Осторожно: законофобия!

Эссе на тему Закона «О персональных данных»

Сергей Вихорев
Заместитель генерального директора по развитию
ОАО «ЭЛВИС-ПЛЮС»

Мы не мыши, мы не птахи,
Мы ночные ахи-страхи!
Мы летаем, кружимся,
Нагоняем ужасы, ужасы...
Песенка из мультфильма «Ничуть не страшно»

Вместо предисловия

По определению фобия — это «навязчивые неадекватные переживания страхов конкретного содержания, иррациональный страх перед определенной ситуацией, необоснованно охватывающий субъекта». «Ну что? — скажет читатель, — а закон здесь при чем?» А при том, дорогой читатель, что отмечаемый последнее время ажиотаж вокруг Закона «О персональных данных» носит, прямо сказать, панический характер. Развивается фобия Закона, вернее, фобия вероятных репрессивных мер за опоздание с реализацией его требований. Чем ближе срок, установленный Законом, тем страхи сильнее. В чем же корень зла? В чем причины страхов и насколько они обоснованы? Будем разбираться...

Сначала о самом Законе

Проблеме защиты персональных данных уже больше 10 лет. Необходимость принятия этого Закона диктовалась необходимостью исполнения Российской Федерацией положений международных договоров и общепринятых международных норм и принципов при сборе и использовании персональных данных, создания гарантий и правовых механизмов защиты прав на личную тайну и неприкосновенность частной жизни. На взгляд автора, Закон «О персональных данных» — один из немногих законов, который выстраивает четкую логическую цепочку: кто устанавливает требования по защите, кто обязан их исполнять и кто несет за это ответственность. Более того, Закон создает *специальный федеральный орган*, своеобразную прокуратуру по вопросам обработки персональных данных, которая надзирает за всем этим безобразием. (Вот где одна из причин фобии!) И как ни странно, Закон, пусть и с задержкой, заработал. Теперь все заговорили о персональных данных, о необходимости их защиты и вообще о защите информации. Ни один закон, касающийся защиты информации (а их уже немало), не имел такого резонанса. А этот действительно привлек внимание широкой общественности к проблеме информационной безопасности, ведь он касается всех, и об этом заговорили все. Но заговорили по-разному — аудитория-то неоднородная! Тутто и выявилось расслоение.

Обыватели и профессионалы

Тех, кого касается Закон, а касается он буквально всех, так как все мы являемся в терминах Закона «субъектами персональных данных», условно можно разделить на две категории: обыватели и профессионалы. Обыватели — это те, кто работал с персональными данными, но никогда не занимался проблемой защиты информации на практике и волею судеб (читай: закона) вдруг оказался субъектом, под закон подпадающим. Профессионалы — это те, кто искушен в защите информации, знает, насколько это сложно и дорого, сколько требует сил и внимания. Обывателей, естественно, больше, чем профессионалов и, что тоже естественно, обыватели прислушиваются к мнению профессионалов. И что же думает профессионал, впервые знакомясь с Законом (а Закон, надо напомнить, вступил в силу аж в 2007 г.)? «О, — думает он, еще не полностью разобравшись в сути, — нас опять хотят загнать в угол! Придумали какие-то новые требования, а нам их выполнять! Что же мне из-за этого всю систему защиты перестраивать? Это время, усилия, деньги!» А дальше его рассуждения сводятся к тому, что: «Ладно, толкач муку покажет! На дворе только 2007 г., а привести в соответствие Закону информационную систему надо только к 2010-му. Да и жесткость наших законов компенсируется необязательностью их исполнения... Может и здесь пронесет — ничего пока делать не буду!» Ан нет, не Америка, а остров Буян, будь он окаян. Не пронесло.

Нежданно-негаданно — как снег в России зимой — оказалось, что заветная дата на носу, ничего не сделано, а надзорные органы шлют предписания! Что должен сделать настоящий профессионал в этой ситуации? Правильно! Приложить максимум усилий, чтобы либо срок затянуть, либо требования устранить. Но это же федеральный закон!.. И начиная где-то с первой половины 2009 г. (время подходящее, можно на кризис списать — деньги-то кончились) нагнетается особое общественное мнение: положения Закона — неверные, требования по технической защите — завышены, если все делать по Закону — дорого, чтобы выполнить все требования — сто лет потребуется, да еще и не учтен баланс интересов бизнеса и личности. Одновременно в Интернете широкому кругу представляется целый ряд интересных справок и аналитических материалов типа «О применимости руководящих документов по технической защите персональных данных и их несоответствии существующей стадии развития ИТ», «О требованиях к технической защите персональных данных в европейских странах» и проч. Сами по себе эти материалы хорошие, правильные, но фактура, которая там приведена... И все это обсуждается на различных форумах, в ассоциациях, в кулуарах. Поднимается волна ажиотажной критики технических требований по защите персональных данных, эта волна ширится, растет, набирает мощь и захлестывает обывателя. Тот, естественно, прислушивается к мнению профессионалов и начинает все сильнее пугаться (так как правильность этого мнения принимает на веру) и добавляет в общий хор свой голос: «Согласен! Действительно...».

Именно в это время отмечаются первые признаки эпидемии законофобии. И вот могучий утес — парламентские слушания. Волна разбивается, откатывается, сроки приведения информационных систем в соответствие с требованиями благополучно переносятся, но волна оставляет наносы, где имеются и большие камни. Я бы выделил три такие основные глыбы: дороговизна защиты и большие сроки ее реализации, жесткость и неприемлемость требований, несбалансированность интересов бизнеса и личности. Именно эти мрачные валуны и остаются базой законофобии. Посмотрим, насколько они ужасны.

Дороговизна защиты и большие сроки ее реализации

Часто можно слышать, что выполнение защиты в полном соответствии с требованиями Закона и нормативными документами — это, мол, очень дорого. Операторы не могут позволить себе такие средства, а бюджетники и подавно, ведь в бюджет под это ни одной копейки не заложили. Делаются жуткие расчеты, что для выполнения всех требований по всей стране у всех операторов потребуется бюджет, сопоставимый с совокупным бюджетом всей Европы и США в придачу. Может, конечно, и так, если не задумываться. Но это же неверный ход! К примеру, по оценкам конца 2008 г. число пользователей службы «Вконтакте» составило более 14 млн человек, а «Одноклассники» — 8 млн. И на этом основании делается вывод: раз при регистрации участники предоставляют свои персональные данные (фамилию, имя, отчество, пол, место проживания, дату рождения, фото), то такая система содержит персональные данные, которые позволяют идентифицировать субъекта и получить о

нем дополнительную информацию. Эта система будет иметь наивысший класс К1, и выполнение требований по защите потребует максимальных затрат. А еще надо получить лицензию на защиту информации и пройти аттестацию. И на все про все потребуется от полугода до полутора лет. Если же учесть необходимость сертификации обновлений самого программного продукта, которые проходят достаточно часто, то к изначальному сроку потребуется прибавить еще с полгодика. Значит, надо два года и кучу денег. Так ли это на самом деле? Давайте обратимся к первоисточнику.

Объем субъектов персональных данных — это не единственный критерий, по которому в соответствии с Приказом трех[1] проводится классификация информационных систем. Есть еще и категория информации, а также шесть дополнительных признаков. Итак, *объем* субъектов в упомянутых информационных системах действительно велик, но вот *категория* информации оценена в этом случае неверно. Фамилия, имя, отчество, пол, место проживания, дата рождения являются, конечно, сведениями, позволяющими идентифицировать субъекта, но субъект, размещая эту информацию добровольно на открытом портале, тем самым сам дал согласие на неограниченный доступ к ним других субъектов. А что это как не общедоступные персональные данные (см. п. 12 ст. 3 Закона)? Далее, размещать или не размещать свою фотографию, которая уже является дополнительной по отношению к идентификационной информации, — это воля и желание самого субъекта, т. е. он сам опять переводит такую информацию в категорию общедоступной (а может и не размещать, если чего-то опасается). Отсюда следует, что в данном случае мы имеем многопользовательскую информационную систему, которая обрабатывает большое (более 100 тыс. субъектов) количество персональных данных 4-й категории (п. 6 Приказа трех). Следовательно, логический вывод: согласно п. 15 Приказа трех такая система должна быть отнесена к классу К4(!), т. е. к информационной системе, для которой нарушение заданной характеристики безопасности не приводит к негативным последствиям для субъектов персональных данных (п. 14 Приказа трех). Все, точка. Особых мер защиты применять не надо, аттестовывать не обязательно, и это не дорого, и времени не занимает, и это можно было сделать в прежние сроки, установленные законом. А все, что сказано выше о классе К1, — это маниакальный бред. Может ли во всем этом без помощи разобраться обыватель? Вот он и пугается, а фобия развивается.

Кстати о сертификации систем, ведь для некоторых систем все-таки не удастся так сразу снизить класс и все-таки придется строить защиту. Здесь вопрос цены сертификата становится немаловажным. Смотрим п. 5 Положения об обеспечении безопасности персональных данных в ИС[2]. Там говорится о том, что процедуру оценки (то бишь сертификации в том числе) проходят *средства защиты*, а не *информационные системы*. О самих системах там ни слова. Это, конечно, нюансы, но именно они придают вкус блюду.

Несколько слов о дороговизне защиты. Бесспорно, защита стоит денег, и подчас немалых. Но многие компании и государственные органы уже давно защищают свои интересы (коммерческие, профессиональные, ноу-хау), строят систему защиты и вкладывают в нее деньги. По данным CNews, совокупная выручка компаний, предлагающих услуги в области ИБ, по сравнению с 2004 г. выросла на 67,5% и продолжает расти. Рынок ИБ показывает устойчивую тенденцию роста даже в условиях кризиса, и рост к концу 2009 г. ожидался на 20—25%[3]. Проведенные опросы показывают, что до половины компаний из разных отраслей в той или иной мере занимаются защитой даже в условиях кризиса[4]. Значит, можно сказать, что в половине организаций защита уже имеется. А «чистых» информационных систем, которые обрабатывают только персональные данные, — нет. Так почему уже существующую систему защиты нельзя применить для персональных данных? Все, кто раньше защищал свою информацию по классу 1Г (а, по оценкам автора, таких большинство), уже практически готовы к защите персональных данных, требуется только привести в соответствие необходимую документацию и, может быть, что-то докрутить в самой системе. Так что денежки-то уже потрачены, система-то уже есть! Вот где кладезь будущей экономии средств!

Обратите внимание, что снижения стоимости защиты и сроков ее реализации автор добился просто путем внимательного прочтения и применения статей нормативных документов вместо того, чтобы ломиться в открытую дверь. Из практического опыта защиты информационных систем я знаю, что внимательная работа с документами дает потрясающий эффект в плане правильного определения категории персональных данных и класса информационной системы. Можно разобрать любой случай и целое пособие написать, как правильно читать и применять документы и требования, в них изложенные, однако время и избранная форма изложения этого не позволяют сделать. Но, поверьте, и денег надо гораздо меньше, чем кажется на первый взгляд, и сроки реализации вполне приемлемые. Правда, если не откладывать все на самый последний момент, ожидая прибытия нашего любимого жареного петуха. Теперь пойдем дальше.

Жесткость и неприемлемость требований

Очень веский аргумент, если он справедлив. Надо сказать, в основном критика касается требований, предъявляемых к системам класса К1. Высказывания резкие: требования по использованию сертифицированных средств защиты информации являются практически невыполнимыми, зачем криптографию применять, зачем применять дорогую защиту от побочных электромагнитных излуче-

[1] Приказ ФСТЭК России, ФСБ России, Минсвязи России от 13.02.2008 № 55/86/20.

[2] Утверждено постановлением Правительства РФ от 17.10.2007 № 781.

[3] http://www.cnews.ru/reviews/free/security2009/rating/rating.shtml.

[4] Security Lab. Исследование «Тенденции ИБ в условиях кризиса» (М., 2009).

ний и наводок (ПЭМИН), зачем использовать оборудование в специальном защищенном исполнении? Вообще у нас в Законе все плохо и неправильно! Другое дело — в благословенной Европе! Там все ясно и понятно: бери стандарт 27001 или BS 17799 и все! А еще лучше, если выбор требований по защите будет делать сам оператор или, к примеру, разработчик информационной системы.

Начну с конца. Если требования будет выбирать оператор или разработчик системы, никакой защиты не будет! Почему? А почему у нас в супермаркетах дату на просроченных товарах перебивают или бензин непонятно чем бодяжат? И стандарты есть, и технические регламенты, и торговая инспекция есть, а порядка — нет. Потому что интересы разные. Не думаю, что отечественный бизнес будет блюсти интересы субъекта в ущерб своим личным. А защита, как мы уже выяснили, дело хлопотное и, главное, затратное! Ну, это я слегка вперед забежал, об этом речь пойдет дальше. Кстати, обращаю внимание и на то, что в документах ФСТЭК и ФСБ по защите персональных данных уже заложена возможность корректировки требований соответственно актуальности угроз — переход к специальным системам, которые практически защищаются по идеологии стандарта ГОСТ ИСО/МЭК 15408. Другими словами, если вы уверены, что вам ничего не угрожает, то и защищать ничего не надо. Но надо все тщательно описать и обосновать, что и как.

Теперь скажите, уважаемые, а кто-нибудь делал защиту своей системы по стандарту ISO 27001? Нет? А жаль... Могу сообщить, что выполнить требования по защите в соответствии с этим стандартом — дорогого стоит (в прямом смысле!). Вернее, не требования по защите (они-то изложены в другом стандарте — ISO 15408 и на самом деле жесткие), а требования по управлению безопасностью (о чем и говорит стандарт), которые нельзя выполнить без выполнения требований по защите. И еще после этого надо пройти процедуру сертификации на выполнение этих требований! Посмотрите стандарт, не ленитесь, там ведь о-ч-ч-чень жесткие требования и по управлению безопасностью, и по защите каналов и по разграничению доступа. Одно только небольшое требование: «целостность информации, доступной в сетях общего пользования, должна быть защищена в целях предотвращения ее несанкционированной модификации» (п. А.10.9.3 Приложения А стандарта) или другое: «Информация, участвующая в электронной коммерции и проходящая по сетям общего пользования, должна быть защищена от мошенничества, нарушений контракта и несанкционированного раскрытия и модификации» (п. А.10.9.13 Приложения А стандарта) сразу же выводит на необходимость повсеместного применения средств криптографии (если кто-то научит меня делать это без средств криптографии, буду очень благодарен). Я уже не говорю о системе разграничения доступа и управлении безопасностью. И обратите внимание: делайте защиту ты сам, а потом докажи экспертам в ходе сертификации, что ты все сделал правильно. И чем это от-

личается от наших требований по сертификации и аттестации информационных систем?

Можно еще сказать, что даже в старом «трехглавом» законе[5] говорилось (ст. 19): «Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в порядке, установленном Законом Российской Федерации...». И еще: «Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств». Так что такая норма существовала уже с 1995 г., а кто ее не выполнял, тот брал все риски на себя и отвечал за все последствия сам и по полной программе. Получается, что новое — это просто хорошо забытое старое.

Несколько слов о защите от ПЭМИН и оборудовании в защищенном исполнении. Действительно, требование достаточно жесткое и дорогое в исполнении (хотя, как посмотреть: можно и одним генератором шума обойтись, решив все проблемы). Но! Это требование необходимо выполнять только для систем класса К1. А как мы уже видели, если правильно и грамотно провести категорирование системы, то класс К1 не всегда вырисовывается. Вообще-то я слышал оценочную цифру наших регуляторов, что систем класса К1 будет не более 10—15% от всех систем. Это не так уж и много. А если учесть, что такие системы, в принципе, обрабатывают в основном информацию о расовой принадлежности, политических взглядах, религиозных убеждениях, состоянии здоровья и интимной жизни и в редких случаях в этот класс попадают системы, позволяющие получить дополнительную к идентификационной информацию о большом количестве субъектов, то согласитесь, такие системы сам Бог велел защищать как зеницу ока. И денег на их защиту не жалко. Кстати, автору могут возразить: а, например, во всех больничках обрабатывают информацию о состоянии здоровья, значит это класс К1, а где им брать деньги? Ну, если там действительно есть необходимость персонифицировать состояние здоровья по отношению к субъекту, то да, надо выполнять жесткие требования. Но имеющаяся практика показывает, что в таких системах вполне можно применить методы обезличивания информации и отделения действительно медицинской информации от общедоступной. На лечебный процесс это особо не влияет, зато снижает категорию обрабатываемой информации и, следовательно, всей информационной системы до класса К3, а это уже совсем другая песня. Кстати, это не выдумка автора, это то, что предполагает ГОСТ 52636-2006 «Электронная история болезни».

Еще один серьезный аргумент «против»: требования вышли поздно, времени на их реализацию нет. Действительно, ФСТЭК России выпустило свое «четырехкнижье» только в феврале 2008 г. Но закон-то вступил в силу еще в 2007 г., а требование к защите персональных данных вообще существует с 1995 г. и успешно некоторыми выполнялось на основе имеющихся Руководящих документов ФСТЭК России. Более того, защищая свои интересы и секреты, многие компании уже давно имеют защищенные информационные системы по классам 1Г—1В (по версии Руководящих документов ФСТЭК России), чего вполне достаточно для защиты и персональных данных класса К3—К2. Получается, что требования не такие уж и жесткие, они были и раньше и успешно применялись для защиты коммерческой информации. Почему же тогда эти требования были не жесткие, а сейчас вдруг!...

Опять слышу возражения: но ведь законодатель признал, что требования жесткие! Например, в последней редакции Закона от декабря 2009 г. из ст. 19 исключена фраза «...в том числе использовать шифровальные (криптографические) средства...», следовательно, криптографию применять не надо! Дудки! В Законе осталось: «Оператор... обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа...» А криптография и есть те самые технические меры, просто убрали уточняющее предложение, вот и все. Тем более что в некоторых случаях, например при передаче информации по открытым каналам, без криптографии просто не обойтись.

Несбалансированность интересов бизнеса и личности

Говоря о сбалансированности интересов, давайте вспомним, что мы не только бизнесмены и чиновники, но еще и люди. И именно наши интересы как субъектов персональных данных защищает Закон. Для нас наши персональные данные ценны настолько, насколько мы сами их ценим. И обрабатывая персональные данные, всегда следует относиться к ним как к своим личным персональным данным. Представьте себе ситуацию. В банк пришла бабушка и принесла тысячу рублей, чтобы положить в банковскую ячейку. А ей говорят: «Э, бабка, да что там тысяча рублей! Вот тебе консервная жестяная банка, клади туда... А ячейку мы дадим тому, кто принесет миллион рублей». С точки зрения бизнеса все правильно, но с точки зрения бабули — нет: для нее и эта тысяча — состояние, и она хочет и имеет право требовать такой же защиты, как и для миллиона рублей. Вот и весь баланс. Здесь вопрос надо ставить так: все ценности (читай: персональные данные) должны быть защищены, если есть деньги (не важно сколько), то они должны быть защищены с одной степенью, а если есть бриллианты (тоже не важно сколько) — с другой. А чтобы не было разноголосицы, государство берет патронат над выработкой требований. Кстати, такой подход никак не противоречит международным требованиям. Напомню п. 46 преамбулы Директивы Европарламента и Совета Европы 95/46/ЕС[6]: «...защита прав и свобод

[5] Федеральный закон от 25.01.1995 № 24-ФЗ «Об информации, информатизации и защите информации» (утратил силу).

[6] Директива Европейского парламента и Совета Европы от 24.10.1995 № 95/46/ЕС «О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных».

субъектов данных в отношении обработки персональных данных требует, чтобы были приняты надлежащие технические и организационные меры, как при разработке системы, так и в процессе самой обработки, в частности для поддержания безопасности и предотвращения любой несанкционированной обработки... государства-участники обязаны обеспечить, чтобы операторы соблюдали эти меры, а меры должны обеспечить надлежащий уровень безопасности...». И во многих странах созданы специальные бюро по защите данных (Data Protection Agency, DPA), которые разрабатывают требования и рекомендации по защите.

А кто может лучше специалистов сказать, какие требования надо применять? Вы же, когда у вас болит зуб, идете к врачу, а не в магазин к продавцу. Врач-то это сделает лучше, потому что знает, как это делать, или хотя бы знаком с анатомией. Так и здесь: Правительство РФ определило тех специалистов, которые знают, как это сделать лучше, или по крайней мере знают, как найти угрозы, которые могут привести к нехорошим последствиям при обработке информации. Давайте доверять профессионалам! Ведь правительство выбрало для этих целей федеральные органы, которые уже много-много лет работают на этом поприще.

Конечно же, баланс надо соблюдать и риски надо учитывать. Но он должен выражаться в том, что техническая защита персональных данных должна не мешать (или по крайней мере минимально мешать) бизнесу и обеспечивать надежную защиту самих данных. Однако кое-кто под маркой соблюдения баланса пытается свести техническую защиту к декларации типа «у нас все хорошо». Если требования по технической защите персональных данных, которые раскрыты в документах ФСТЭК и ФСБ, выполнены — данные защищены. Это надо считать аксиомой. Трудно выполнить? Дорого? В некоторых случаях — соглашусь. Но не думаю, что это сильно повлияет на те бизнес-процессы, которые реализуются операторами, а следовательно, не сильно повлияет на бизнес. А вот невыполнение требований, боюсь, может сильно сказаться на бизнесе, если в защиту выступят контрольные органы. Так что некий баланс здесь выдержан...

Маленький эпилог

В первой декаде декабря 2009 г. Государственная Дума приняла Закон «О внесении изменений в статьи 19 и 25 Федерального закона “О персональных данных”». Согласно этому Закону срок приведения информационных систем, которые обрабатывают персональные данные и созданы до 1 января 2010 г., в соответствие с требованиями Закона «О персональных данных» продлен до 1 января 2011 г. Идя навстречу пожеланиям трудящихся, дали передышку на год. Ура! Так давайте не ждать того самого русского жареного петуха, а используем это время с пользой для защиты персональных данных. Цели ясны, задачи определены. За работу, товарищи! (Или господа...)