ПОДЗАКОННАЯ ПЕРСОНА

СО СЛЕДУЮЩЕГО ГОДА ОПЕРАТОРЫ СОТОВОЙ СВЯЗИ БУДУТ ИСПОЛЬЗОВАТЬ ЕДИНУЮ ТЕХНОЛОГИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ АБОНЕНТОВ. УТЕЧКИ ИНФОРМАЦИИ, ПО МНЕНИЮ СПЕЦИАЛИСТОВ, СКОРЕЕ ВСЕГО, НЕ ПРЕКРАТЯТСЯ, НО ВОЗРАСТЕТ КОЛИЧЕСТВО ПРЕТЕНЗИЙ К ОПЕРАТОРАМ СО СТОРОНЫ АБОНЕНТОВ. КЛАВДИЯ БОЛЬШАКОВА

С января 2010 года в силу вступает требование закона «О персональных данных», согласно которому все компании, имеющие дело с информацией о гражданах, должны обеспечить защиту этой информации на основе единого стандарта. Закон регулирует отношения, связанные с обработкой персональных данных (ПД): условия обработки, права абонента, обязанности оператора, меры по обеспечению безопасности ПД, контроль и надзор за обработкой информации, ответственность за нарушение требований законодательства.

Правительство РФ утвердило положение об обеспечении безопасности ПД. ФСТЭК России и ФСБ России разработали и утвердили требования и рекомендации, касающиеся обеспечения безопасности ПД в вопросах, отнесенных к их компетенции.

Для реализации мер по защите ПД абонентов «большая тройка» сотовых операторов (МТС, «Вымпелком», «МегаФон») и Инфокоммуникационный союз (ИКС) привлекли компанию ReignVox. Эта компания будет разрабатывать первый отраслевой стандарт защиты ПД для операторов связи. ИКС выступает не только в роли заказчика, но и координирует работу всех участников проекта.

Таким образом, будут выработаны общие для всех телекоммуникационных компаний правила. «Для приведения своих систем в соответствие требованиям законодательства операторы вынуждены модернизировать свои системы защиты данных, что связано с определенными финансовыми затратами. Стоимость модернизации определяется для каждого оператора индивидуально и зависит от того, насколько высокий уровень защищенности имеют его информационные системы», — говорит Генеральный директор компании ReignVox Андрей Коробицын. По его словам, компании, которые всегда уделяли должное внимание вопросам обеспечения информационной безопасности, смогут ограничиться лишь применением необходимых организационных мер по защите и разработке корпоративной документации. Однако затраты компаний, осуществляющих обработку большого объема ПД граждан и до сих пор не предпринявших никаких мер по обеспечению информационной безопасности, могут составлять миллионы рублей, считает господин Коробицын.

PHOTOXPRESS

КУПИТЬ ВОРОВАННУЮ БАЗУ ДАННЫХ СТАЛО СЛОЖНЕЕ С ТЕХ ПОР, КАК ЕЕ ПРОДАВЦОВ СТАЛИ ПРЕСЛЕДОВАТЬ

ЧЕРНЫЕ БАЗЫ Несколько лет назад свежие БД с паспортными данными абонентов сотовых операторов можно было легко найти на радиорынках. С тех пор ситуация изменилась. Но и теперь при определенном желании эту информацию найти можно, утверждает адвокат юридической компании «Усков и партнеры» Вадим Усков. Генеральный директор SecurIT Алексей Раевский замечает, что информацию стало сложнее найти из-за того, что преследуют продавцов информации. Но спрос на ПД абонентов меньше не стал — существует множество сайтов, которые за предоплату от 500 рублей до нескольких тысяч якобы могут прислать информацию об абоненте, детализацию счета или даже распечатку SMS-сообщений. Правда, никто не может поручиться, что чересчур любопытного клиента не обманут.

Хотя иногда и не обманывают. Операторы не раз фиксировали случаи, когда сотрудникам компании предлагали деньги за распечатку SMS или детализацию счета того или иного абонента. Впрочем, уговорить удается далеко не всех, так как разглашение конфиденциальной информации может обернуться для сотрудника не только увольнением с работы, но и уголовной ответственностью.

Пресс-секретарь МТС Ирина Осадчая отмечает, что для сотрудников ответственность за разглашение ПД высокая — от административной до уголовной в зависимости от ущерба. «Если мы выявляем факты неправомерного доступа, на сотрудника может быть наложено дисциплинарное взыскание вплоть до увольнения. Если данные несанкционированно переданы третьему лицу, может быть возбуждено уголовное дело»,— рассказывает госпожа Осадчая.

Андрей Коробицын также замечает, что в случае нарушения установленного законом порядка сбора, хранения, использования или распространения информации о гражданах влечет предупреждение или наложение административного штрафа. А вот неправомерный доступ к охраняемой законом компьютерной информации наказывается гораздо серьезнее: от штрафа в размере до двухсот тысяч рублей до лишения свободы на срок до двух лет.

ОПЕРАТОРСКИЙ ИНСАЙД Но случаи хищения информации тем не менее случаются. По словам партнера юридической компании Salans Виктора Наумова, «источников утечки может быть три: сотрудники операторов, хакеры и сотрудники правоохранительных органов». С ним согласен и адвокат юридической компании «Усков и партнеры» Вадим Усков, отмечающий, что возможно и распространение информации без согласия ее владельца через интернет. Андрей Коробицын отмечает, что чаще всего хищение информации обусловлено умышленными действиями и реже небрежностью или халатностью персонала, отвечающего за защиту информации. «Большинство работодателей уверены, что их собственные сотрудники представляют для сохранности защищаемых данных куда большую угрозу, чем хакеры и прочие злоумышленники, действующие извне. Согласно статистике, внутренний персонал компаний виновен в 75% случаев утечки информации, в то время как действующие извне хакеры виноваты лишь в 1% таких случаев», — замечает господин Коробицын.

ПРОБЛЕМЫ АБОНЕНТА Если ПД распространяются без согласия абонента, то прежде всего нарушается его конституционное право на частную жизнь. Но этой неприятностью дело не ограничивается. Базы данных сотовых операторов используются в основном для того, чтобы проводить спам-рассылки. Это может быть реклама товаров или услуг, а может быть SMS с просьбой положить денег на телефон.

Абонентом могут заинтересоваться мошенники и посерьезнее. Например, позвонить и рассказать, что кто-то из близких попал в милицию и, чтобы его оттуда вызволить, нужно принести определенную сумму в назначенное место. Иногда люди верят и отдают деньги.

Бывали случаи, когда отцу семейства звонили и говорили, что его сын сбил пешехода и для решения проблемы без уголовного дела нужно заплатить $5 тыс. Отец срочно собирал деньги и отдавал их, но позже выяснялось, что его обманули. Бывает, когда мошенники говорят, что сын или дочь задержаны с наркотиками. Иногда мошенники звонят, представляются работниками банка и пытаются выяснить PIN-код кредитной карты.

ДАННЫЕ ПОД ЗАМКОМ? Сотовые операторы уверены, что сейчас данные их пользователей защищены достаточно надежно и что вступление закона в силу не отразится серьезно на их деятельности. Пресс-секретарь «Вымпелкома» Екатерина Осадчая говорит, что «речь идет не о внедрении чего-то нового». Ирина Осадчая отмечает, что в МТС действует политика информационной безопасности, а также реализован комплекс организационно-технических мер, направленных на защиту информации об абонентах. По словам госпожи Осадчей, в компании работает подразделение, которое отвечает за организацию защиты, и разработаны регулирующие документы, позволяющие разграничивать доступ к информации, проводить мониторинг и контроль выполнения порядка использования технических средств. «Доступ к персональной информации имеют только сотрудники, которые уполномочены выполнять операции с базами данных: сотрудники офисов продаж, контактных центров, служб маркетинга, абонентского обслуживания, ИТ. В компании действует режим коммерческой тайны и защиты информации. Сотрудники заключают соглашение о неразглашении информации, к которой они получают доступ»,— говорит госпожа Осадчая.

По мнению Ирины Осадчей, законодательство внесет изменения главным образом в технические требования к системам защиты персональной информации: они станут более четкими. PR-директор компании «Микротест» Олег Плотников напоминает, что операторы сотовой связи являются одними из наиболее технологически развитых компаний. «Вопросы защиты ПД абонентов решаются на высоком уровне. При этом учитываются все необходимые аспекты в отношении автоматизированной обработки и предотвращения крупномасштабных утечек. В этих компаниях в той или иной мере развернуты требуемые системы защиты данных: системы контроля и предотвращения утечек, ретроспективного анализа инцидентов и другие»,— рассказывает господин Плотников. Главный вопрос, по его мнению, заключается в том, насколько эти меры являются достаточными: российский и зарубежный опыт показывает, что стопроцентно эффективных систем защиты не существует и утечки информации все равно будут.

АБОНЕНТ ВСЕГДА ПРАВ По мнению экспертов, в будущем реакция абонентов сотовых операторов на разглашение их ПД станет более острой, что может привести к увеличению издержек компании. Олег Плотников считает, что будут попытки привлечения операторов к ответственности хотя бы за счет нарастающего «потребительского экстремизма». «Тем не менее,— отмечает он,— судебная перспектива подобных дел пока не ясна. Поэтому крупным компаниям не стоит опасаться ни возможных выплат компенсации абонентам, ни появления новых рейдерских схем, связанных с проверками защищенности обработки ПД. Но возрастание издержек из-за воздействия регулирующих органов все-таки возможно».

Олег Плотников подчеркивает, что важна реакция на утечки со стороны государства. Если меры по расследованию утечек будут эффективными, а репутационные и финансовые издержки из-за утечек высокими, то вложения в обеспечение безопасности со стороны компаний станут оправданными. Андрей Коробицын также говорит, что закон о персональных данных позволяет обжаловать действия или бездействие оператора в суде либо Федеральной службе по надзору в сфере связи и массовых коммуникаций (Россвязькомнадзоре).

Это ведомство является уполномоченным органом по защите прав субъектов ПД. Россвязькомнадзору предоставлены права на обращение в суд в защиту интересов граждан. Ведомство также может обращаться в лицензирующий орган с просьбой рассмотреть вопрос о приостановлении действия или аннулировании лицензии. Россвязькомнадзор также может направлять материалы для привлечения к уголовной либо административной ответственности в прокуратуру.

Закон «О персональных данных» не описывает мер ответственности, которые могут быть применены к гражданам, организациям, органам государственной власти, органам местного самоуправления за несоблюдение законодательства. Закон отсылает к другим нормативным актам, предусматривающим разные меры ответственности. К таким мерам можно отнести ликвидацию юридического лица, привлечение к административной или уголовной ответственности, компенсацию морального вреда и другое. Инициатором привлечения к ответственности могут выступить Россвязькомнадзор, ФСБ, ФСТЭК, уполномоченные осуществлять мероприятия по контролю и надзору и составлять протоколы об административных правонарушениях в сфере ПД. «Решение о ликвидации организации может быть принято судом при грубых или неоднократных нарушениях законодательства», — говорит господин Коробицын.

НЕСВОЕВРЕМЕННЫЙ ЗАКОН Помимо сотовых операторов работой с ПД граждан занимаются и другие компании. В основном это государственные и муниципальные учреждения: институты, школы, больницы, поликлиники. Таких компаний в России более 870 тыс. В связи с этим в конце января в рамках «Инфофорума-11», посвященного вопросам информационной безопасности России, мнения по поводу срока выполнения закона разделились. Представители Государственной думы (ГД) и Института законодательства сравнительного правоведения при правительстве РФ считают, что закон и все его акты нуждаются в серьезной доработке. По их мнению, требования регуляторов должны быть открытыми и пройти регистрацию в Минюсте. ГД предлагает отсрочить вступление в силу ФЗ «О персональных данных», ведь поправки к нему могут быть выпущены не раньше третьего квартала 2009 года.

Регуляторы и интеграторы придерживаются противоположной точки зрения. Они согласны с тем, что в законе есть неточности, но считают, что это не должно отразиться на его исполнении. В течение 2009 года могут быть внесены небольшие поправки в требования регуляторов, но серьезных изменений, скорее всего, не будет. Проверки начнутся с января 2010 года, а сама методика их проведения будет разработана к четвертому кварталу 2009 года. ■