

ФЕДЕРАЛЬНЫЙ ЗАКОН № 152 «О ПЕРСОНАЛЬНЫХ ДАННЫХ»: ГОТОВНОСТЬ НОМЕР?..

Проблемы обеспечения информационной безопасности (ИБ), в том числе касающиеся исполнения требований ФЗ № 152, постепенно решаются, уверены представители компаний, работающих в этой сфере. Только решать их надо не фрагментарно, а комплексно.

— В чем сложности исполнения Федерального закона РФ № 152 от 27 июля 2006 г. «О персональных данных»? И каковы, по вашему мнению, пути их преодоления?

Д.В. Савченко, руководитель департамента систем и методов обеспечения ИБ «Микротест»: Закон действует уже более трех лет, тем не менее его практическая реализация по-прежнему проблематична. Это связано с тем, что требования регулирующих органов, регламентирующие технические и организационные меры защиты ПДн, появились только в 2008 г. и все еще проходят переработку. Причем эти нормативы разрабатывались на основе действующих уже много лет требований по защите конфиденциальной информации, не учитывающих отраслевую специфику современных систем.

На наш взгляд, решение существующих проблем невозможно без активного участия в законотворческом процессе консультационных советов, занимающихся обеспечением защиты ПДн в информационных системах (ИС) различных сфер деятельности. Это поможет консолидировать вопросы, связанные с реализацией требований закона, и предложить законотворческим органам оптимальное решение по каждому направлению. Мы полагаем, что существующие подзаконные акты необходимо пересмотреть и дополнить с учетом действующих нормативных правовых документов. Активное участие экспертов различных сфер деятельности будет способствовать приведению законодательства к актуальному и действительно реализуемому состоянию.

В. А. Сердюк, генеральный директор «ДиалогНаука», к. т. н., CISSP: В настоящее время можно выделить следующие основные сложности в реализации положений ФЗ № 152:

- отсутствие финансирования в объеме, необходимом для решения задачи по защите ПДн. В этой ситуации многие компании начинают работу по приведению своих ИС в 2009 г., а завершение работ планируют на 2010 г. вместе с выделением необходимых средств из бюджета;

- неточность формулировок и положений в нормативных документах, содержащих требования к защите ПДн. В настоящее время планируется внести изме-

нения как в ФЗ № 152, так и в локальные нормативные акты, что поможет снять основную часть неточностей, допускающих различные варианты толкования одних и тех же требований.

В.И. Скиданов, технический специалист Aflex Software: Закон еще довольно сырой, и отдельные моменты его исполнения вызывают вопросы. Порой не всегда четко можно определить необходимый комплекс мер по защите ПДн с учетом особенностей конкретной компании.

Множество решений по обеспечению ИБ, которые компании внедряли по собственной инициативе, не обладают необходимыми лицензиями. Причем эти решения могут быть стандартом де-факто в международном корпоративном секторе, но не адаптированными к особенностям работы в России. Часть этих решений сейчас проходит этап лицензирования, еще часть не сможет получить лицензии (например, решения по шифрованию данных). Таким образом, компании, ранее построившие защиту ПДн, будут вынуждены модифицировать свою ИТ-инфраструктуру с учетом новых требований, другим придется создавать подобную инфраструктуру заново. Исполнение закона не внесет существенных изменений в отношении компаний к ИТ-безопасности. Если раньше были компании, имеющие систему качественной ИТ-безопасности и не имеющие таковой, то теперь компании разделятся на те, которые внедрили удовлетворяющие закону решения, и те, которые выполнили требования ФЗ № 152 формально, «для галочки».

Вообще говоря, это проблема общей ИТ-грамотности российских специалистов, и топ-менеджеров в частности. До тех пор пока не будет четкого осознания необходимости качественной ИТ-инфраструктуры (и рисков, которые несет ее отсутствие), никакой закон не приведет к кардинальным изменениям. Впрочем, остается надежда, что все же часть компаний, озадачившись необходимостью строить защиту ПДн с нуля, отнесутся к этому как к возможности создать надежную систему безопасности.

Для небольших компаний имеет смысл обратиться к услугам сторонних экспертов и компаний-интеграторов. Аут-

сорсинг хранения ПДн облегчает выполнение требований к комплексу мер по защите, хотя не освобождает от этого целиком.

В.В. Ульянов, руководитель аналитического центра Perimetrix: Основные сложности исполнения ФЗ № 152 — это, традиционно, бюджетные ограничения, нехватка квалифицированного персонала и отсутствие понимания, как эти требования реализовать.

Что касается первого пункта, то средства должны быть выделены: закон обязателен для исполнения. Да и экономия на безопасности до добра не доводит. Нет сомнений, что сегодня защита ПДн входит в число приоритетных проектов большинства организаций. Нехватка квалифицированного персонала, наверное, будет преодолеваться естественным образом по мере накопления опыта сегодняшними специалистами, которые только начинают заниматься ПДн. Если, конечно, импульсивное руководство не начнет требовать каких-то мгновенных результатов. Наконец, неясности закона постепенно ликвидируются с помощью подзаконных актов, постановлений, рекомендаций регуляторов.

— Каким образом можно решить проблемы ИБ в федеральных, региональных и муниципальных органах власти и управления, в том числе в связи с ФЗ № 152 «О персональных данных»?

Д.В. Савченко: В первую очередь в органах государственной власти и управления следует провести организационные мероприятия по защите как ПДн, так и другой информации: они помогут регламентировать порядок и способы обработки данных, а также минимизировать риски нарушения ИБ. Необходимо упорядочить существующие ИС, провести обучение пользователей основам информационной безопасности и обязать их соблюдать требования по ИБ. Конечно, это связано с существенными финансовыми затратами, однако эту работу можно разбить на небольшие этапы, что позволит бюджетным организациям создавать системы защиты постепенно.

В.А. Сердюк: Как один из вариантов — разработка типовых решений по защите ПДн для органов государственной власти различных уровней, обладающих свойствами масштабируемости и тиражируемости.

В.И. Скиданов: Начинать надо с проведения адекватного и конкурентоспособного тендера по поиску поставщика и ин-

тегратора систем. Велосипед здесь изобретать не требуется — у серьезных компаний есть опыт разработки и внедрения систем защиты информации для госсектора развитых стран. Эти СЗИ отвечают высоким стандартам качества.

Внедрение комплекса мер защиты предусматривает, в том числе, автоматизацию и защиту от ошибок пользователей, поэтому не стоит беспокоиться за ИТ-навыки чиновников, скорее наоборот — качественно построенный процесс ИТ-безопасности снижает ответственность рядового пользователя за возможность утечки информации, забота об этом перекладывается на специалистов. Так что исполнение ФЗ № 152 может качественно улучшить ИТ-безопасность систем госсектора, если правильно подойти к этому вопросу.

В. В. Ульянов: Прежде всего должна быть определена ответственность органов власти за утечку ПДн — только тогда госструктуры будут мотивированы на их защиту. Вряд ли можно рассчитывать, что в ситуации, когда никто никакой ответственности не несет, чиновники будут ревностно блюсти интересы третьих лиц.

Что касается непосредственно методов сохранения конфиденциальности ПДн, то эта проблема не должна решаться в отрыве от ИБ в целом: необходимо использовать те же средства предотвращения утечек, что и для коммерчески важной информации, для служебной тайны.

— Как вы оцениваете перспективы создания единой инфраструктуры открытых ключей Российской Федерации (ИОК РФ)? Есть ли на российском рынке решения, полностью удовлетворяющие условиям задачи?

В. А. Сердюк: Насколько нам известно, в настоящее время ведутся исследования по созданию единой ИОК РФ. Над этой задачей работает Федеральное агентство по информационным технологиям совместно с ФГУП НИИ «Восход». С нашей точки зрения, при этом необходимо использовать комплексные решения, предусматривающие применение технологий от разных разработчиков и интеграторов.

Д. В. Савченко: Сегодня ситуация для создания единой ИОК РФ среди государственных органов вполне благоприятная. Мы считаем, что объединение существующих удостоверяющих центров органов власти и управления в общую систему, а также выработка и реализация единых стандартов ИОК РФ вполне возможны.

Что касается создания ИОК, которая объединила бы коммерческие и государственные организации, то на данный момент это затруднительно. Существующие стандарты и нормативные правовые акты, регламентирующие использование

открытых ключей, электронной цифровой подписи и шифрования, не учитывают в полной мере особенности работы коммерческих организаций. Средства и требования по реализации ИОК зачастую не совместимы с используемыми системами автоматизации, стоимость их внедрения не всегда оправдана, поэтому зачастую их внедрение в ряде коммерческих структур оказывается невозможным.

Одной из основных проблем при разворачивании ИОК становится использование зарубежных криптографических алгоритмов, необходимых для защищенного обмена информацией с иностранными компаниями. Для создания единой ИОК РФ необходимо внесение изменений в законодательные и подзаконные акты, а также их детальная проработка с учетом особенностей деятельности коммерческих структур, их взаимодействия с государственными организациями и сотрудничества с иностранными компаниями.

— Какие решения наиболее важны для организации защищенной инфраструктуры телекоммуникаций? В чем заинтересован потребитель и что может дать ему оператор?

А. В. Бугаенко, директор по ИТ компании «Синтерра»: Обеспечение подавления атак и аномалий трафика до его попадания к потребителю, защита ПДн на сетевых сегментах процесса обработки данных, сетевая статистика, аутсорсинг, принципиально новые и инновационные услуги, которые позволят повысить надежность предоставления информационных сервисов и функционирования информационных систем заказчика. Например, системы стриминга приложений, Content Delivery Network, позволяющие более эффективно бороться с атаками типа DDoS, и т. п.

В. А. Сердюк: Для обеспечения защиты инфраструктуры телекоммуникаций необходимо использовать комплекс мер, предусматривающий защиту от спама, компьютерных вирусов, сетевых атак, контентного анализа, утечки конфиденциальной информации и т. д. Выбор конкретных технологий зависит от специфики защищаемой инфраструктуры.

Д. В. Савченко: Для потребителей ИКТ-услуг важно быстро и качественно получать и осуществлять обмен информацией, а также надежно защитить передаваемые данные — обеспечить конфиденциальность, целостность и неизменность информации. Для этого необходимо комплексное использование организационных и технических мер по защите телекоммуникационной инфраструктуры. Именно совокупное применение решений в части антивирусной защиты, централизованное управление политиками

безопасности, использование средств идентификации и аутентификации пользователей, обеспечение безопасности сегментов сети, применение средств контроля, а также регламентирование используемых средств защиты и выработка правил безопасности в компании позволят организовать защищенную инфраструктуру телекоммуникаций наиболее эффективно.

— Как ваша компания решает задачи ИБ? По каким стандартам вы оцениваете уровень обеспечения информационной безопасности своей организации?

А. В. Бугаенко: Основой для обеспечения ИБ корпоративной сети «Синтерры» являются национальные стандарты ГОСТ Р ИСО/МЭК 17799-2005, ГОСТ Р ИСО/МЭК 13335-1-2006, ГОСТ Р 50922-2006, а также международные — ИСО/МЭК 27000 и COBIT. Обеспечение ИБ клиента требует еще и решения конкретных задач его ИТ-департамента. Например, для защиты от DDoS-атак ИС и ресурсов крупных компаний, ведущих активную экономическую деятельность в Интернете, мы используем многослойную систему защиты, в которую входят программно-аппаратные комплексы операторского класса иностранного производства, собственная разработка, не уступающая по своим характеристикам зарубежным образцам, системы очистки трафика от вредоносных воздействий.

В. А. Сердюк: В ЗАО «ДиалогНаука» применяется комплексный подход для обеспечения информационной безопасности, предусматривающий применение как технических, так и нормативно-методических мер защиты. В своей работе мы ориентируемся на международные стандарты серии ISO 27000, а также на российское законодательство, в частности Федеральный закон «О персональных данных».

Д. В. Савченко: При реализации защиты информации в компании «Микротест» применяются организационные и технические решения. Использование доменной политики позволяет осуществлять централизованное управление и контроль за работой пользователей; для повышения эффективности и защиты сети разработаны и применяются антивирусная и парольная политики, реализованы меры ограничения доступа работников компании к ССОП. Для снижения рисков нарушения ИБ осуществляется контроль телефонии и электронной почты, а также использования внешних и внутренних сетевых ресурсов. Для оценки уровня ИБ в компании применяются международные и отечественные стандарты.