важную роль имеет качество производимой продукции. К сожалению, иногда российское оборудование значительно уступает по качеству зарубежным аналогам, периодически появляется брак и срываются сроки поставок.

Что естественным образом вынуждает приобретать оборудование зарубежного производства.

Российским производителям, несомненно, нужна законодательная и финансовая поддержка, необходимы государственные программы стимулирования. Целесообразно ввести систему, позволяющую четко отделять отечественного производителя от зарубежного. Распространять методики, которые, рассчитывают уровень локализации продукции и тем самым получать различные преференции, как на федеральном, так и региональном уровне. Вводить в практику, применение справочника технологических решений отечественных производителей. Не допускать проявления случаев коррупции и контрафакта.

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

В связи с дальнейшим усилением секторальных санкций в отношении топливно-энергетического комплекса Российской Федерации, возрастает актуальность задач по обеспечению

информационной безопасности объектов критической информационной инфраструктуры ТЭК, необходимой, в свою очередь, для обеспечения соответствующего уровня энергобезопасности ТЭК в целом.

Одним из инструментов решения указанной задачи, который уже используется организациями ТЭК, является импортозамещение программного обеспечения.

В реализации политики импортозамещения, в том числе в части программного обеспечения, активное и непосредственное участие с 2014 года принимает Минэнерго России.

Во исполнение поручения Президента Российской Федерации от 21.12.2015 № Пр-2654ГС и поручения Правительства Российской Федерации от 14.01.2016 Минэнерго России совместно с Минкомсвязи России проводит работу по замещению используемых на критически важных объектах ТЭК АСУ ПТП, инженерного и программного обеспечения, оборудования для систем безопасности иностранного производства на отечественные аналоги.

Минкомсвязью России в 2015 году утвержден План импортозамещения программного обеспечения, содержащий мероприятия по импортозамещению всех видов ПО, используемого, в том числе организациями ТЭК.

Кроме того, Минкомсвязи России реализуется дорожная

карта государственной программы «Цифровая экономика» по направлению «Информационная безопасность», предусматривающая в том числе определение приоритетных направлений разработки отечественного общесистемного и прикладного ПО, а также его создание в период с 2018 по 2020 годы.

В соответствии с Федеральным законом от 26.06.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 08.02.2018 № 127 ФСТЭК России, в настоящее время осуществляется категорирование объектов критической информационной инфраструктуры *(далее - КИИ)*, в ходе которого, в том числе собираются сведения о программных и программно-аппаратных средствах, используемых на объектах КИИ.

На основании вышеизложенного представляется целесообразным осуществить следующие мероприятия:

в рамках программ импортозамещения на законодательном уровне рассмотреть возможность создания условий, мотивирующих отечественные компании к разработке собственного системного и прикладного программного

обеспечения для АСУ ПТП, 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»;

предусмотреть единый подход с определением критериев по выбору импортозамещающих средств с приоритетом инновационного и перспективного решения информационной безопасности, для реализации стратегических целей, определенных пунктами 25 и 26 Доктрины информационной безопасности: ликвидация 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.

Спасибо за внимание!