По результатам обсуждения Координационным Советом разработчиков и производителей радиоэлектронной аппаратуры, электронной компонентной базы и продукции машиностроения предложений по мерам обеспечения технологической независимости и безопасности критической информационной инфраструктуры путем использования преимущественно отечественного оборудования и программного обеспечения.

26.08.2019

Формирование рынков в условиях ВТО.

В ГАТТ п. п. 4, 8 "а" ст. III ч. II, установлено следующее:

"Товарам с территории любой договаривающейся стороны, ввозимым на территорию другой договаривающейся стороны, предоставляется режим не менее благоприятный, чем тот, который предоставлен аналогичным товарам отечественного происхождения в отношении всех законов, правил и требований, затрагивающих их внутреннюю продажу, предложение к продаже, покупку, транспортировку, распределение или использование...".

"Положения настоящей статьи не применяются к законам, правилам или требованиям, регулирующим закупки правительственными учреждениями товаров, приобретаемых для правительственных целей, а не для коммерческой перепродажи или для использования в производстве товаров для целей коммерческой продажи".

Аналогичные положения содержатся в ст. II Генерального Соглашения по торговле услугами (ГАТС) (ВТО, Уругвайский раунд многосторонних торговых переговоров, 15 апреля 1994 г.):

"В отношении любой меры, охватываемой настоящим Соглашением, каждый Член немедленно и безусловно предоставляет услугам и поставщикам услуг любого другого члена режим, не менее благоприятный, чем тот, который он предоставляет для аналогичных услуг или поставщиков услуг любой другой страны".

Таким образом, иностранной продукции стран - участниц данного Соглашения необходимо предоставить приоритет наравне с российской продукцией. Под исключение подпадают только

закупки в рамках Закона N 44-ФЗ

Обоснования ограничения допуска продукции, происходящей из иностранных государств.

Идея необходимости защиты национальной безопасности доминировала и доминирует до настоящего времени в антироссийской санкционной политике. С точки зрения законодательства ВТО,, национальная безопасность действительно представляет собой одно из правовых оснований применения исключений из общих принципов ВТО. К таким основаниям, установленным ст. XXI ГАТТ 1994 и ст. XIV-бис ГАТС

СТАТЬЯ XX. ОБЩИЕ ИСКЛЮЧЕНИЯ

При условии, что такие меры не применяются таким образом, который мог бы стать средством произвольной или неоправданной дискриминации между странами, в которых преобладают одинаковые условия, или скрытым ограничениям международной торговли, ничто в настоящем соглашении не препятствует принятию или применению любой договаривающейся стороной мер:

(b) необходимых для защиты жизни или здоровья человека.....;

СТАТЬЯ XXI. ИСКЛЮЧЕНИЯ ПО СООБРАЖЕНИЯМ БЕЗОПАСНОСТИ

Ничто в настоящем Соглашении не должно быть истолковано

(a) как требование к какой-либо договаривающейся стороне предоставлять какую-либо информацию,

раскрытие которой, она считает противоречащим существенным интересам ее безопасности, или

(b) как препятствующее любой договаривающейся стороне предпринимать такие действия, которые она

считает <u>необходимыми для защиты существенных интересов своей безопасности</u>:

(iii) если они принимаются в военное время или в <u>других чрезвычайных обстоятельствах в международных отношениях</u>,

Правила ВТО и ФЗ-187

Изначально ФЗ-187 планировался, как механизм практической реализации исключений правил недискриминационного доступа ВТО:
СТАТЬЯ XX. ОБЩИЕ ИСКЛЮЧЕНИЯ

СТАТЬЯ XXI. ИСКЛЮЧЕНИЯ ПО СООБРАЖЕНИЯМ БЕЗОПАСНОСТИ

Основания для разработки ФЗ-187 - поручение Президента Пр-72 (разработать порядок использования телекоммуникационного оборудования, на объектах инфраструктуры, критически важных областей: транспорт, нефтехимия, энергетика и т.д.)

Кажется очевидным, что первый уровень обороны- защита от незадекларированных возможностей самого оборудования.

В принятой версии Закона речь идет только о защите от компьютерных атак, а не о порядке использования российского оборудования.

Концептуальные проблемы ФЗ-187 «О критической инфраструктуре…»

- Отсутствие порядка отнесения оборудования к критически влияющим на безопасность объекта КИИ.
- Отсутствие определения порядка использования российского оборудования с учетом категорий объектов КИИ.
- Отсутствие мониторинга использования импортного/российского оборудования на объектах КИИ.
- Не определен порядок перехода объектов КИИ на российское оборудование.
- Отсутствие ответственности за нарушение требований нормативных актов, определяющих порядок использования оборудования российского происхождения на объектах КИИ.

В рамках обсуждения порядка использования российского оборудования на объектах КИИ поступили предложения по внесению изменений в следующие НПА

1. Федеральный закон №187 « О критической информационной инфраструктуре»

2. Постановление Правительства №127 «Правила категорирования объектов критической информационной инфраструктуры»,

3. Приказ Минкомсвязи №127 « Методические указания по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры»

4. Разработка постановления Правительства «О мерах по обеспечению выполнения целевых показателей государственной программы «Цифровая экономика» по импортозамещению для объектов инфраструктуры обработки данных, создаваемых или приобретаемых за счет государственного бюджета и бюджетов государственных внебюджетных фондов или предназначенных для оказания услуг государственным органам компаниями любой формы собственности»

Предложения по ФЗ-№187-2

Пункт 8 статьи 2 изложить в следующей редакции:

«8) субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Установить, что российские юридические лица и индивидуальные

предприниматели, которые обеспечивают взаимодействие указанных систем или сетей:

не должны иметь обязательства финансового характера перед иностранной компанией и (или) иностранным гражданином или иностранными гражданами;

конечными бенефициарами (выгодоприобретателями) указанных юридических лиц могут быть граждане российской федерации без двойного гражданства;

индивидуальными предпринимателями могут быть граждане российской федерации без двойного гражданства.»

Предложения по ФЗ-№187-З

Статью 6 (полномочия Президента и органов государственной власти) дополнить частью 6 следующего содержания:

«6) Федеральный орган исполнительной власти, осуществляющий функции по противодействию легализации (отмыванию) доходов, полученных преступным путем, осуществляет мониторинг соблюдения положений пункта 8 статьи 2 настоящего Федерального закона в части отсутствия иностранного участия в уставном капитале и обязательств финансового характера перед иностранной компанией и (или) иностранным гражданином или иностранными гражданами в отношении российских юридических лиц.»;

Предложения по ФЗ-№187-4

дополнить часть 2 статьи 6 (полномочия Правительства) пунктом 4 следующего содержания:

« 4) случаи и правила по использованию российского программного обеспечения и оборудования на объектах критической информационной инфраструктуры, включая минимальные потребительские свойства такого программного обеспечения и оборудования (при необходимости);

5) **утверждает обязательный для исполнения субъектами критической информационной инфраструктуры график перевода объектов критической информационной инфраструктуры на использование отечественных товаров (работы, услуг).»**

Предложения по ФЗ-№187-5

Статья 11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры :

1. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, дифференцируются в зависимости от категории значимости объектов критической информационной инфраструктуры и этими требованиями предусматриваются:

1) планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) принятие организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

3) установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры.

2. Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, могут устанавливать дополнительные требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, содержащие особенности функционирования таких объектов в установленной сфере деятельности.

Статью 11 предлагается дополнить частью 3 следующего содержания:

«3. При создании, обслуживании, эксплуатации, модернизации, выводе из эксплуатации и утилизации объектов критической информационной инфраструктуры либо их элементов (составных частей) запрещается:

использование иностранных товаров;

выполнение работ, оказание услуг иностранными юридическими лицами, юридическими лицами, в которых суммарная доля прямого и (или) косвенного участия российских организаций без иностранного участия, граждан Российской Федерации составляет менее ста процентов;

выполнение работ, оказание услуг, в рамках которых осуществляется поставка или использование иностранных товаров.».

Проект ПП «О мерах по обеспечению выполнения целевых показателей государственной программы «Цифровая экономика» по импортозамещению

В рамках исполнения Протокола от 26.10.2017 и Пр-2265 от 05.11.2017 «Правительству разработать и утвердить до 01.04.2018 требования к госорганам, госкорпорациям, компаниям с госучастием более 50% по закупками применению ТКО со статусом ТОРП и российского ПО для создания телекоммуникационной инфраструктуры за счет бюджетных средств, а также для предоставления услуг связи указанным органам и организациям» предлагается:

1. Установить, что компании любой формы собственности при закупке оборудования для создания объектов критической информационной инфраструктуры за счет государственного бюджета и бюджетов государственных внебюджетных фондов или оказания услуг (включая, но не ограничиваясь, такими как: лизинг, услуги классов SaaS, HaaS и подобные, услуги, предусматривающие иные способы приобретения оборудования и программного обеспечения без постановки на баланс государственных органов или государственных внебюджетных органов и подобные) должны руководствоваться постановлениям Правительства № 878 и постановлением Правительства №1236.

2. Включить в состав госконтрактов по закупкам услуг и оборудования, перечисленных в пункте 1, в качестве обязательной статью, предусматривающую обязательное указание идентификатора данной закупки в федеральной государственной информационной системе учета информационных систем (ИС), создаваемых и приобретаемых за счет средств федерального бюджета и бюджетов государственных внебюджетных фондов, и содержащую запись поля «номера компонентов информационно-телекоммуникационной инфраструктуры (ИТКИ) в реестрах отечественного оборудования и ПО» в электронном паспорте ИС».

О изменениях в Приказ Минкомсвязи

Для объектов инфраструктуры обработки данных, создаваемых и приобретаемых за счет государственного бюджета и бюджетов государственных внебюджетных фондов, внести в состав реквизитов электронных паспортов таких объектов, создаваемых в рамках исполнения Приказа Минкомсвязи России от 31.05.2016 №127 «Об утверждении методических указаний по осуществлению учета информационных систем и компонентов информационно-телекоммуникационной инфраструктуры (компонента ИТКИ)» в состав электронного паспорта компонента ИКТИ (раздел III Методики, пункт 18 «Электронный паспорт содержит следующие разделы» раздел 1, подраздел 1.1 «Общие сведения») дополнительную запись: «**номера компонентов ИТКИ в реестрах отечественного оборудования и ПО**», В **случае отсутствия сведений** о принадлежности компонента ИТКИ к одному из реестров в данной записи должен быть указан идентификатор **Заключения уполномоченного на проведение экспертизы органа об обоснованности требований** к ИКТИ в рамках данной ИС и отсутствии отечественных аналогов для реализации данной ИС.

О изменениях в ПП №127 «Об утверждении правил категорирования объектов критической инфраструктуры Российской Федерации ...»

1. В пункте 8 Правил категорирования объектов КИИ РФ» второй абзац изложить в следующей редакции:

Для создаваемого объекта критической информационной инфраструктуры, указанного в абзаце первом настоящего пункта, категория значимости может быть уточнена в ходе его проектирования. **В ходе проектирования субъект критической инфраструктуры должен руководствоваться требованиями по использованию компьютерного, серверного и телекоммуникационного оборудования российского происхождения на объектах ОИОД в соответствии с категорией объекта.**

Примечание. Оборудованием российского происхождения считается оборудование, находящееся в Едином реестре радиоэлектронного оборудования Минпромторга РФ, программное обеспечение в реестре отечественного ПО Министерства цифрового развития РФ.

О изменениях в ПП №127 «Об утверждении правил категорирования объектов критической инфраструктуры Российской Федерации ...»

4. В пункте 10 (Исходные данные для категорирования) подпункт «а)» изложить в следующей редакции:

а) сведения об объекте критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи), **сведения о нахождении компьютерного, серверного и телекоммуникационного оборудования объектов, входящего в состав ОИОД в соответствующем реестре оборудования и программного обеспечения российского происхождения, (номер в реестре) или заключение уполномоченного Экспертного совета об отсутствии отечественного оборудования и программного обеспечения в соответствующем реестре.**

О изменениях в ПП №127 «Об утверждении правил категорирования объектов критической инфраструктуры Российской Федерации ...»

1. В пункте 17 (Сведения о результатах присвоения категории объекту КИИ, направляемые в уполномоченный орган исполнительной власти) подпункт «д)» изложить в следующей редакции:

д) сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры, в том числе средствах, используемых для обеспечения безопасности объекта критической информационной инфраструктуры и их сертификатах соответствия требованиям по безопасности информации (при наличии), **номера регистрации программных средств в реестре отечественного ПО Министерства цифрового развития РФ, номера компьютерного, серверного и телекоммуникационного оборудования, используемого на объекте в критической инфраструктуры в соответствующем реестре оборудования российского происхождения Минпромторга РФ или Заключение экспертного совета о невозможности использовать отечественное оборудование для решения задач данного ОКИ (обязательно)**

ВЫВОДЫ

1.В рамках ФЗ-187 наделить Правительство РФ полномочиями утверждать:

- перечень оборудования и ПО, подлежащих импортозамещению на объектах КИИ;
- правила применения российских оборудования и ПО для каждой категории объектов КИИ;
- обязательный для исполнения субъектами критической информационной инфраструктуры порядок перевода объектов КИИ на использование российских оборудования и ПО;
- установить ответственность за нарушение требований нормативных актов, определяющих порядок использования оборудования российского происхождения на объектах КИИ.

2.Федеральному органу исполнительной власти, уполномоченному в области обеспечения безопасности КИИ проводить мониториг соблюдения правил использования российских оборудования и ПО на объектах КИИ в зависимости от категории

3.Доработать нормативные акты, обеспечивающие приоритетное использование оборудования и ПО российского происхождения