Система стандартизации России изменяется: возможные последствия

В России принят Закон «О техническом регулировании» № 184-ФЗ. О том как вступление в силу этого документа отразится на информационной безопасности в стране в форме публицистического эссе рассуждает директор аналитического департамента компании «Элвис-Плюс» Сергей Вихорев.

Часть первая, полемическая

И мне масла в попку…
(Из старого анекдота)

Вот и мы стали «большими»! Вот и у нас, «лапотных», как и у всех, «цивилизованных» в скором времени появятся Технические регламенты и мы будем жить так же, как и вся Европа! Ура! Мы так хотим побыстрее вступить ВТО, что готовы как всегда — «…до основанья, а затем…» (или, пользуясь нашим безмерным желанием, нас просто вынуждают к этому?).

Жалко, конечно, что одна из самых старейших систем стандартизации, которой более ста лет, рухнула, но так или иначе, еще немного времени и у нас больше не будет тех стандартов, к которым мы привыкли. Будут другие — Технические регламенты.

Правда, не совсем понятно, чем наши ГОСТы были хуже, но это не важно! Главное, что бы «как у всех»: технический регламент — обязательные требования, касающиеся безопасности, стандарт — добровольные, то есть не обязательные, касающиеся качества. У «них» синтетические и трансгенные продукты, и у нас будут! Это же не «безопасность» — никто же не доказал, что они вредны — и государством, то бишь Техническим регламентом[1], не регулируется, это всего лишь «качество», а за качество теперь государство не отвечает, это теперь прерогатива рынка, то бишь базара, а за базар известно кто ответит. Но волноваться не надо, вас обязательно предупредят, что продукты — мутанты (это требует закон). И дома теперь можно строить из картона: дом есть? — есть, если рухнет не придавит? — нет, а остальное — качество. Выбирай, потребитель сам. И многое, что еще можно. Например, можно, чтобы вода в кране пахла навозом — это же не «стрихнин», не отравимся. Кстати, обратите внимание, требования к безопасности продукции, используемой в единой сети связи Российской Федерации, вообще выведены из под действия нового Закона[2]. Это значит, что если у вас закипят мозги от мощного электромагнитного излучения при использовании сотового телефона, например корейского производства — никто не виноват: технический регламент, даже если он и будет содержать требования по электрической и биологической безопасности на эти продукты не распространяется.

Бесспорно, не все было хорошо в «усопшей», но ведь не такая и плохая была покойница, было в ней что-то… Да она нуждалась в чистке, да ее надо было «гармонизировать» с международными родственницами, но зачем же под корень.

Нельзя не согласиться с необходимостью реформы, проведения в жизнь политики «дерегулирования» и «дебюрократизации», как об этом говорит А. В. Данилов-Данильян[3]. Конечно мы все устали от чрезмерного вмешательства государства в экономическую деятельность предприятий, но причем здесь ГОСТы? Действительно, когда, как отмечают наши депутаты, подчеркивая своеволие чиновников и ведомств, «в коммерческую структуру приходит пожарный с проверкой и при этом руководствуется инструкцией принятой при царе горохе[4]» — это плохо. Но это говорит о плохих, устаревших инструкциях чиновникам, а не стандартах пожарной безопасности. И если требования стандарта позволяли защитить от пожара «социалистическую собственность», наверное они позволят защитить и просто собственность, а вот действия пожарного — надо корректировать с учетом современной обстановки и права этой самой собственности. Внятные и стабильные правила игры, как отмечает начальник Экономического управления Администрации Президента РФ, действительно нужны. Но они должны скорее регулировать процедуру контроля, устанавливать рамки (и лучше в области тарифного и налогового регулирования), ограничивать произвол чиновника, но почему для этого надо разрушить старую систему стандартов (читай — требований) и строить новую с нуля?

Согласен, пусть потребитель сам следит за качеством продукции, он не глупый и всегда отличит плохое от хорошего, но государство должно все-таки установить нижний предел, не границы «сверху-снизу», а именно нижний предел, ниже которого уже вряд ли к тому что поступает на рынок применим термин «продукция». Тогда бы всем было бы хорошо: чиновник следил бы за тем, чтобы то, что появляется на рынке называлось бы «продукцией» и дальше не вмешивался (нижний предел), а производитель

стремился бы повысить конкурентность этой самой продукции за счет повышения ее качества (верхнего предела нет, а значит нет и предела совершенства).

Хотелось бы еще отметить, что в Послании Президента РФ Федеральному Собранию в 2002 году, которым часто обосновывают необходимость отмены обязательности существовавших ГОСТов, резкой критике подверглась именно сложившаяся практика контроля предпринимательской деятельности и действующая нормативная база по этим вопросам, а не сами стандарты. А новый закон говорит именно о стандартах, как требованиях к продукции. Кстати, порядок разработки стандартов, предусмотренный новым Законом и предполагающий активное участие в этом процессе представителей самого бизнеса — использовался и ранее, и показывал замечательные результаты. Хорошо, что теперь это закрепили законодательно. Позволю напомнить факты из той сферы, которая мне ближе: практически все нормативные требования по обеспечению безопасности информации при ее обработке с использованием информационных технологий, разрабатывались с привлечением производителей этих самых технологий, но под контролем государственных органов. И мировое сообщество приняло эти требования.

Далее, еще один вопрос. А что такое, собственно, «продукция» и почему Закон приравнивает к ней и «услуги[5]»? (Вопрос не праздный — обеспечение безопасности информации во многом лежит в сфере оказания услуг.) Ведь господа, ратующие за этот Закон немного лукавят, говоря, что международным сообществом «услуга» трактуется как «продукция», что она ничем не отличается и это все одно и тоже[6] и на них также распространяется действие Технических регламентов.

Если уж мы стремимся в ВТО и хотим, что бы было все «как у них», то надо сказать, что торговля услугами регулируется «Генеральным соглашением по торговле услугами» (ГАТС), которое вместо понятий «технический регламент» и «стандарт» использует термин «меры», понимая под этим нормативные правовые акты, регулирующие торговлю услугами. А это совсем другие отношения, имеющие, кстати, свои обязательные ограничения. В области информационной безопасности такие ограничения в законах есть и они, как показывает практика, оправданы.

Часть вторая, пессимистическая

«Если приснится, что кто-
то гладит мохнатой рукой
— спроси: «к добру или худу»…
(«Домострой»)

Человечеству потребовалось не одно столетие, чтобы понять опасность бесконтрольного использования пороха и ввести контроль за использованием взрывчатых веществ. Более полувека ему потребовалось, чтобы оценить опасность радиоактивного излучения. Но, наверное, еще недостаточно времени прошло для того, чтобы у всех, кому положено, пришло осознание опасности неправильного использования информации. Подчеркну, у всех. Президент РФ — понимает эту опасность, свидетельством тому Доктрина информационной безопасности, как особый правовой акт. Многие законодатели — тоже понимают (некоторые испытали эту опасность на себе), у нас законодательно определено более сорока видов тайн, направленных на предотвращение угроз безопасности личности, общества, государства, защиту наших конституционных прав, в том числе на сохранение личной тайны, персональных данных. И если неправомерное обращение с информацией может нанести кому либо ущерб, она должна быть защищена, причем, защищать должен не только сам собственник информации, но и любой другой, кому она стала известна по необходимости[7]. И после всего этого оказывается, что это совсем даже и необязательная компонента, что все это очень даже как добровольно! Жалко, что разработчики этого закона «не увидели в понятии „информация“ один из видов где контролируется безопасность[8]».

Ау! Государство! Ты же должно охранять мои конституционные права, почему же ты бросаешь меня на произвол судьбы? Конечно, сам свою тайну я смогу защитить и буду делать это добровольно. Но если я вынужден (в силу определенных обстоятельств) делиться этой тайной с другими (и необязательно государственными учреждениями), то почему нет обязательных требований по ее защите для них? Они будут делать это добровольно? Дудки! Это им не выгодно, дорого, хлопотно, да и на «качество» это слабо влияет. Государство, ты меня кинуло, и не гладь меня мохнатой рукой, не успокаивай, все равно новый закон применительно к сфере информационной безопасности скорее «к худу», чем «к добру».

Информация очень опасный предмет! Сколько еще должно погибнуть людей из-за нарушения конфиденциальности, сколько компаний разориться, сколько еще должно быть искалеченных судеб, пока некоторые чиновники поймут, что требования по информационной безопасности должны быть обязательными, что надо, пока еще не поздно, менять ст.7 Закона и наряду с биологической безопасностью,

электромагнитной совместимостью, ядерной и радиационной безопасностью вводить и информационную безопасность. И опять лукавят чиновники, говоря, что ничего страшного нет, что «если различные стороны, участвующие в процессе доработки и принятии технического регламента, инициируют ограничительные требования по информационной безопасности для включения в проект технического регламента, и остальные стороны с этим согласятся, значит, так и будет[9]». Позволю себе напомнить выдержку из Закона: «Принятие технических регламентов в иных целях не допускается[10]». Да и сама процедура разработки технических регламентов такова, что мнение заинтересованного лица (который не в состоянии отследить все возможные регламенты по различным видам продукции — ожидается, что их будет около 600, потребуется еще время на формулирование и проталкивание предложений), при всем демократизме и открытости обсуждения проекта регламента, вряд ли будет учтено. А какой разработчик сам, добровольно, себе на выю хомут оденет?

Наверное, говоря об информационной безопасности, и ссылки на 5 статью Закона, определяющую порядок предъявления технических требований к продукции, производимой по государственному заказу, не совсем справедливы. Если бы речь шла только о государственных учреждениях — вопрос был бы решен. Однако, по жизни приходится доверять свои тайны не только государственным учреждениям, которые собственно и осуществляют государственный заказ, но и частным клиникам (медицинская тайна), нотариусам (тайна нотариата), адвокатам (адвокатская тайна), кредитно-финансовым организациям (банковская тайна) и пр. Все они не занимаются «госзаказом», но хранят секреты и должны соблюдать определенные технические требования при автоматизированной обработке информации. На эту тему даже есть международные конвенции, которые говорят об обязательности таких требований.

Часть третья, конструктивная и заключительная

Dura Lex, Sed Lex
(Закон суров, но это — закон)

Мы строим правовое государство. Мы должны исполнять принятые законы, независимо от того, нравятся они нам или нет. Поэтому и этот, уже принятый Федеральный Закон «О техническом регулировании» исполнять надо. Но все-таки, есть еще время. Закон предусматривает семилетний переходный период в течение которого будут разрабатываться технические регламенты. Давайте не упустим эту возможность. Можно на некоторый период специальным распоряжением Президента РФ или Правительства РФ сохранить действующий в настоящее время порядок применения технических требований к средствам обеспечения информационной безопасности. За это время еще раз внимательно посмотреть на проблемы информационной безопасности, внести соответствующие изменения в новый закон и разработать соответствующий технический регламент (не «размазывать» эти вопросы по всем регламентам, а собрать их в один). Это дело тех государственных органов, которые отвечают за обеспечение безопасности информации в России.

Ну а что же делать всем остальным? Как же защитить себя в это достаточно смутное время? Можно предположить, что производители средств защиты, окрыленные новыми требованиями, будут старательно убеждать, что их средства обеспечат защиту, что у них сделано все как на западе, что вообще «зачем ставить межсетевые экраны, давайте поставим средства активного контроля и все проблемы решим». Все это так, да не так. Во-первых, еще, к великому сожалению, встречаются недобросовестные производители, а «пощупать» качество защиты информации — весьма затруднительно. Во-вторых, для того, что бы разобраться во всех этих технических тонкостях — не один пуд соли надо съесть. Поэтому выход здесь видится один: найти высококвалифицированных специалистов, в которых уверены, которым действительно доверяешь и положиться на их опыт. К счастью, сейчас все больше и больше появляется серьезных компаний, которые имеют опыт создания надежных систем защиты информации и предлагают консалтинговые услуги в этой области. Такая компания должна проникнуться проблемами заказчика, стать его партнером по духу, ведь ей доверяются самые дорогие секреты — систему обеспечения безопасности информации. Можно дать несколько советов, на что надо обращать внимание при выборе такого партнера.

Во-первых, не следует слишком часто менять своих консультантов: чем меньше народа знает секреты, тем лучше. Поэтому надо сразу рассчитывать на длительные и доверительные отношения и подходить к такому выбору весьма тщательно.

Во-вторых, убедитесь в надежности компании, предлагающей консалтинг. Естественно, нельзя доверять свои тайны первому встречному. Прежде чем принять решение, посмотрите сколько лет эта компания представлена на рынке, каковы ее успехи, попросите представить рекомендательные письма, может быть воспользоваться советом друзей, которые уже приглашали специалистов.

В-третьих, убедитесь в компетенции специалистов компании. Здесь прежде всего следует обращать внимание на наличие лицензий на выполнение работ в области защиты информации. Правда не обольщайтесь очень, если вам представят все возможные лицензии. Обратите внимание на срок ее выдачи и область ее применения. Обычно лицензию выдают на 3 года. Надо помнить, что, после этого срока, как правило, лицензия продляется. И если за первый срок компания не сделала никаких работ по безопасности информации или к ней были претензии, ей вряд ли продлят лицензию. Поэтому, чем старше лицензия, чем дольше компания занимается вопросами безопасности информации, тем больше уверенности в компетенции ее специалистов. Еще следует обратить внимание на образование специалистов. Наука защиты информации постоянно развивается и требует пополнения знаний. Сейчас достаточно много учебных заведений, которые готовят специалистов нужного профиля. Но среди них есть так сказать «доверенные», то есть те, результаты обучения на которых признаются при выдаче лицензий. Не стесняйтесь, попросите подтвердить квалификацию приглашаемых специалистов.

В-четвертых, отнеситесь к проблеме обеспечения безопасности информации так же, как вы бы отнеслись к выбору своего костюма. Можно пойти и купить подешевле, например, «Москвашвея», но не удивляйтесь, если он будет плохо сидеть, жать в подмышках и мешать при ходьбе. Можно купить подороже, «Пионер», он и сидеть будет, и в подмышках не жмет, но что-то все-таки не так. Ну и, наконец, можно заказать костюм, например у Зайцева — вот это действительно будет, хоть и дорого, но зато именно так, как вам хочется. Так же и в защите информации: типовое решение от «Москвашвея» хотя и дешево, но не всегда решит ваши проблемы. Можно, конечно использовать решения от «Карденов» безопасности, например Microsoft, Cisco и пр., но и это еще не то. И вот только специально построенная под ваш бизнес система обеспечения безопасности информации, учитывающая все нюансы вашей бизнес-модели и возможные угрозы ей — наверное и будет тем самым надежным щитом, который обезопасит вашу информацию.

Кстати, неплохо бы было бы задуматься и об оценке возможностей ваших противников и злоумышленников, которые охотятся за вашими секретами. Без этого невозможно вообще «сшить» надежную систему, так же как без снятия мерки — хороший костюм.

Ну и наконец, самое главное: спасение утопающих — дело рук самих утопающих! Если вы сами не захотите защищать свои интересы, и не будете требовать этого от других — ваши тайны станут известны всем. Сейчас, когда грядет «доброволизация» требований по обеспечению безопасности информации, последнее слово остается за вами.

Сергей Вихорев / Элвис-Плюс

---

[1]«Технический регламент не может содержать требования к продукции, причиняющей вред жизни или здоровью граждан, накапливаемый при длительном использовании этой продукции и зависящий от других факторов, не позволяющих определить степень допустимого риска» — Федеральный Закон № 184-ФЗ «О техническом регулировании», ст.7.7.

2 Федеральный Закон № 184-ФЗ «О техническом регулировании», ст.1.2.

3 «О русском бизнесе без акцента», еженедельный деловой журнал «Русский Фокус», № 32 (69), 29.09.2002.

4 Н. Медведев, член комитета Совета Федерации по экономической политике и предпринимательству Интервью РТР, 01.02.2003 г.

5 Федеральный Закон № 184-ФЗ «О техническом регулировании», ст.1.1.

6 Б. Алешин, Пресс-конференция в Центре стратегических разработок 14.02.2003 г.

7 Федеральный закон «Об информации, информатизации и защите информации», № 24-ФЗ, Гл. 5.

8 Б. Алешин, Пресс-конференция в Центре стратегических разработок 14.02.2003 г.

9 А. Данилов-Данильян, Пресс-конференция в Центре стратегических разработок 14.02.2003 г.

10 Федеральный Закон № 184-ФЗ «О техническом регулировании», ст.6.2