

В противовес «ленивым»

В преддверии наступления упоминаемой всеми и вся даты – 1 января 2010 года – мы беседуем с генеральным директором ЗАО «НПО «Эшелон» А. С. Марковым.



Алексей Сергеевич, страна находится в ожидании 1 января 2010 года – даты полноценного вступления в силу закона «О персональных данных». С момента его принятия в сторону этого федерального закона выпущено немало критических стрел и юристами, и экономистами, и организациями-операторами персональных данных. Как бы вы прокомментировали наступление этого события?

В настоящее время только ленивый не критикует ФЗ-152 «О персональных данных». Однако Закон возник не на пустом месте и направлен на решение уже ставших традиционными для нашей страны нарушений прав субъектов персональных данных. Требования Закона коснулись организаций различной формы собственности и разного уровня достатка, что и вызвало резонанс в обществе, которое оказались не готово к защите приватной информации.

При очевидной сложности технической реализации Закона, следует

отметить позитивные моменты, связанные с его появлением.

Во-первых, новые методические документы потребовали от юридических лиц разработки и внедрения комплекса организационных мер по защите информации. Как известно, организационные меры в области безопасности (как социальной сферы человеческих взаимоотношений) представляют собой более действенный механизм по сравнению с использованием даже самых замысловатых технических средств защиты.

Главным документом по технической защите стала частная модель угроз, а не, скажем, предъявляемое при проверках в госпредприятиях какое-нибудь руководство по качеству или положение по ПДИТР. Это означает, что произошел переход от директивной системы защиты информации определяемой античными Руководящими документами, к адаптивной защите конкретных информационных ресурсов от актуальных угроз нарушения целостности, доступности и конфиденциальности. Рекомендации по разработке модели угроз стали не просто формальностью, а инструментом, позволяющим оптимизировать затраты на защиту информации, например, путем исключения неактуальных угроз. Данный подход может быть базовым в развитии национальных стандартов, гармонизации с лучшими зарубежными практиками, в формализации вопросов защиты (например, путем гармонизации с метастандартом ИСО 15408), при изучении систем менеджмента персональных данных.

Во-вторых, Закон запустил новый виток развития технологий за-

щиты. В методических документах определены более современные средства защиты, в явном виде указано на контроль уязвимостей программных средств (недекларированных возможностей). Сейчас активно обсуждаются передовые подходы к организации систем в защищенном исполнении, например систем с терминальным доступом, систем разделения обработки данных, возможные способы анонимизации персональных данных. Закон обострил честную конкуренцию разработчиков систем (особенно антивирусных) и обозначил культуру аутсорсинга. Требования косвенно ориентированы на российского разработчика, поскольку подразумевают предоставление исходных кодов при оценке соответствия средств защиты. Неиспользование этой возможности может быть объяснимо только нерадивостью соратников.

В-третьих, именно ФЗ-152 позволил проконтролировать ряд сегментов госсектора, где традиционно игнорировали защиту конфиденциальной информации (например, на станциях переливания крови или в региональных ЗАГСх). Первые проверки, проведенные регуляторами, выявили исключительную халатность, допускаемые работниками этих заведений в отношении информации ограниченного доступа, граничащую с опасностью для здоровья и жизни людей. Вследствие этого в ряде организаций уже прошла волна мероприятий, направленных на ликвидацию безграмотности в данной области, в них сформированы перечни конфиденциальной информации, приняты элементарные организационно-распорядительные меры, про-

веден аудит защищенности, отсеяны некомпетентные соисполнители. Таким образом, важное политическое следствие ФЗ-152 заключается в поднятии проблемы защиты информации ограниченного доступа вообще, а не только персональных данных.

По исконно российской причине была продемонстрирована исключительная актуальность в нашей стране механизмов госрегулирования, таких как лицензирование, аттестация и сертификация. Указанные процедуры оценки соответствия приподняли проблему использования нелегальных средств защиты (хотя бы в отношении корпоративных антивирусов и межсетевых экранов). Фактически ФЗ-152 выявил теневой пласт экономики, где ряд учреждений осуществлял незащищенную обработку и передачу информации ограниченного доступа. К примеру, владельцы систем и соисполнители работ игнорируют требования по лицензированию, это позволяет им избежать плановых проверок регуляторов, а соответственно, аттестации, соблюдения лицензионной чистоты, наличия самых элементарных правил защиты личных данных.

И последнее. Роль Закона в определении параметров технической защиты приватной информации, безусловно, важна. Но, что еще более важно, Закон, возможно, послужил толчком к изменению отношения общества к правовым моментам обработки информации. Примером тому является обсуждение в СМИ фактов беспардонных публикаций персональных данных, а также новые правила проверки организаций малого и среднего бизнеса. Очевидна лояльность регуляторов при решении проблемных вопросов.

По итогам октябрьских парламентских слушаний сложилось впечатление об имеющемся противостоянии в обществе в отношении к ФЗ-152.

Если посмотреть рекомендации по совершенствованию ФЗ-152, высказанные на октябрьских парламентских слушаниях, становится очевидной оппозиция банковского сектора. Если говорить о технической стороне проблемы, это вполне



xxxx
InfoSecurity'08

объяснимо. В банках существует внутренняя эффективная нормативная база в данной области, сложилась система взаимодействия с регуляторами, ущерб от нарушений безопасности глубоко значим для организации. Достраивать систему в соответствии с общероссийскими методическими, но «сырыми» документами, болезненно.

Что касается других сфер деятельности, то аргументом для переноса даты полноправного вступления в силу ФЗ-152 может служить лишь факт задержки опубликования открытых выписок из методических документов ФСТЭК и их «незаконченность».

Основным аргументом против ФЗ-152 называют высокие финансовые затраты на реализацию данного закона, называются даже цифры в районе 3–4 % бюджета страны.

В нашей стране кроме государственной тайны существует около 50 видов тайн, исторически отнесенных к конфиденциальной информации. За нарушение защиты, дай Бог памяти, тринадцати видов тайн предусмотрена даже уголовная ответственность. Поэтому говорить, что защиту персональных данных надо начинать с нуля, неверно. Если сравнить затраты на создание и аттестацию подсистемы защиты, например корпоративной сети, по требованиям защиты конфиденциальной информации (СТР-К) и по тре-

бованиям новых методических документов, то разница коснется, главным образом, стоимости разработки проектной документации. Скорее всего, означенная сумма не превысит 5–10 % от общей стоимости решения. Следует добавить, что грамотно разработанная модель угроз в ряде случаев позволяет существенно снизить затраты, например исключить затраты на ПЭМИН!

При этом реализация организационных мер защиты скорее связана с ударом по народному разгильдяйству и с мобилизацией внутренних ресурсов.

С другой стороны, слабым местом российских законов, причем не только в области персональных данных, является отсутствие условий для их экономичного выполнения. Очевидно, что аттестовать абсолютно все нельзя, быть может, в каких-то случаях достаточно было сделать упор на организационные меры (назначить виновного), а в ряде случаев — нет. Это требует переработки как самого понятия информации ограниченного доступа (50 видов тайн), так и уровней ее защиты. Но это — другая тема.

При всем при том следует признать, что на данный момент именно ФЗ-152 является краеугольным камнем защиты прав субъектов персональных данных и становления передовой взвешенной технической политики в области защиты информации ограниченного доступа. ■