ловий для оформления такого согласия. Компании-операторы мобильной связи вышли из положения просто. К примеру, как сообщили BG в пресс-службе МТС, с Нового года компания внесла изменения в договор. Теперь при его заключении абонент дает согласие на использование сведений о нем (в том числе третьими лицами) «в случаях, необходимых для исполнения договора».

Более сложная проблема стояла перед МГТС. Как отмечает заместитель генерального директора компании по коммерческой деятельности Денис Лобанов, на бизнесе по большому счету закон никак не отразился. Однако он косвенно сказался на обслуживании абонентов-граждан, так как теперь данные об абоненте-физлице могут включаться в систему информационно-справочного обслуживания только с его согласия. В МГТС сейчас идет реконструкция сети, часть абонентов переводится с кода 495 на код 499. «Иногда меняется не только код, но и часть номера,— отмечает Денис Лобанов.— Абоненты оповещаются о предстоящей замене и сообщают об этом близким. Но иногда кто-то из знакомых абонента не знает о смене номера, набирает старый и не может дозвониться. Тогда он обращается в справочную МГТС и просит дать новый номер телефона. Но по закону МГТС не имеет права дать такую информацию, ведь это персональные данные абонента, который добровольного согласия на их предоставление не давал».

Для выхода из этой ситуации в МГТС была введена платная услуга «Барышня, соедините» по 009. Оператор может позвонить тому, у кого сменился номер, и спросить, согласен ли абонент на соединение с человеком, который его разыскивает. В случае согласия оператор соединяет абонентов. «Однако я не уверен, что это решение, подходящее всем без исключения абонентам,— говорит Денис Лобанов.— Вместе с тем МГТС может предоставлять другим операторам связи без согласия абонентов данные, для которых установлено исключение из режима конфиденциальности. Это Ф.И.О., абонентский номер, адрес установки конечного оборудования — стационарного телефона. Эти данные необходимы в рамках межоператорских взаимоотношений, мы имеем право предоставить их на условиях конфиденциальности тому оператору, который оказал услугу абоненту МГТС».

КАК ОНИ УТЕКАЛИ Именно база данных МГТС появилась на рынке одной из первых — в 1992 году. В дальнейшем она постоянно обновлялась, и приобрести диски можно до сих пор. Регулярно крадут данные и из различных государственных ведомств. В 2002 году, к примеру, отличился Госкомстат — в продаже появилась его база, содержавшая результаты Всероссийской переписи населения. Ведомство нашло простой выход из неприятной ситуации — не признало факта утечки. А вот Центробанку не удалось так легко замять проблему с базами данных о платежах через расчетно-кассовые центры за второй и третий кварталы 2004 года. Диски появились в продаже в феврале 2005 года по цене 3 тыс. рублей. Депутаты Госдумы потребовали от Генпрокуратуры расследовать инцидент.

Однако серьезных результатов это обращение не принесло. Через несколько месяцев воры усовершенствовали продукт — в продаже появилась новая, более полная версия диска ЦБ, включавшая данные за четвертый квартал 2004 года. После этого Банк России провел наконец собственное расследование. В конце октября 2005 года в управлении безопасности ЦБ заявили, что «источник утечки перекрыт». Кто именно был ее виновником, так и осталось неизвестно. А в феврале 2006 года появились спам-сообщения с предложениями о продаже базы ЦБ за первый квартал 2005 года. Впрочем, диск не содержал информации ни об одной реальной проводке, продавцы всего лишь попытались заработать на продолжительной истории с утечками из Центробанка.

В ноябре прошлого года хитом нелегальных продаж стала база с налоговыми декларациями за 2004 год. Информацию о почти 10 млн москвичей с указанием их мест работы и адресов продавцы оценили вдвое дешевле, чем базу ЦБ,— всего в 1,5 тыс. рублей.

Пожалуй, именно после этого происшествия терпение законодателей переполнилось, и в Думу был внесен первый вариант законопроекта «О защите персональных данных». Документ вполне мог бы не дойти до последнего чтения, если бы за этой историей не последовала еще более шокирующая.

Внимание соответствующих органов привлек Московский центр экономической безопасности (МЦЭБ), который уже около года принимал на своем сайте заказы на базу паспортных данных 16 млн москвичей. Кстати, стоила эта информация недешево — $1,2 тыс. Однако никаких юридических оснований для привлечения представителей МЦЭБ к ответственности не было — продажа чужих персональных данных в России, по сути, на тот момент еще являлась легальным бизнесом. А вот сотрудники московской паспортно-визовой службы, укравшие эту информацию, могли бы ответить по закону — если бы их нашли. Аналогичная история произошла с данными на московских и петербургских клиентов «большой тройки» — «Вымпелкома», МТС и «МегаФона». Информация предлагалась на сайте sherlok.ru. Провели расследование, задержали семерых подозреваемых, в том числе сотрудников «Вымпелкома». А сайт благополучно существует по сей день — ответственность за продажу личной информации ввел лишь закон о персональных данных.

ВНУТРЕННЯЯ УГРОЗА Впрочем, утечки информации из МГТС и компаний-операторов мобильной связи были цветочками по сравнению с тем, что произошло в августе 2006 года. На черный рынок поступили сразу две базы данных (700 тыс. и 3 тыс. записей), содержащие кредитные истории людей, бравших потребительские кредиты в нескольких российских банках, в частности в Хоум Кредит энд Финанс Банке, банке «Русский стандарт» и Финансбанке. Они включали фамилию, имя, отчество и адрес заемщика, название торговой сети, где приобретались товары, размер и срок кредита, ежемесячный платеж и размер просрочки.

В начале апреля нынешнего года депутат Госдумы Анатолий Аксаков заявил, что это фальшивка. Когда СМИ сообщили о появлении в продаже баз заемщиков банков, он обратился с запросом в правоохранительные органы. «В ответ мне было сказано, что было проведено специальное расследование МВД и соответствие тех данных, которые продавались, реальным не выявлено»,— сообщил Анатолий Аксаков. Не подтвердили факт утечки и сами банки, проводившие внутреннее расследование. Однако тогда, в августе 2006-го, обзвон журналистами Ъ заемщиков, указанных в базе, подтвердил, что данные настоящие.

В середине марта этого года Банк России отреагировал на прошлогодние скандалы — разослал письма с предупреждениями о грядущих проверках уровня информационной безопасности, то есть мер защиты от утечки конфиденциальной информации, в первую очередь о клиентах. В стандарте ЦБ «Обеспечение информационной безопасности организаций банковской системы РФ», утвержденном распоряжением ЦБ №Р-27 от 26 января 2006 года, указывается, что наибольшими возможностями для того, чтобы устроить утечку информации, обладает персонал банка. Кстати, как показало исследование «Внутренние ИТ-угрозы в банковском секторе 2005», проведенное компанией Infowatch, банкиры с мнением ЦБ согласны: 54% опрошенных считают, что основная причина утечки — халатность сотрудников. В стандарте ЦБ приводятся конкретные рекомендации по защите от инсайда, в том числе регламентируются методики моделирования угроз утечки данных, политика и система управления информационной безопасностью, а также требования к программным средствам внутреннего контроля. Впрочем, эти требования носят рекомендательный характер, исполнять их необязательно. ■

В МГТС ВВЕДЕНА ПЛАТНАЯ УСЛУГА «БАРЫШНЯ, СОЕДИНИТЕ» ПО 009. ОПЕРАТОР МОЖЕТ ПОЗВОНИТЬ ТОМУ, У КОГО СМЕНИЛСЯ НОМЕР, И СПРОСИТЬ, СОГЛАСЕН ЛИ ТОТ НА СОЕДИНЕНИЕ С ЧЕЛОВЕКОМ. В СЛУЧАЕ СОГЛАСИЯ ОПЕРАТОР СОЕДИНЯЕТ АБОНЕНТОВ

НЕКОТОРЫЕ ТРЕБОВАНИЯ ЗАКОНОВ ЗАПАДНЫХ СТРАН К ИТ-БЕЗОПАСНОСТИ

Закон SB 1386 (Калифорния, США)
Секция 2 (a): «Любая организация, которая владеет персональными компьютерными данными или лицензирует их, обязана оповестить всех резидентов штата Калифорния об утечке или потенциальной утечке их приватных данных в незашифрованном виде. Сделать это следует немедленно — сразу же после того, как утечка будет выявлена».

Data Protection Directive (Евросоюз)
Статья 17 секция VIII глава 2: «Персональные данные должны быть защищены разумными средствами безопасности от таких угроз, как утрата или неавторизованный доступ, разрушение, использование, модификация или утечка».

Data Protection Act (Великобритания)
Приложение 1 часть 2 пункт 9: «Каждая организация должна реализовать разумные технические меры, чтобы предотвратить ущерб своих клиентов в результате неавторизованной или незаконной обработки персональных данных, а также их потери, уничтожения или повреждения. Вдобавок каждая организация должна сделать разумные шаги, чтобы обеспечить надежность любого служащего, имеющего доступ к персональным данным».

Personal Information Protection Act 2003, PIPA (Япония)
Статья 21: «Когда организация, на попечении которой находится персональная информация, использует служащих для обработки этих данных, она должна внедрить необходимые и адекватные меры наблюдения и контроля, чтобы обеспечить безопасность персональной информации».

The Federal Privacy Act или Privacy Act 1988 (Австралия)
Принцип 4: «Каждая организация, на попечении которой находятся личные сведения граждан, должна убедиться, что эта информация защищена от утечки, потери, неавторизованного доступа, использования, модификации и другого злоупотребления. Кроме того, организация обязана предусмотреть средства контроля над тем, чтобы доступ к информации и полномочия по ее использованию имели только те работники, которым это необходимо в силу служебных обязанностей».

Personal Information Protection and Electronic Document Act, PIPEDA (Канада)
Приложение 1 принцип 4: «Каждой организации, на попечении которой находятся персональные данные граждан, рекомендуется назначить ответственное лицо, которое будет следить за безопасностью этой информации и соблюдением положений приватности». Пункт 4.7: «Каждой организации рекомендуется принимать меры безопасности для защиты приватной информации в соответствии с характером ее чувствительности».
Пункт 4.7.1: «Эти меры безопасности должны защитить персональные данные от утечки, потери или кражи, неавторизованного доступа, копирования, использования или модификации».

АЛЕКСЕЙ ДОЛЯ

ПОДЗАКОННЫЕ СТРАНЫ

За последние годы законодательная база многих государств эволюционировала в сторону улучшения защиты персональных данных граждан. Практически каждая страна имеет нормативные акты, регулирующие оборот приватных сведений граждан и защищающие личную информацию от утечки, разглашения, неавторизованного использования и т. д. Область действия таких законов включает в себя абсолютно все организации, действующие на территории страны. При этом основная цель — предотвратить утечку и злонамеренное использование личной информации граждан. Бизнесу самому по себе невыгодно допускать утечку персональных данных. Например, согласно последнему исследованию Forrester Research, в ходе которого было опрошено 28 компаний, допустивших утечки в последнее время, каждая украденная запись о клиентах фирмы обходится ей в $90–305. Наибольшая часть этого ущерба приходится на потерю репутации, отток лояльных клиентов и трудности в привлечении новых клиентов. Казалось бы, зачем нужны законы, если компаниям невыгодно допускать утечки? Оказывается, существуют государственные организации, а также целый ряд коммерческих компаний, успех которых практически не зависит от имиджа и привлечения новых клиентов. Такие организации представлены в основном в секторах со слабой конкуренцией. Например, даже если госструктура допустит утечку информации, покинуть ее, перейдя к конкуренту, граждане не смогут. Таким образом, чтобы исключить безалаберное отношение к персональным данным даже в таких предприятиях со слабой конкуренцией, государства возводят защиту приватных сведений в ранг закона.

Наибольшие трудности в этом отношении испытывают крупные организации, ведущие операции на рынках нескольких стран. В этом случае бизнесу приходится иметь дело с требованиями сразу целого ряда законов. Отметим, что помимо этих законов практически в каждой стране существуют специализированные нормативные акты, действие которых распространяется на компании, работающие в определенных секторах экономики. Например, в США закон HIPAA требует от организаций защищать приватные медицинские сведения граждан, а закон GLBA предписывает обеспечить безопасность приватных финансовых записей.

На первый взгляд сам факт существования закона о приватности должен устрашающе действовать на представителей бизнеса и заставлять их очень бережно обращаться с персональными данными клиентов. Однако на практике законы часто дают сбои.

Японский закон PIPA (Personal Information Protection Act 2003) был принят в 2003 году, а в начале 2007 года прокуратура не смогла его применить в реальном судебном разбирательстве. Дело обстояло следующим образом. Хирофуми Йокояма, инсайдер из полиграфического и электронного гиганта Dai Nippon Printing, украл винчестер с приватными данными (именами, адресами, телефонами и номерами кредитных карт) почти 9 млн граждан летом 2006 года. Прежде чем полиция задержала инсайдера, он успел продать часть добытых сведений. Пострадали клиенты 43 компаний, в том числе Toyota Motor Corp., American Home Assurance, Aeon Co. и NTT Finance. Когда дело дошло до суда, обвинение не смогло инкриминировать инсайдеру нарушение закона PIPA. И его обвиняют лишь в краже винчестера стоимостью $200. По мнению экспертов InfoWatch, это показательный случай. Так что ожидать скорой отдачи от российского закона «О персональных данных» не приходится.

Между тем не все так плохо. Примером в области защиты приватности может служить Великобритания. Национальный закон о приватности уже много раз доказывал свою состоятельность. Например, в начале 2006 года служащие Гранд Отеля в Брайтоне выбросили в мусорный бак тысячи бумажных документов с именами, адресами, номерами кредитных карт, телефонными номерами и подписями постояльцев гостиницы. Когда об этом стало известно, вопросы к руководству Гранд Отеля возникли даже у членов британского парламента. Компанию обвинили в нарушении закона DPA (Data Protection Act), она долго извинялась и компенсировала ущерб пострадавшим.

Крупные утечки персональных данных практически всегда приводят к многомиллионным убыткам для организации. Даже если у властей нет действенного инструмента в виде закона о приватности, они всегда могут найти повод придраться к фирме и оштрафовать ее. Скажем, в США все еще нет единого федерального закона, но власти могут обвинить фирму в недобросовестной конкуренции, нарушении отраслевых нормативных актов, а также закона о защите прав потребителей. По мнению аналитического центра InfoWatch, закон о защите прав потребителей действительно очень часто спасает обвинение в зале суда, так как утечка персональных данных может привести к нарушению некоторых его положений.

АЛЕКСЕЙ ДОЛЯ