Первые результаты анализа дискуссии

1 августа 2011 года

Итак, можно подводить первые результаты дискуссии по поводу письма Президенту РФ о Законе о ПДн.

Во-первых, и это, наверное, главное, оппоненты сосредоточились в своей критике ответа, в основном, на ТЕХНИЧЕСКИХ вопросах защиты (критика ст. 19 Закона). Лейтмотив выступлений: «Регуляторы хотят защищать устаревшими (20-ти летней давности) СЗИ, требуют обязательную сертификацию, аттестацию и вообще все это дорого, неэффективно и отстает от современного прогресса!» При этом никто из участвующих в дискуссии не говорит, КАКИЕ интересы СУБЪЕКТА ПДн ущемлены в законе, и ПОЧЕМУ он плох для субъекта ПДн (хотя в блогах о-о-очень много разговоров именно о том, что права субъекта не защищены, и именно поэтому закон плох).

Во-вторых, за это время эпистолярный жанр в этой области пополнился письмами в адрес Президента РФ и Председателя Правительства РФ от АРБ и позицией РСПП. Оппоненты обрадовались и с криками: «Вот! Видите! Нас поддерживают серьезные структуры!» продолжили и дальше говорить о ТЕХНИЧЕСКИХ вопросах, не затрагивая интересы субъекта ПДн. Надо сказать, что письма АРБ и РСПП – более взвешенные, содержат аргументацию и правильные ссылки, более того, они выступают не против ВСЕГО Закона, а только против ст. 19. Однако, обе эти уважаемые организации, представляющие интересы далеко не малого и среднего бизнеса и уж, конечно, не субъектов ПДн, ОТКРЫТО заявляют, что новый вариант Закона не выгоден именно ОПЕРАТОРАМ, совершенно игнорируя интересы субъекта ПДн (*«…была рекомендована к принятию принципиально иная редакция статьи 19 Закона № 152-ФЗ, которая предусматривает сохранение ныне действующей, крайне жесткой, неэффективной и чрезвычайно затратной для всех операторов персональных данных модели регулирования мер по обеспечению безопасности персональных данных при их обработке … сохранены положения, применение которых вызывает самые значительные возражения со стороны субъектов рынка и дальнейшая реализация которых повлечет несоразмерные поставленным целям затраты и издержки для всех субъектов Закона № 152-ФЗ как государственных органов, так и юридических лиц.»*[1] *или «…вступление в силу данного закона в принятой редакции, по мнению Комиссии, способно оказать негативное влияние на большинство предприятий, осуществляющих обработку персональных данных работников и клиентов*[2]*»*). Поддержка-то действительно есть, но только такая поддержка опять-таки подтверждает высказанный мною тезис, что подписанты, обращаясь в адрес Президента РФ, преследуют узкокорпоративную цель: защитить интересы бизнеса (даже скорее конкретно банков, что следует и из ремарки А. Токаренко [toparenko] на одном из блогов: «…Алексей Лукацкий и я были приглашены в рабочую группу ЦБ/АРБ как независимые эксперты» http://www.ispdn.ru/news/9270/?ELEMENT_ID=9270&PAGEN_3=2 - обидно же – свое!), чтобы снять с них (операторов) бремя выполнения защиты по требованиям регуляторов и предоставить самим решать КАК защищать. Все снова сводится к недовольству ТЕХНИЧЕСКИМИ мерами защиты. Странная позиция получается: «Мне не нравится ст. 19 закона, потому что это дорого и неэффективно, поэтому весь закон плох и его не надо принимать!»

В-третьих (в письме этого нет, но при обсуждении проявилось), существенная претензия к закону: «Закон не определяет ответственности за ущерб! Вот если бы он это определял, то субъект ПДн был бы защищен! А сейчас получается, что требования по защите превыше всего: штрафуют за невыполнение требований, а не реальные утечки!».

---

[1] Из Письма АРБ Президенту Российской Федерации Медведеву Д.А. "О новой редакции статьи 19 Федерального закона № 152-ФЗ «О персональных данных»", 18.07.2011, Исх. № А-01/5-557. (http://www.arb.ru/site/docs/docs.php?doc=1187)

[2] Протокол № 24 Комиссии РСПП по телекоммуникациям и информационным технологиям, 08.07.2011 г., http://media.rspp.ru/document/1/f/9/f93fc58b3a5fd3acdfa4d132db261c69.pdf

В-четвертых, четко определилась позиция авторов письма в вопросах, КАК надо делать техническую защиту: «Не надо нас учить! Зачем нам требования регуляторов? Мы сами знаем, КАК защищать. Главное для субъекта – получить возмещение ущерба. Вот когда будет такой ущерб, вот тогда и спрашивайте с нас по всей строгости закона! Неправильно наказывать за неисполнение требований, если они не привели к ущербу для субъекта ПДн. Да и вообще, существующая система штрафов не защищает субъекта ПДн, а только увеличивает коррупционную составляющую Закона».

О том, кто «сам с усам»

Начнем с последнего. Здесь уместно вспомнить ст. 2 Конституции РФ: «*Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства*». Обратите внимание: ГОСУДАРСТВА, а не оператора ПДн! А там же в ст. 11 говорится: «*Государственную власть в Российской Федерации осуществляют Президент Российской Федерации, Федеральное Собрание (Совет Федерации и Государственная Дума), Правительство Российской Федерации, суды Российской Федерации*». И еще, там же в ст. 156: «*Законы и иные правовые акты, принимаемые в Российской Федерации, не должны противоречить Конституции Российской Федерации*». Следовательно, по Конституции Государство в лице законодателя (Госдумы) и исполнителя (Правительства) ОБЯЗАНО принять меры к защите прав и свобод, определенных ст. ст. 23-24 Конституции РФ. По-моему, в этой части Закон о ПДн не противоречит, а, наоборот, четко следует принципам, изложенным в Конституции РФ. Можно еще посмотреть ст. 4 Конвенции[3]: «*Каждая сторона принимает необходимые меры в рамках своего внутреннего законодательства в целях придания юридической силы основополагающим принципам защиты данных*…». То есть сама Конвенция как раз и предполагает, чтобы меры защиты ПДн были заложены именно в законе, так как это придаст им юридическую силу. И в чем же здесь неправ наш российский Законодатель? На мой взгляд, он полностью выполнил рекомендации международной Конвенции и требования Конституции РФ. Может быть он что-то не то ввел в закон? Давайте посмотрим.

Новая редакция Закона о ПДн	Положения международных актов
Ст. 18[1], ч.1 Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:	Для защиты данных личного характера, хранящихся в автоматизированных файлах данных, принимаются надлежащие меры безопасности, направленные на предотвращение их случайного или несанкционированного уничтожения или случайной потери, а так же на предотвращение несанкционированного доступа к ним, их изменения или распространения таких данных. (**ст. 7 Конвенции ETS № 108**)
1) назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;	
2) издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;	Государства-участники могут определить информацию, указываемую в уведомлении…. (f) общее описание, позволяющее произвести предварительную оценку правомерности мер, принятых согласно ст. 17 для обеспечения безопасности обработки (**ст. 19 Директивы ЕС 95/46/ЕС**). Государства-участники обеспечат, что контролер должен будет реализовать надлежащие технические и организационные меры для защиты персональных данных…, обеспечивающие надлежащий уровень безопасности … (**ст. 17 Директивы ЕС 95/46/ЕС**)
3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;	… защита прав и свобод субъектов данных в отношении обработки персональных данных требует, чтобы были приняты надлежащие технические и организационные меры … (**ст. (46) Преамбулы Директивы ЕС 95/46/ЕС**)
4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему	… надзорный орган, либо официальное лицо по обработке данных совместно с этим органом должны проверить такую

[3] Конвенция о защите физических лиц в отношении автоматизированной обработки данных личного характера (ETS # 108)

Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;	обработку до ее осуществления… (**ст. (54) Преамбулы Директивы ЕС 95/46/ЕС**)
5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим Федеральным законом;	… технические о организационные меры должны обеспечить надлежащий уровень безопасности … состояние и стоимость их реализации по отношению к рискам, связанных с обработкой и характером защищаемых данных…(**ст. (46) Преамбулы Директивы ЕС 95/46/ЕС**)
6) ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.	

Получается, что за исключением мелочей типа «назначить ответственного» и «ознакомить сотрудников с порядком защиты» (что объясняется менталитетом россиян), закон предписывает меры, которые соответствуют положениям международных актов и введение их в закон - требование этих самых международных актов. И именно эти акты признают прерогативу государства в определении требований, а не отдают все на откуп оператору.

Кроме того, надо отметить, что закон - это юридический акт, принятый высшим представительным органом государственной власти либо непосредственным волеизъявлением народа (в порядке референдума) и регулирующий, как правило, наиболее важные ОБЩЕСТВЕННЫЕ ОТНОШЕНИЯ. То есть Закон по определению не может содержать никаких технических норм. Он управляет отношениями между людьми.

Об ущербе и его компенсации.

В блогах уже задавался вопрос: «А КАК оценить ущерб?» Я бы задал еще несколько вопросов: «А КТО конкретно причинил ущерб? А почему причинен ущерб, что явилось причиной: кража, утрата, халатность, случайность, или еще что? А КТО выступит экспертом в оценке ущерба?» Можно и еще вопросов поназадавать. В гражданском праве ущерб – это невыгодные для кредитора имущественные последствия, возникшие в результате ПРАВОНАРУШЕНИЯ, допущенного должником. Прежде чем возмещать ущерб, надо определить, какое деяние привело к нему и является ли оно правонарушением. Составов правонарушений может быть много, и в каждом конкретном случае они будут разные, но всегда страдает субъект ПДн. В каждом конкретном случае надо разбираться, искать виновного и взыскивать убытки (подчеркну – убытки[4], а не ущерб, разница существенная). Надо ли все это описывать в Законе «О ПДн»? Наверное, нет. Этому посвящена целая вторая часть УК РФ. Зачем ее повторять и выискивать то, что уже сделано.

Тут надо бы еще учесть, что существует две системы права: публичное и частное. Частное право регулирует имущественные и личные неимущественные отношения между гражданами или коллективами людей (предприятиями, фирмами и пр.). Частные отношения обусловлены тем, что в них (и это важнейший критерий разграничения частных и публичных отношений) преимущественно реализуются ИНДИВИДУАЛЬНЫЕ интересы участников, в данном случае субъектов ПДн. В противовес (а может быть и в дополнение) частному праву, публичное право регулирует отношения, в которых реализуется интерес ОБЩЕСТВА В ЦЕЛОМ. Важнейшим признаком публичных отношений является участие в качестве одной из сторон государства. Так вот, общественные отношения в области защиты интересов субъектов ПДн лежат в плоскости публичного права, так как затрагивают интересы НЕОГРАНИЧЕННОГО круга лиц, а возмещение ущерба (убытков) – в области

[4] Убыток – выраженный в денежной форме ущерб, который причинен одному лицу противоправными действиями другого лица. Под убытками понимают: 1. Расходы, произведенные кредитором. 2. Утрату или повреждение имущества. 3. Доходы, которые он получил бы, если обязательство было бы выполнено должным образом (неполученная прибыль), 4. Расходы на восстановление нарушенных прав. *«Юридический энциклопедический словарь»*, 1997 г.

частного права, так как затрагивают интересы КОНКРЕТНОГО субъекта ПДн. Поэтому Закон «О ПДн» относится к публичному праву, а положения о возмещении ущерба – к частному. Следовательно, и найти свое отражение они должны именно в актах частного права, например, ГК РФ, что, в принципе, и сделано в России. Кстати не только в России.

Посмотрим, а как же с этими вопросами ”там”, у “них” (Эх, нет пророка в своем отечестве …). Как говорит в одной из своих публикаций один из оппонентов – Д. А. Тогер [tigger-66], «”Там”, конечно, тоже люди не безгрешны, но на их стороне большой опыт, большая консолидация и практика применения (в том числе и судебная)». Последуем разумному совету. Для начала, какова ситуация в Испании. Закон Испании[5] предполагает, что «…*субъект ПДн …, которому нанесен материальный ущерб или чьи права ущемлены, имеет право на возмещение нанесенного ущерба. …В случае нанесения ущерба государственными органами – ответственность определяется согласно законодательству, регулирующему порядок ответственности государственных органов. … В случае нанесения ущерба частными лицами – в судебном порядке*». Датчане, в силу особенностей своей судебной системы, поступили еще проще[6]: «*Оператор возмещает любые убытки, вызванные обработкой данных в нарушение положений настоящего закона, если только не будет установлено, что требуемые в связи с обработкой данных осторожность и старательность не могли предотвратить эти убытки*». Аналогично и в Финляндии[7]: «*Ответственность за причиненный ущерб регулируется … Законом о возмещении ущерба (412/1974)*». Этот ряд можно продолжать и дальше, но побережем место. Как видно, государства старушки Европы НЕ ГОВОРЯТ в своих Законах о ПДн как возмещать ущерб, а дают отсылку к действующим в этих странах системам возмещения ущерба, установленных другими законами. А как у нас? «*Лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, … подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков*[8]». А в ГК РФ (ст. 15) как раз и говорится, что «*Лицо, право которого нарушено, может требовать полного возмещения причиненных ему убытков*». И в чем здесь разница с “тамошним” законодательством? И зачем говорить, что «Закон не определяет ответственности за ущерб», когда это не так? Может быть и испанское, датское, финское законодательство тоже не соответствуют Конвенции? Наверное, авторы вряд ли возьмут на себя ответственность за такое заявление. Тогда зачем говорить, что российское законодательство не защищает интересы субъекта и не позволяет получить компенсацию ущерба? Бороться надо не с ветряными мельницами, а развивать судебную практику. Были бы обращения в суды – были бы и решения, накапливалась судебная практика, глядишь, и Верховный Суд обобщил бы ее. Плох не Закон О ПДн, а то, что обращений в суды от субъектов нет. Не верят нашим судам? Вполне возможно. Значит, надо укреплять доверие к судебной системе, разъяснять людям их права, оказывать содействие в решении вопросов компенсации ущерба (примерно так, как это делает Общество защиты прав потребителей, организуя правовую поддержку обиженных покупателей). Вот это будет действенная помощь субъектам ПДн. Но Закон о ПДн здесь ни при чем, он выполнил свою миссию – ввел в правовое поле возможность компенсации ущерба и морального вреда (наверное, для ПДн – это более актуально) от противоправных действий оператора, дальше - дело субъектов ПДн, прокуроров и судов. Ругайте суды, а не Закон о ПДн, это будет честнее и для дела пользы будет больше.

[5] «Органический закон 15/99 от 13 декабря о защите персональных данных» ст. 19 - *Испания*
[6] «Закон об обработке персональных данных» № 429 от 31.05.2000 г., ст. 69 - *Дания*
[7] «Закон о персональных данных» от 22.04.1999, № 523/1999, ст. 47 - *Финляндия*
[8] Закон РФ «О персональных данных», ст. 24

О системе штрафов и коррупции.

То, что любая система штрафов может способствовать коррупции – к сожалению, истинная правда. Но и без штрафов нельзя – если не будет стимула[9], слон дальше не пойдет. Ну, разве что, ему морковку (льготы) дать. Представьте (гипотетически), что после вступления в силу Закона о ПДн в новой редакции, в НК РФ появилась статья, которая говорит о том, что для оператора ПДн, полностью выполнившего требования по защите ПДн, предписанные уполномоченными федеральными органами, и своевременно уведомившего Роскомнадзор об обработке ПДн, ставка социального налога или НДС снижается на 5% (кстати, я такую форму стимулирования предлагал в одной из своих статей)? Думаю, что много-много операторов, не задумываясь над тем, КТО разработал требования по защите и насколько они дороги, поспешило бы их выполнить и сообщить об этом в Роскомнадзор. И, при этом, наверное, они не сетовали бы на то, что «требования невыполнимы». Правда, наверное, экономическая ситуация в стране пока не позволяет Правительству применить такой вид стимулирования, но в любом случае, это также не задача Закона о ПДн, а задача совершенствования налоговой системы России. Вот за это бороться – благородное дело! Да и бремя затрат на защиту ПДн в этом случае частично возьмет на себя государство, что также справедливо. Но этого никто не замечает, проще бороться за то, чтобы ничего не делать, и за это все было.

Но вернемся к штрафам[10]. Штрафы в сфере выполнения требований по обработке (подчеркиваю, не по защите только, а по обработке в целом) ПДн это не «ноу-хау» российских законодателей. Аналогичная система предусмотрена законами Испании, Дании, Финляндии и многих других стран, не буду подробно это описывать. Правда, там никому в голову не придет предложить взятку должностному лицу за неналожение штрафа. Вот и получается, что не норма Закона коррупционноемкая, а люди, которые ее реализуют – коррупционеры. Так и бороться надо не с Законом, а с коррупцией в целом и конкретными коррупционерами в частности! А мы все: «Закон виноват!» Штраф, по своей сути, это санкции за невыполнение принятых (или установленных) обязательств и он никоим образом не связан с компенсацией ущерба. В контексте рассматриваемого закона, защита интересов субъекта ПДн через штрафные санкции состоит в том, что под этим «дамокловым мечем» оператор ВЫНУЖДЕН создавать защиту ПДн. Его обязательства прописаны в законе: принимать необходимые организационные и технические меры защиты. Получается, что эти санкции носят скорее превентивный характер по отношению к факту неправомерных действий с ПДн. Ну, согласитесь, если оператор выполнит требования, предписанные законом (пусть даже, по мнению оппонентов, не современные), то вероятность того, что ПДн подвергнутся противоправным действиям, гораздо меньше, чем если оператор вообще не будет принимать каких-либо мер защиты. Поэтому и наказывают именно за невыполнение мер, а не за причиненный ущерб. Здесь состав правонарушения именно в том, что предписанные законом требования не выполнены. И это совсем не означает, что законодатель ставит исполнение требований превыше всего, наоборот, здесь защита интересов субъекта ПДн, законодатель обязывает (превентивно) оператора исполнять требования, чтобы не было утечек и противоправных действий с ПДн.

О самом главном, о технической защите.

Сначала о несоответствиях, которые отмечали многие блогеры: «…*сейчас "могут" и "обязаны" перемешаны до неприличия (ст. 18прим, 19, 22прим)*…». Конечно, прежде всего приходит на ум эпизод замечательного мультфильма про Простоквашино. Помните, когда Дядя Федор писал письмо родителям, а Кот Матроскин и Шарик его дописывали? В результате получилось, что у Дяди Федора все в порядке, только лапы ломит и хвост от-

[9] Стимул (от лат. stimulus, буквально — остроконечная палка, которой погоняли животных, стрекало), побуждение к действию, побудительная причина поведения. (*БСЭ*)
[10] Штраф (от нем. Strafe — наказание), денежное взыскание, мера материального воздействия, применяемая в случаях и порядке, установленных законом. (*БСЭ*)

валивается, а еще лохматость повысилась. Примерно то же можно сказать и о законе. Жаркие дебаты, разные мнения, сжатые сроки – все смешалось в кучу и, конечно, в такой обстановке возможны огрехи. Но есть ли они? Оппоненты говорят так: «*В 18[1] статье написано, что к мерам "могут относиться" то-то и то-то, а в 19 статье "оператор обязан выполнять меры", что противоречит друг другу и делает обязательным выполнение мер, предложенных регуляторами*». А на самом деле ст. 18[1], часть 1 гласит: «*Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим Федеральным законом или другими федеральными законами. К таким мерам могут, в частности, относиться:… применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона*…». И далее ст. 19 «Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры … для защиты персональных данных …». В чем разница? Да в том, что в ст. 18[1] говорится о мерах для обеспечения выполнения ОБЯЗАННОСТЕЙ ОПЕРАТОРА, а в ст. 19 об организационных и технических мерах ЗАЩИТЫ ПДн, выполнение которых как раз и является обязанностью оператора. Это суть разные вещи! Получается, что оператор может САМОСТОЯТЕЛЬНО определить состав мер, необходимых ему для выполнения обязанностей оператора, используя РЕКОМЕНДОВАННЫЙ (не обязательный и открытый) перечень мер, приведенных в ст. 18[1], но ОБЯЗАТЕЛЬНО должен выполнить меры по защите ПДн в соответствии со ст. 19. Мне возразят: «Ага! Вот и получается, что оператор обязан выполнить ВСЕ требования, которые определит регулятор! Вот! И никакого альтернативного выбора у него нет!» Это не так. Вариативность содержания требований по защите ПДн заложена в том, что они дифференцируются по уровням защищенности ПДн при их обработке в ИСПДн в зависимости от угроз безопасности этих данных (ст. 19, ч. 3). И здесь ключевое слово "угрозы безопасности", которые определяют самостоятельно ведомства (ст. 16. ч. 5). Думаю, что в нормативных документах Правительства, разрабатываемых по этому закону, будет заложена необходимость разработки частных моделей угроз для конкретных объектов, которая и позволит актуализировать угрозы, исключить (через доказательство) неактуальные и определить оптимальный набор требований (в принципе, это логика, заложенная еще в ГОСТ/ИСО 15408: угрозы есть, но меры по их устранению можно и не применять, если доказано, что на данном конкретном объекте эта угроза не актуальна).

Действительно, новая редакция закона предполагает, что уровни защиты ИСПДн "навязываются" оператору Правительством, а состав требований – регуляторами. И этот факт использовался авторами письма как доказательство несоответствия Конвенции. Но, возвращаясь к анализу аналогичных законов европейских стран, мы можем увидеть, что, например, в Дании меры безопасности (технические и организационные) устанавливает Министр юстиции[11], а Агентство по защите данных (государственный орган) может запретить оператору использовать определенную технологию обработки ПДн, если считает, что эта технология небезопасна[12] или даже отдать приказ оператору выполнить специальные технические и организационные меры защиты ПДн[13]. В Финляндии Совет по защите данных (опять же государственный орган), выдавая разрешение на обработку ПДн, определяет правила, необходимые для защиты ПДн[14]. Так же и в Швеции, где надзирающий орган имеет право обязать оператора принять конкретные меры безопасности ПДн[15]. Просмотреть все 43 закона разных стран у меня просто нет возможности. Но, думаю, что во многих из них можно найти аналогичные положения. И что же, все эти страны тоже не

[11] «Закон об обработке персональных данных» № 429 от 31.05.2000 г., ст. 41, п.(5) - Дания
[12] «Закон об обработке персональных данных» № 429 от 31.05.2000 г., ст. 59 п.(2) - Дания
[13] «Закон об обработке персональных данных» № 429 от 31.05.2000 г., ст. 59 п.(3) - Дания
[14] «Закон о персональных данных» от 22.04.1999, № 523/1999, ст. 43 п.(3) - Финляндия
[15] «Закон о защите персональных данных» (1998:204), ст. 34 - Швеция

придерживаются рекомендаций Конвенции и наглым образом ее попирают? Думаю, что это не так. Правда, ради объективности надо сказать, что, например, в Испании правила организации обработки ПДн, нормы безопасности, программы и оборудование для безопасности прописываются в типовых кодексах, которые разрабатывают операторы, но такие кодексы должны пройти экспертизу в Агентстве по защите персональных данных и зарегистрироваться в Генеральном реестре по защите персональных данных, а Агентство, в свою очередь, может потребовать внесения изменений, если посчитает, что законные требования не выполняются[16]. Так, что мы не одиноки во Вселенной: установление для операторов ПДн требований на уровне государственных органов – это сложившаяся международная практика.

Поэтому и бороться надо не за отмену закона, а за правильное содержание (с точки зрения бизнес-сообщества и субъектов ПДн) тех подзаконных актов, которые должны быть выпущены во исполнение этого закона. А с учетом того, что Дмитрий Медведев подписал Указ, который обеспечивает участие бизнеса в экспертизе ведомственных нормативных актов с целью выявления в них положений, затрудняющих инвестиционную и предпринимательскую деятельность - это не какая-то маниловщина, а вполне реальное дело, тем более, что и сами регуляторы это понимают. Здесь я хотел бы процитировать Ю. В. Травкина: «… *руководство ФСТЭК, насколько мне известно, и что было неоднократно подчеркнуто - мало того, что разделяет "рекомендательность" [закона], но отстаивало ее. Заодно и взгляд на саму структуру и цель "подзаконных" [актов]*[17]».

О дороговизне защиты.

Кто-то правильно сказал, что тезис о дороговизне, выдвинутый ранее и много раз повторенный, теперь стал как бы аксиомой, которую никто не проверял. Я много раз выступал и говорил, что это не так, что если считать, как А. Лукацкий «в лоб», то, действительно, можно выйти на 6% ВВП. Здесь я не хотел бы долго останавливаться и только процитирую высказывание М. Ю. Емельянникова (кстати, присоединившегося к “письму пяти”, и которого я считаю одним из грамотнейших экспертов в области защиты информации) в одной из последних его статей: «…. рекомендации органа власти (Рособразования, хотя и упраздненного) и имеющиеся на рынке сертифицированные ИБ-продукты дают возможность решить ее [задачу защиты ПДн] с разумными затратами, не прибегая к излишним дорогостоящим и сложным мерам[18]».

И в заключение.

Пока читал, анализировал, думал, осознавал, писал – произошли серьезные события. 26.07.2011 г. Президент РФ подписал закон о внесении изменений в Закон о ПДн. Казалось бы, зачем теперь ломать копья. Ан, нет, критика закона еще будет (может быть, это и правильно – пределу совершенства нет, только бы она не перешла в разряд критиканства). Но, на мой взгляд, сейчас надо сосредоточиться именно на корректности подзаконных актов, которые будут выпущены во исполнение этого закона. И именно поэтому, аргументация, приведенная мною здесь, может помочь направить усилия в нужном русле и не бороться с ветряными мельницами.

С. Вихорев

[16] «Органический закон 15/99 от 13 декабря о защите персональных данных» ст. 32 - Испания
[17] Блог Ю. В. Травкина, 11.07.2011, http://travkin333.livejournal.com/28117.html
[18] «Персональные данные в образовательных учреждениях: сложно, но возможно!», PCWEEK, М. Емельянников, 22.07.2011 http://www.pcweek.ru/security/article/detail.php?ID=132703