ЗАКОНОДАТЕЛЬСТВО О ЗАЩИТЕ ИНФОРМАЦИИ нужно выполнять

Справка «ТБ»

Сапрыкин Александр Михайлович.*1979—1996 — служба в Вооруженных силах СССР и Республики Беларусь на командно-технических должностях. Полковник запаса.1996—2003 — начальник управления информационных технологий МИД Беларуси. 2003—2008 — советник — начальник отдела электронных СМИ и информационных технологий Посольства Республики Беларусь в России. С 2008 года по настоящее время — директор ИП «С-Терра Бел». Имеет четыре образования — радиотехническое (базовое), юридическое, лингвистическое и специальное.*

Прошло более года с момента принятия в Республике Беларусь закона «Об информации, информатизации и защите информации» и полгода со дня вступления его в силу. Время поделиться первыми, не претендующими на всесторонность и исчерпывающую глубину, впечатлениями и наблюдениями. Причем, в данной публикации речь пойдет не о законе в целом, который носит комплексный и универсальный характер, а лишь о некоторых его аспектах, связанных с проблемой защиты информации в госорганах и организациях, работающих с персональными данными.

Новое белорусское законодательство в сфере защиты информации давно и с нетерпением ожидали эксперты и специалисты. Защита информации (информационная безопасность) представляет собой своего рода «элитный» сектор ИТ-отрасли, ведь без отечественных средств защиты информации трудно себе представить создание полноценного электронного государства. Дело в том, что средства защиты выполняют в нем функции, сравнимые с независимостью и суверенитетом территориального государства. Остановимся на ходе реализации требований нового законодательства в госорганах и организациях, работающих с персональными данными.

Построение защищенных информационных систем государственных органов.

На первый взгляд, ничего нового закон не привнес — многие государственные органы занимались этим и ранее. Однако теперь без мер по защите законодательно **запрещается эксплуатировать информационные системы всех без исключения госорганизаций**. Также в законе дается четкое разъяснение, что использовать в этих целях можно только средства защиты, которые прошли экспертизу (сертификацию) в национальной системе соответствия. На практике это привело к сложившейся по «умолчанию» ситуации, когда существующие информационные системы госорганов продолжают работать без внесения корректив, но в случаях модернизации или создания новых систем в смету закладываются расходы на защиту информации. В целом, в бюджетных организациях особой активности по использованию защитных средств в истекшем периоде не наблюдалось. Понятно, что главным сдерживающим фактором стали неблагоприятные экономические условия, при которых бюджеты сократились до минимума.

Защита информационных систем организаций, содержащих персональные данные.

Это первый серьезный подход в республике к проблеме защиты персональных данных, причем подход достаточно эффектный. В законе не разграничиваются понятия защиты информационных систем госорганов и организации с персональными данными — оговаривается лишь то, что используемые в этих целях средства защиты должны пройти сертификацию (госэкспертизу).

Однако для организаций, работающих с персональными данными, до настоящего времени фактически ничего не изменилось. Дело в том, что ни в самом законе, ни в подзаконных актах, принятых с целью его развития, **не были установлены сроки и перечни защищаемых данных**. Неудивительно, что эта часть законодательства на практике не начала действовать и защитой персональных данных согласно новым требованиям не занимались даже ведущие участники этого рынка. Точнее, если и занимались, то приобретали в этих целях несертифицированные средства защиты, которые с принятием закона на официальном уровне таковыми уже не признаются.

Чтобы понять, хорошо это или плохо, обратимся к международной практике. Практически все **развитые страны активно и целенаправленно решают проблему защиты персональных данных** уже длительное время. Как известно, катализатором процессов по защите персональных данных в европейских странах стала Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных», принятая еще в 1981 г.

Для сравнения можно отметить подходы России к решению этой проблемы. Российская Федерация, подписав указанную конвенцию в 2001 г., ратифицировала ее спустя 4 года, а к практической защите персональных данных приступила лишь с 2007 г. Завершить в целом этот процесс, как планировалось, к началу 2010 г. ей не удалось из-за экономических условий, и Госдума продлила срок еще на год.

В наших условиях (географических, транзитных), когда с одной стороны — Евросоюз, с другой — Россия, с такими же европейскими нормами в законодательстве, подписание конвенции не только желательно, но и объективно отвечало бы интересам Беларуси как развитой в информационном плане страны мирового сообщества. Соответствовало бы оно и социальной направленности политики нашего государства по защите интересов своих граждан. Немаловажно в этом контексте и то, что европейское и российское законодательства устанавливают ограничения на передачу персональных данных в государства, где правовое регулирование не обеспечивает их должной защитой. **Трансграничная передача данных — не пустая формальность, за этим понятием стоят международные авиа — и железнодорожные перевозки, деятельность миграционных и консульских служб и т. п**. Поэтому решение этой проблемы представляется не менее важным и значимым, чем обеспечение наземной инфраструктуры транзитных коммуникаций.

Международные аспекты защиты персональных данных представляются актуальными нашим соседям — об этом свидетельствуют прошедшие

в текущем году союзная (белорусско-российская) и евразийская конференции, посвященные теме трансграничной передачи данных. Белорусской стороне большей частью пришлось участвовать в обсуждении теоретических наработок, ведь практические в республике отсутствуют. И если в России за последнее время прошли многие десятки семинаров, конференций и круглых столов по теме защиты персональных данных, то **в Беларуси не отмечено ни одного мероприятия в контексте требований нового законодательства о защите персональных данных**.

Немаловажно и следующее обстоятельство. Российские эксперты единодушно отмечают, что работающий у них (но не у нас!) закон о персональных данных придал серьезный импульс развитию национального рынка информационной безопасности (ИБ) в целом, что в период финансового кризиса оказалось как нельзя кстати. Причем доминируют на этом рынке отечественные производители средств защиты информации. У нас же сфера ИБ пока целиком «бюджетная» — только госорганы вкладывают средства в ее развитие, а **организации, работающие с персональными данными, как и прежде работают на иностранного производителя** и выполнять требования законодательства вовсе не торопятся.

Можно с высокой степенью достоверности полагать, что целенаправленные и, может быть, даже жесткие действия по защите персональных данных (ПД) будут с пониманием восприняты мировым сообществом — подобные ценности относятся к абсолютным и незыблемым для всех цивилизованных стран и находятся под пристальным вниманием и экспертов, и правительств.

В частности, недавно проведенный в США опрос организацией Unisys Security Index показал, что современные американцы в большей мере опасаются быть ограбленными в киберпространстве, чем подвергнуться нападению в реальном мире. Согласно результатам опроса, 65 % респондентов заявили о возможном злоупотреблении их персональными сведениями. Исследователи называют кражу идентификационной информации одной из наиболее актуальных проблем для большей части населения США.

Белорусов пока не в такой степени волнует утечка информации об их кредитах, доходах и налогах, владении недвижимостью, состоянии вкладов и т. п., но ведь это реальное будущее и к нему надо готовиться. К примеру, если в развитых странах утечка информации для организаций, работающих с персональными данными, означает удар по имиджу, потерю клиентов и серьезные финансовые издержки, то у нас систематические утечки подобных данных у некоторых операторов связи фактически никак не сказываются на их популярности. Многие из нас испытывают, как минимум, дискомфорт от подобных утечек, но свыклись с этим чувством и не слишком верят в то, что их данные могут быть надежно защищены.

Некоторые специалисты ожидали, что в связи с принятием нового законодательства **возрастет число исковых заявлений, которые стимулируют организации, работающие с персональными данными, к принятию мер по их защите**. На первый взгляд, действительно, если кому-то удастся доказать причинно-следственную связь между нанесенным ему ущербом и утечкой таких данных из организации, где они хранились, то закон будет явно на его стороне. Другое дело, что какой-либо массовости подобных действий в силу сложившегося менталитета поведения у населения ожидать все же не стоит.

Следовало бы определиться и в вопросе, **какие данные нужно защищать**. К счастью, чужого опыта и наработок по этой теме более, чем достаточно. Очевидно: то, что апробировано практикой многих стран — это подготовка отраслевых стандартов безопасности персональных данных. Ведь одни персональные данные об одном и том же лице хранятся в банке, включая тайну вкладов, другие — в медучреждении, включая врачебную тайну, и совсем иные — у оператора связи. Поэтому логично в каждой отрасли защищать свое, специфичное.

В том, что в республике не решается проблема защиты ПД, виновата отнюдь не кризисная ситуация в экономике — у основных участников рынка ПД в республике была сосредоточенна крупная сумма денег на приобретение несертифицированных средств защиты информации. Их приобретали и банки, и операторы связи. Как и раньше, словно ничего не изменилось, звучали традиционные заявления, что у них все «качественно и надежно защищено», клиентам давались самые серьезные гарантии конфиденциальности и сохранности. Возможно, так оно и есть, но пусть бы в этом убедились и белорусские эксперты, и наши регулирующие органы. Ведь это дело уже не частного характера…

Однако существуют и положительные наработки. В частности, основной регулирующий орган в сфере информационной безопасности в республике — Оперативно-аналитический центр при Президенте Республики Беларусь подошел к исполнению нового законодательства с максимально возможной степенью открытости — на его интернет-сайте представлен перечень всех сертифицированных в Беларуси средств защиты информации. Их, кстати, немало — более полутора сотен, и в истекшем периоде их количество заметно увеличилось. Законопослушным организациям, аккумулирующим в своих информационных системах персональные данные, всего-то и надо, что сделать выбор в пользу сертифицированных средств защиты — как того требует закон. Там же, на сайте, обнародован и список лицензиатов — тех, кому разрешено проведение работ по защите информации. Среди лицензиатов ОАЦ почти две сотни компаний и организаций. Это очень значительный ресурс — не меньший, к примеру, чем у Парка высоких технологий, и нет сомнений, что ему по силам реализовать на практике закон № 455 как в части защиты госорганов, так и организаций, работающих с персональными данными.

Из всего вышесказанного следует очевидный вывод: **защитой персональных данных целесообразно заняться сейчас и всерьез**, причин для дальнейшего незаинтересованного отношения к проблеме просто не существует. Напротив, даже поверхностный анализ внутренних и международных аспектов этой проблемы свидетельствует в пользу активных и целенаправленных действий в этом направлении.