

Закон избирательного применения

За несколько дней до того, как была написана эта статья, электронная почта принесла мне очередное предложение — купить базу данных «Таможня — 2009 год», которая, как пишет отправитель, содержит «полные и подробные данные по сделкам компаний, предприятий и индивидуальных предпринимателей (экспорт и импорт)», а также «полную и подробную информацию о покупателе, поставщике, количестве, стоимости товара, дате сделки» и т. д.

текст:
Юрий Курочкин

З а все про все просят 4500 руб., обещают ежемесячные обновления базы и дают телефон для связи (адрес отправителя в сообщении наверняка подложный): 8-916-069-60-50. Доставка курьером, покупателю — подарок: ручка с исчезающими чернилами.

Если это предложение не фикция, то предприниматели, доверившие информацию о себе государству, в очередной раз оказались «голыми среди волков»: сведения о том, каковы масштабы и характер их бизнеса вместе с адресами и прочими данными, может не за дорого приобрести любой злоумышленник, а уж как он эти сведения использует — одному богу известно.

ПОКА ЖАРЕНый ПЕТУХ НЕ КЛЮНЕТ...

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152 «О персональных данных» вступил в силу без малого три года назад, 27 января 2007 г. Спустя почти 10 месяцев, 29 ноября 2007 г., вышло и вступило в силу постановление Правительства Российской Федерации № 781 г. «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», возложившее обязанность устанавливать методы и способы защиты информации в информационных системах на Федеральную службу по техническому и экспортному контролю (ФСТЭК) и Федеральную службу безопасности (ФСБ) Российской Федерации. Тем же постановлением ФСБ и ФСТЭК предписывалось в трехмесячный срок утвердить нормативные правовые акты и методические документы, необходимые для выполнения требований, предусмотренных Положением. Эти документы были утверждены в феврале 2008 г. (правда, с грифом «Для служебного пользования»), после чего продолжали выходить разъяснения, приказы и другие документы, касающиеся выполнения закона №152-ФЗ.



Согласно закону, все организации, начинающие после 27 января 2007 г. работать с персональными данными граждан (за некоторыми исключениями, перечисленными в законе), должны были об этом «уведомить уполномоченный ор-

Неторопливость регуляторов, по-видимому, породила в компаниях, работающих с персональными данными, иллюзию о необязательности выполнения закона, столь характерную для российского менталитета

ган по защите прав субъектов персональных данных» и зарегистрироваться в реестре операторов, а также обеспечить выполнение всех требований закона. Операторы информационных систем, уже работавших с персональными данными на момент вступления закона в силу, должны были направить уведомление об этом не позже 1 января 2008 г. (статья 25.4). Очевидно, что сделать этого они не могли ввиду отсутствия соответствующих подзаконных актов: даже образец уведомления об обработке персональных данных был утвержден приказом Федеральной службы по надзору в сфере связи и массовых коммуникаций лишь в июле 2008 г.

Неторопливость регуляторов, по-видимому, породила в компаниях, работающих с персональными данными, иллюзию о необязательности выполнения закона, столь характерную для российского менталитета. Задумываться о проведении необходимых мероприятий многие начали лишь в нынешнем году, преимущественно во второй его половине, за считанные месяцы до 1 января 2010 г. — даты, когда организации, имевшие информационные системы для обработки ПДн еще до января 2007 г., должны были привести их в соответствие с требованиями закона.

ЦЕНА ВОПРОСА

Функции уполномоченного органа по защите прав субъектов персональных данных выполняет в настоящее время Федеральная служба по надзору в сфере связи, информационных технологий и массовых

коммуникаций (РОСКОМНАДЗОР), в которой создано Управление по защите прав субъектов персональных данных. На его портале <http://pd.rsoc.ru> среди разнообразной информации, относящейся к реализации ФЗ №152, представлены данные о количестве операторов персональ-

ных данных, занесенных в реестр. На 9 ноября их было 68 906. Если учесть, что общее количество операторов персональных данных в нашей стране, по разным оценкам, составляет от одного до семи миллионов, то это — капля в море. На что надеются остальные?

Надеются, и не безосновательно, на то, что сроки ввода закона в действие будут перенесены. Хотя бы потому, что обеспечение безопасности информации стоит немалых денег. Закон «О персональных данных» разрабатывался и принимался в относительно безоблачные годы, когда бизнес ИТ-компаний рос быстрыми темпами и никаких признаков экономического кризиса не было на горизонте. Сегодня эксперты посчитали расходы — и задумались. По их оценкам, для того чтобы привести в соответствие с требованиями закона одно рабочее место по 1 (высшей) категории защиты, нужно потратить около 70 тыс. рублей. Если взять эту цифру за основу, то на

ЗАКОН «О ПЕРСОНАЛЬНЫХ ДАННЫХ» РАЗРАБАТЫВАЛСЯ И ПРИНИМАЛСЯ В ОТНОСИТЕЛЬНО БЕЗОБЛАЧНЫЕ ГОДЫ, КОГДА БИЗНЕС ИТ-КОМПАНИЙ РОС БЫСТРЫМИ ТЕМПАМИ И НИКАКИХ ПРИЗНАКОВ ЭКОНОМИЧЕСКОГО КРИЗИСА НЕ БЫЛО НА ГОРИЗОНТЕ

КОММЕНТАРИЙ



Михаил Емельяников,
автор и преподаватель учебных курсов Учебного центра «Информзащита», директор по развитию бизнеса компании «Информзащита»:

По разным оценкам, прозвучавшим на парламентских слушаниях 20 октября, количество одних только законов, в которые необходимо внести изменения в связи с ФЗ «О персональных данных», составляет от 30 до 80. По общему мнению законодателей, лоббистов и профессионального сообщества, требования к технической защите избыточно жесткие и слишком детализированные. Но их изменение требует не просто корректировки документов, а пересмотра самого подхода к защите персональных данных, что вряд ли возможно в ближайшее время. Жесткость требований создает у всех без исключения операторов ПДн сложности в их реализации, как с финансовой, так и с технической точки зрения, при этом, к сожалению, на первый план выходит выполнение формальных условий, а не реальная защищенность информационных систем. В то же время сама обязательность требований об использовании только сертифицированных средств защиты информации, в том числе и прошедших проверку на отсутствие недеklarированных возможностей (НДВ), вызывает сомнения. Многие средства защиты не имеют отечественных аналогов, а сертификация по НДВ требует раскрытия исходных кодов, на что западные вендоры идут крайне неохотно. Складывается парадоксальная ситуация, когда нельзя применять общепризнанные продукты мировых лидеров, а это приводит в конечном итоге к ослаблению системы защиты.

модернизацию даже ста тысяч рабочих мест потребуется около 7 млрд рублей — цифра более чем внушительная, в послекризисный период практически нереальная. Вспомним о том, что с персональными данными работают немало компаний среднего и даже малого бизнеса, которые очень стеснены в средствах. Добавим к этому необходимость отвлечения сотрудников компаний от основной работы и обращения к услугам специализированных организаций, количество которых ограничено. Вспомним и о том, что на многочисленных в последнее время обсуждениях проблемы защиты ПДн указывалось на множество противоречий в сформированной правовой базе, высказывалось немало претензий и к закону, и к подзаконным актам, — и станет понятен масштаб трудностей, с которыми пришлось столкнуться всем, кто имеет отно-

шение к этой проблеме. Немудрено, что многие компании среднего бизнеса, работающие с персональными данными, занимают выжидательную позицию. Некоторую растерянность испытывают даже крупные разработчики информационных систем, знакомые с проблемой во всей ее

это очень щекотливая тема, и что бы я ни сказал, это будет мне не в плюс».

ЗАИНТЕРЕСОВАННЫЕ ЛИЦА

Предложения о переносе сроков ввода закона в действие до сих пор наталкивались на твердую позицию

ВЕДУЩИЕ СИСТЕМНЫЕ ИНТЕГРАТОРЫ, РАБОТАЮЩИЕ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ГОВОРЯТ, ЧТО СПРОС НА РЕШЕНИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРЕВЫШАЕТ ПРЕДЛОЖЕНИЕ

глубине. Попросив комментарий у одного из руководителей фирмы, разрабатывающей банковское программное обеспечение, я услышал отказ: «На сегодняшний день

регуляторов, считающих, что у операторов было достаточно времени, чтобы привести свои информационные системы в соответствии с законом. Однако больше всего в соблюдении установленных сроков и требований заинтересованы, пожалуй, отечественные поставщики технических и программных средств обеспечения информационной безопасности. Этот сектор инфокоммуникационного рынка сегодня переживает своеобразный бум: ведущие системные интеграторы, работающие в сфере информационной безопасности, говорят, что спрос на решения по защите персональных данных превышает предложение. По словам генерального директора LETA IT-company Андрея Конусова, обороты его компании, в первом полугодии сократившиеся на 30% по сравнению с тем же периодом прошлого года, по итогам трех кварталов 2009 г. на 15% превысили прошлогодние показатели — и все благодаря проблеме охраны ПДн. Лидеров отрасли беспокоит лишь то, что на рынке уже появляются компании, которые предлагают операторам персональных данных за относительно небольшую цену произвести «косметический ремонт» их информационных систем: это позволит если не удовлетворить полностью требования надзорных инстанций, то хотя бы продемон-

КОММЕНТАРИЙ



Алексей Сабанов,
заместитель генерального директора компании Aladdin:

Процессы по обеспечению защиты персональных данных идут: работают и регуляторы, и операторы, и представители рынка системной интеграции, и поставщики СЗИ и СКЗИ. Закон заставил многих задуматься об информационной безопасности: операторы поняли, что защищать персональные данные действительно надо, иначе последуют санкции, регуляторы смогли оценить реальное положение дел в стране в части защиты информации такой категории. Единственные, кто по-прежнему остается достаточно далеким от реалий, связанных с персональными данными граждан, — это, как ни парадоксально, сами граждане. Когда гражданин должен предъявлять паспортные данные? Каковы гарантии, что они защищены от неразглашения и случайной утечки? Что касается защищенности прав гражданина и социальных гарантий со стороны государства, тут по-прежнему больше вопросов, чем ответов. Обратная ситуация: если гражданин сообщил в РОСКОНАДЗОР о нарушении требований защиты его персональных данных тем или иным оператором, а на деле все проводимые с ними операции вполне легальны — будет ли он нести ответственность за навет? Где это прописано? Это существенная недоработка нормативной базы ФЗ-152.

В силу целого ряда причин на данный момент не наблюдается массового исполнения требований регуляторов в части защиты ИСПДн. И, конечно, за ближайшие 1,5–2 месяца в корне ничего не изменится. Но дальнейшие перспективы уже намечены: часть из них была озвучена на недавних Парламентских слушаниях в Государственной думе. Это внушает надежду, что №152-ФЗ действительно обеспечит защиту прав и свобод граждан, а не превратится в инструмент лоббирования интересов отдельных групп.



стрировать стремление приблизиться к этой цели и таким образом избежать возможных санкций.

Стоит отметить, что в нынешней ситуации отечественные вендоры получили определенное преимущество перед зарубежными. Дело в том, что средства защиты персональных данных должны быть сертифицированы ФСТЭК и ФСБ; в частности, программные средства должны быть проверены на отсутствие недекларированных возможностей — так называемых «закладок». Для такой проверки необходимо представить сертификационным органам ФСТЭК исходные коды программных продуктов, на что, как правило, не соглашаются зарубежные вендоры: российский рынок приносит им слишком малую часть доходов, чтобы они рискнули ради нее миллиардами, потраченными на разработку своих программ. К примеру, среди производителей антивирусных программ на это решилась лишь одна зарубежная компания — сертификацию прошел антивирус ESET NOD32 Platinum Pack 4.0. При этом представителям ФСТЭК пришлось выехать в штаб-квартиру компании в Братиславе (Словакия), где в обстановке строжайших мер безопасности была проведена проверка исходных кодов антивируса, причем флеш-карта с программными средствами, которую использовали проверяющие, по окончании проверки была немедленно подвергнута физическому уничтожению.

Кроме поставщиков и регуляторов, на соблюдении сроков ввода в действие закона «О персональных данных» не настаивает сегодня никто, включая и граждан, интересы которых должен защищать закон.

КАК БЫ НЕ ЗАБЫТЬ О ГЛАВНОМ

При обсуждении требований к информационным системам для обработки персональных данных и их ответственности установленным нормам отошел на второй или даже более далекий план вопрос о том, каким образом может защитить свои права

КОММЕНТАРИЙ



Игорь Ляпунов,
начальник Центра информационной безопасности компании «Инфосистемы Джет»:

Большинство компаний начали активно заниматься темой защиты персональных данных только в середине 2009 г. Для тех, кто стартовал сейчас, выполнить все требования закона до 1 января 2010 года в полном объеме не представляется реальным, так как осталось менее двух месяцев. В этих условиях многие операторы персональных данных выбрали в качестве основной стратегии принцип «быть не хуже других», то есть, если и не провести работы в полном объеме, то хотя бы продемонстрировать регуляторам положительную динамику, какие-то шаги в сторону реализации требований.

Один из наиболее часто задаваемых вопросов — дадут ли отсрочку? Моя оценка как эксперта: переноса сроков не будет. Конечно, будут дорабатываться документы, будет происходить их гармонизация, устранение противоречий. Но это будет плавный процесс совершенствования нормативной базы, без «революций».

главный субъект закона — гражданин, данные о котором собираются, хранятся и обрабатываются теми или иными способами в различных информационных системах. Между тем именно этот вопрос должен быть в центре внимания на всех этапах обсуждения и внедрения закона. А неясностей здесь очень много. Скажем, статья 22.2.2 разрешает оператору без уведомления уполномоченного органа по защите прав субъектов персональных данных (а значит — без регистрации в реестре) производить обработку персональных данных, «полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных...». Спрашивается, значит ли это, что оператор кабельного телевидения или дирекция по экс-

Для того чтобы закон №152-ФЗ стал работоспособным и принес реальную пользу, его и подзаконные акты необходимо корректировать и приводить в соответствие реальным потребностям граждан и возможностей операторов

Если бы рыночные продавцы баз данных выявлялись и подвергались строгому наказанию, утечки персональных данных происходили бы значительно реже, а их коммерческое использование было бы весьма затруднено

плуатации зданий могут собирать и хранить данные о своих клиентах, не заботясь о соблюдении требований закона? Другой пример: та же статья, пункт 22.2.6, разрешает без уведомления уполномоченного органа обработку данных, «необходимых в целях однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях». Сегодня на проходных многих предприятий, даже торговых, от посетителей требуют предъявления паспорта или иного документа, данные из которых заносятся в компьютерную базу данных. Что будут делать с этими данными, куда и к кому они могут попасть?

Закон предоставляет гражданину право запросить у оператора персональных данных сведения о том, как используются его персональные данные, и запретить их дальнейшую обработку. Насколько реализуемо это право? На эти вопросы должны быть даны однозначные ответы, гражданам необходимо разъяснить их права, только тогда закон выполнит свою главную задачу.

НЕ НАДО «КОШМАРИТЬ БИЗНЕС»

Ситуация, сложившаяся вокруг закона №152-ФЗ «О персональных данных», напоминает ситуацию

КОММЕНТАРИЙ



Алексей Филатенков,
и. о. начальника отдела ИБ,
компания «Открытые Технологии»:

Если проанализировать количество зарегистрировавшихся операторов персональных данных, становится видно, что большинство организаций заняло выжидательную позицию. На мой взгляд, к этому их подталкивают как сложности с выполнением требований закона и подзаконных актов, так и не слишком понятная правоприменительная практика в плане санкций к нарушителям. Требования регуляторов описаны таким образом, что буквальное их выполнение порой ложится непосильной ношей на организации. Есть и еще проблема: при внедрении всех предписанных мер защиты внесение любых заметных изменений в систему влечет необходимость ее переаттестации. Поэтому крупные организации стараются уйти от буквального выполнения требований, ищут пути модификации своих информационных систем, обезличивания персональных данных, разработки специальной модели угроз для снижения расходов на обеспечение соответствия требованиям закона.



Юрий Малинин,
ректор Академии Информационных Систем:

Зачастую в качестве основного довода в пользу невозможности проведения работ операторы приводят отсутствие денежных средств. Да, покупка сертифицированных средств защиты и проведение аттестации (необходимость каковой еще необходимо обосновать) требуют финансовых затрат. Однако до этого этапа придется провести большой комплекс работ, таких как оптимизация ПДн в информационной системе и процессов их обработки, анализ состояния защищенности ПДн, классификация, выявление и моделирование наиболее актуальных угроз безопасности ПДн, разработка комплекта необходимой внутренней нормативной и регламентирующей документации, выработка рекомендаций по построению системы защиты ПДн. Большую часть этих работ оператор в состоянии сделать сам (при условии наличия в штате оператора подготовленных специалистов), что позволит значительно уменьшить финансовые затраты на выполнение требований российского законодательства.

с парковкой автомобилей на тротуарах: закон (статья 12.19 Административного кодекса РФ) запрещает остановку или стоянку автомобиля на тротуаре и предусматривает штраф за это в размере трехсот рублей. Скажите об этом москвичу, и ничего, кроме грустной ухмылки, у него это не вызовет: наличие закона компенсируется массовостью нарушений, и автомобили стоят на тротуарах по всему городу.

Для того чтобы закон №152-ФЗ стал работоспособным и принес реальную пользу, его и подзаконные акты необходимо корректировать

и приводить в соответствие реальным потребностям граждан и возможностям операторов. Похоже, что события развиваются в этом направ-

лении. После прошедших в октябре парламентских слушаний по закону «О персональных данных» аппарат Госдумы готовит рекомендации, Комитет по конституционному законодательству формирует рабочую группу, и до нового года, согласно имеющейся у нас информации, предполагается внести в Думу проект изменений закона — в нем собираются отредактировать больше половины статей.

ЗАКОН ЕСТЬ ЗАКОН?

Будет ли изменен закон №152-ФЗ или отложен срок его ввода в действие, мы скоро узнаем. К сожалению, малоэффективными и трудно реализуемыми оказываются и другие действующие законы, такие как статья 183 УК РФ, предусматривающая лишение свободы на два года за сбор сведений, составляющих коммерческую или банковскую тайну, и на срок до трех лет за их использование, или статья 272 УК — «Неправомерный доступ к компьютерной информации», предусматривающая тюремный срок до пяти лет. Если бы рыночные продавцы баз данных или злоумышленники вроде тех, с предложения которых я начал статью, выявлялись и подвергались строгому наказанию, утечки персональных данных происходили бы значительно реже, а их коммерческое использование было бы весьма затруднено. Если же закон нечеток, не соответствует жизненным реалиям, а его полномасштабное применение не может быть обеспечено — такой закон становится инструментом избирательного применения, создающим почву для злоупотреблений. ☒

СЕГОДНЯ НА ПРОХОДНЫХ МНОГИХ ПРЕДПРИЯТИЙ, ДАЖЕ ТОРГОВЫХ, ОТ ПОСЕТИТЕЛЕЙ ТРЕБУЮТ ПРЕДЪЯВЛЕНИЯ ПАСПОРТА ИЛИ ИНОГО ДОКУМЕНТА, ДАННЫЕ ИЗ КОТОРЫХ ЗАНОСЯТСЯ В КОМПЬЮТЕРНУЮ БАЗУ ДАННЫХ. ЧТО БУДУТ ДЕЛАТЬ С ЭТИМИ ДАННЫМИ, КУДА И К КОМУ ОНИ МОГУТ ПОПАСТЬ?