

БЕЗЗАЩИТНЫЕ ДАННЫЕ

В КОНЦЕ ПРОШЛОГО ГОДА ПОЯВИЛАСЬ И СРАЗУ СТАЛА ХИТОМ НЕЛЕГАЛЬНЫХ ПРОДАЖ БАЗА С НАЛОГОВЫМИ ДЕКЛАРАЦИЯМИ ПОЧТИ 10 МЛН МОСКВИЧЕЙ, С УКАЗАНИЕМ ИХ МЕСТА РАБОТЫ И АДРЕСОВ. ЭТО ПЕРЕПОЛНИЛО ЧАШУ ТЕРПЕНИЯ ЗАКОНОДАТЕЛЕЙ, И В ГОСДУМУ БЫЛ ВНЕСЕН ПЕРВЫЙ ВАРИАНТ ЗАКОНОПРОЕКТА «О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ». В ЯНВАРЕ 2007 ГОДА ЗАКОН ВСТУПИЛ В СИЛУ, НО ЗАМЕТНЫХ ИЗМЕНЕНИЙ НА РЫНКЕ ЭТО ПОКА НЕ ПРОИЗВЕЛО. ПО КРАЙНЕЙ МЕРЕ, В ПРОДАЖЕ, КАК И РАНЬШЕ, ЕСТЬ КРАДЕННЫЕ БАЗЫ ДАННЫХ БАНКОВ, МОБИЛЬНЫХ ОПЕРАТОРОВ И ТАМОЖНИ. ВИКТОРИЯ ЗАВЬЯЛОВА

КРАДУТ ПО-ПРЕЖНЕМУ Впрочем, нельзя сказать, что закон предъявил рынку какие-то новые требования, скорее унифицировал существовавшие ранее. Главное, что сделал закон, — зафиксировал ответственность компаний, допустивших утечку информации о клиентах, а также регламентировал порядок работы с персональными данными клиентов. Информация о гражданах и их персональных данных должна храниться таким образом, чтобы утечки не произошло. А если это все-таки случилось, компания может быть наказана штрафом или лишением лицензии. И наконец, отвечать за утечку данных будет не только компания, откуда они были украдены, но и продавец информации.

Серьезных изменений на рынке технологий обеспечения информационной безопасности после выхода закона еще не произошло, но в будущем, полагают специалисты, этот рынок окажется в большом выигрыше. «Мы считаем, что в перспективе закон обязательно отразится на нашем бизнесе», — говорит технический специалист департамента программных решений «НР Россия» Сергей Знаменский. — В частности, на продажах наших программных продуктов для управления доступом к ИТ-ресурсам — HP Select Access Software. Сегодня это ПО применяется на российских предприятиях и обладает возможностями по защите идентификационной информации и персональных данных».

Представители ИТ-компаний и эксперты в целом оценивают закон позитивно и говорят о его положительном влиянии на рынок. По мнению старшего менеджера, руководителя направления информационной безопасности в России и странах СНГ компании Deloitte & Touche Нины Парфеновой, принятие закона активизировало внедрение средств шифрования и создание соответствующей инфраструктуры хранения данных.

А директор по информационной безопасности Владимир Мамыкин, вице-президент Microsoft в России и СНГ, считает, что уже сейчас заметно влияние закона на коммерческие и государственные структуры, работающие с

УЖЕ ПОСЛЕ ПРИНЯТИЯ ЗАКОНА «О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ» ПИРАТСКИЕ ДИСКИ ПРИ ЖЕЛАНИИ МОЖНО НАЙТИ В ПОДЗЕМНЫХ ПЕРЕХОДАХ, НА РАЗВАЛАХ И НЕКОТОРЫХ САЙТАХ



СЕРГЕЙ МИКЕЕВ

КАК УТЕКАЕТ У НИХ

Ужесточение и развитие законодательства в сфере информационной безопасности — мировая тенденция. К примеру, новый законопроект по защите персональных данных, который обещает ввести жесткую ответственность компаний за утечки сведений, готовят сейчас в США. Инициаторами выступают независимый сенатор Бернارد Сандерс и Патрик Лихи от демократической партии. Согласно проекту закона, наказание должны нести не только преступники, но и компании, допустившие утечку. Новые правила для компаний об обязательном уведомлении граждан в случае любой утечки или кражи информации с начала этого года разрабатывает и Европейская комиссия. Правило, согласно которому компании будут обязаны сообщать об утечке персональных данных, вводит и главный надзорный орган над финансовым рынком Великобритании FSA (Financial Service Authority). Причиной такого решения стало то, что британские компании часто скрывают факты утечки персональных данных, при этом халатно относясь к хранению информации. Например, как выяснилось этой осенью, некоторые банки выбрасывают носители информации, содержащие приватные сведения о клиентах, в обычные мусорные баки. В конце 2006 года расследование офиса комиссара по информации (Information Commissioner's Office) выявило 11 крупных организаций, которые нарушают закон о защите информации. Среди них оказались United National Bank, Barclays Bank, HFC Bank и даже почта Соединенного Королевства — UK Post Office. То есть в цивилизованном мире информацию крадут не реже, чем в России.

Одна из самых скандальных историй последних лет — утечка 40 млн записей о владельцах кредитных карт MasterCard, Visa, American Express и Discover (см.

статью на стр. 27). В России информацию обычно сливает источник в компании, здесь же действовали внешние враги — хакеры. Как выяснилось, крупный сотрудник информации для банков и фирм CardSystems Solutions не уделял должного внимания обеспечению безопасности. Компания продолжала хранить записи, подлежащие удалению, а данные о транзакциях не шифровались. Хакеры смогли установить в сети CardSystems Solutions трояна, перехватывающего данные о кредитных картах в процессе проведения финансовых транзакций. Так они получили информацию об именах владельцев карт, номерах их счетов и кодах подтверждения. Вскоре сообщения о мошенничествах стали поступать из банков. То, что перехват происходит через CardSystems, выяснили специалисты Cybertrust. Через некоторое время Visa, на которую приходилось больше половины операций CardSystems, отказалась работать с этой компанией.

Печальная история произошла в Bank of America. Его сотрудники потеряли носители с информацией о более чем 1 млн клиентов, среди которых были и американские сенаторы. Пропадали и персональные данные Калифорнийского и Стэнфордского университетов, информационных брокеров ChoicePoint и LexisNexis. В прошлом году отметились банк Sovereign, министерство образования и министерство транспорта США. Перечислять можно до бесконечности. И во всем мире одним из наиболее значительных факторов риска в системе защиты данных остается не совершенство технологий или законодательства, а внутренняя угроза, исходящая от сотрудников компаний и банков.

ВИКТОРИЯ ЗАВЬЯЛОВА

информацией о гражданах. «Возрос не только спрос на защиту соответствующих приложений, работающих с такими данными, но и внимание контролирующих органов к выполнению положений этого документа, что отродно», — отмечает Владимир Мамыкин. — Что касается технологий Microsoft, которые потребители могут использовать для выполнения требований этого закона, то их спектр очень широк, он охватывает большинство наших продуктов. Хотя, вне всякого сомнения, повышенным спросом для этих целей у потребителей пользуются сертифицированные в ФСТЭК и ФСБ по требованиям российского законодательства продукты — от операционных систем до офисных приложений и баз данных».

ТРЕБОВАНИЯ БУДУТ ЗАВТРА Что касается ужесточения требований к работе самих компаний, то здесь, как всегда, строгость российских законов сводится к нет необходимости их исполнения. Участники рынка, может, и рады бы выполнить, но пока не могут. Закон не содержит конкретных требований. В нем, например, говорится, что для защиты информации организация должна принимать необходимые технические меры. В том числе использовать шифровальные (криптографические) средства, «чтобы защитить персональные данные от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения». А какими именно должны быть эти средства, не сказано. Эти требования должна сформулировать Федеральная служба по техническому и экспортному контролю (ФСТЭК) Министерства обороны РФ, но когда это будет сделано, неизвестно: в Минобороны от комментариев на эту тему отказались. Пока же основным документом, регламентирующим работу компаний, остаются «Специальные требования и рекомендации по технической защите конфиденциальной информации». Они были разработаны ФСТЭК еще в 2002 году, в них описываются и меры по технической защите персональных данных, но многие из этих мер уже утратили актуальность.

Так что большинство компаний в ожидании указаний сверху используют прежние системы защиты данных. «С технической точки зрения мы готовы к тем требованиям, которые накладывает на нас закон», — говорит пресс-секретарь МТС Ирина Осадчая. — У нас гибкая инфраструктура, и мы давно работаем с системами защиты данных. Вместе с тем, пока уполномоченным контрольным органом не разработаны необходимые критерии, мы не можем провести оценку того, насколько наши системы защиты соответствуют требованиям закона».

АБОНЕНТ В ЗАКОНЕ Статья 9 закона («Согласие субъекта персональных данных на обработку персональных данных») предусматривает необходимость получения письменного согласия клиента на передачу сведений о нем третьему лицу. В ней же приведено шесть необходимых ус-

КАК ВСЕГДА, СТРОГОСТЬ РОССИЙСКИХ ЗАКОНОВ КОМПЕНСИРУЕТСЯ НЕОБЯЗАТЕЛЬНОСТЬЮ ИХ ВЫПОЛНЕНИЯ. УЧАСТНИКИ РЫНКА, МОЖЕТ, И РАДЫ БЫ «ВЫПОЛНИТЬ», НО НЕ МОГУТ — ПО НЕ ЗАВИСЯЩИМ ОТ НИХ ПРИЧИНАМ