ВСКОЛЫХНЕТ ЛИ ВТОРУЮ ВОЛНУ МИРОВОГО КРИЗИСА ТОНУЩЕЕ «ДУБАЙСКОЕ ЧУДО»? Стр. 14

ЕЖЕНЕДЕЛЬНЫЙ ЖУРНАЛ 30 ноября 2009

Итоги

www.itogi.ru

Андрей Костин

Худшее позади...

Интервью с президентом ВТБ. Стр. 30

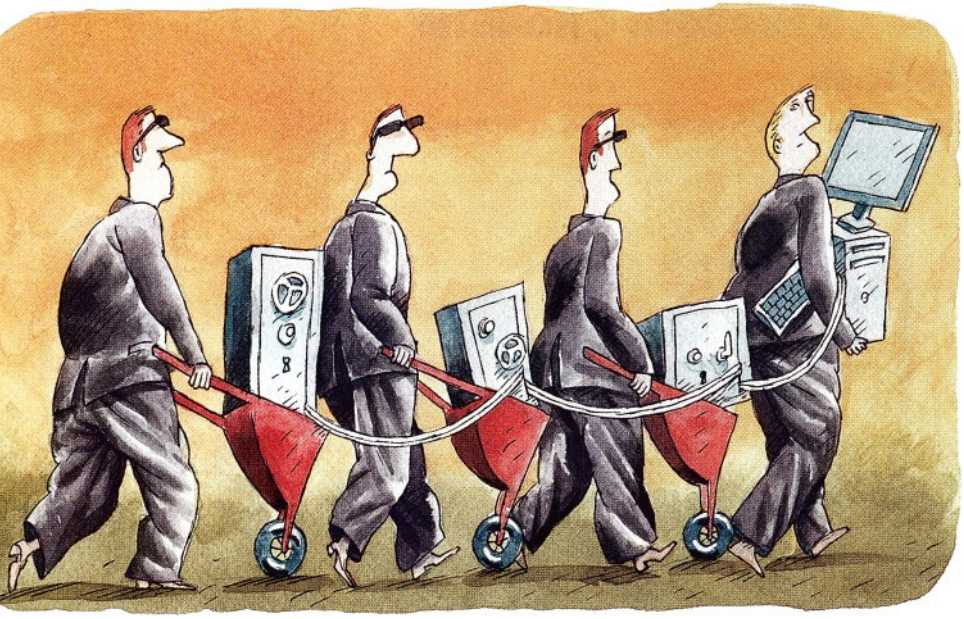
№49 (703)

Подписка на журнал «Итоги» принимается без ограничений по всей территории РФ. В розницу журнал распространяется в Москве и Московской обл., Санкт-Петербурге, Архангельске, Астрахани, Барнауле, Брянске, Владивостоке, Владимире, Волгограде, Вологде, Воронеже, Выборге, Екатеринбурге, Иркутске, Казани, Кинешме, Кирове, Костроме, Краснодаре, Красноярске, Мончегорске, Мурманске, Нерехте, Н.Новгороде, Н.Тагиле, Великом Новгороде, Орле, Перми, Пскове, Ростове, Ростове-на-Дону, Рыбинске, Рязани, Самаре, Саратове, Смоленске, Сочи, Ставрополе, Хабаровске, Шуе, Элисте, Ярославле, в странах СНГ: Азербайджане, Армении, Белоруссии, Грузии, Казахстане, Киргизии, Молдавии, Украине. Журнал можно приобрести также в Австрии, Великобритании, Венгрии, Германии, Италии, Испании, Польше, США, Финляндии, Швейцарии.

ISSN 1027-3964

9 771027 396001 49

Эх, защищу!



Персональные данные россиян еще не скоро окажутся под защитой

ТОСДУМА РФ СКЛОНЯЕТСЯ К ТОМУ, ЧТОБЫ ПЕРЕНЕСТИ еще на год срок, к которому все информационные системы предприятий, работающих с персональными данными (ПД) граждан, должны соответствовать требованиями закона № 152-ФЗ «О персональных данных». Пока не более пяти процентов операторов ПД причислили себя к этой категории. Почему, вступив в силу еще в 2007 году, закон до сих пор не может реально заработать?

По оценке Юрия Черкаса, руководителя отдела технической защиты информации компании ReignVox, сегодня есть все условия для того, чтобы операторы ПД смогли обеспечить их адекватную защиту в положенные сроки. Правда, отмечает Александр Васюнин, специалист по маркетингу компании «Информзащита», чтобы разобраться в нормативных документах, помимо глубоких технических знаний нужно обладать неплохой юридической подготовкой. Каждая система защиты ПД оказывается уникальным проектом, внедрение которого целесообразно поручить компании, уполномоченной регулятором. При этом типовых несложных решений для небольших компаний нет. Образно говоря, частный стоматологический кабинет должен заказать IT-проект на уровне небольшого банка, поскольку медицинские данные законом отнесены к специальной категории значимости. Но ведь большую часть небольших операторов ПД составляют бюджетные организации: школы, больницы, предприятия ЖКХ и т. д., а средств на реализацию закона из федерального бюджета не выделено ни в этом, ни в следующем году. Средства, между прочим, требуются немалые. По оценке Владислава Резника, председателя комитета Госдумы РФ по финансовому рынку, — на уровне 4—6 процентов ВВП. Минздравсоцразвития оценивает свои начальные потребности в 15 миллиардов рублей. А каждый из более чем тысячи банков затратит, по расчетам АРБ, в среднем по 50 миллионов рублей. Однако эти организации и без того обладают мощными средствами информационной безопасности, в том числе средствами защиты от утечек информации (DLP-системами). «Для защиты ПД могут использоваться только сертифицированные средства, — поясняет Андрей Конусов, генеральный директор LETA IT-company. — А большинство современных систем, особенно западных производителей, подобной сертификации не имеет». Соответствие закону выливается в еще один полномасштабный проект миграции информационной системы банка на новое ПО. Кроме того, некоторые нормы закона № 152-ФЗ вступают в противоречие с отраслевым законодательством, в частности с законом «О банковской тайне». А ряд других просто затрудняет основную деятельность, как, скажем, требование уничтожения ПД через три дня после того, как они были использованы. Это будет мешать банкам распознавать мошенников, предъявляющих недостоверные личные данные. Явно нужны отраслевые стандарты защиты ПД. «Для небольших бюджетных организаций нужно разработать недорогие типовые «коробочные» решения, которые с минимальными затратами можно быстро устанавливать в таких учреждениях», — говорит Андрей Конусов.

К 1 января 2010 года страна подошла с пониманием, что законодательство о защите ПД нужно сильно дорабатывать. Сегодня ФСТЭК и ФСБ определяют для оператора ПД все: от угроз и способов защиты до контроля исполнения требований. Для бюджетных организаций это оправданно. А вот для коммерческих операторов ПД целесообразнее риск-ориентированный подход, при котором сама компания берет на себя ответственность за сохранность ПД и создает (или не создает) необходимые системы защиты. Тогда смысл защиты ПД из административного требования превращается в конкурентное преимущество. В любом случае возможные риски от утечки ПД должны коррелироваться с ответственностью оператора. Пока за неисполнение закона № 152-ФЗ можно получить разве что штраф до 10 тысяч рублей, стимула к IT-проектам не будет. Настоящая забота о персональных данных только начинается. ■

Елена Покатаева

Чего не хватает для того, чтобы закон реально защищал персональные данные?

Николай Федотов, главный аналитик InfoWatch

Сегодня закон говорит предприятию: «Выполняй требования, иначе понесешь наказание», фактически просто велит ему потратить определенное количество денег. Правда, эти требования еще должны уточнить ведомства. Они же решат, как проверять выполнение требований. Не ранее чем через год после начала массовых проверок со стороны контролирующих органов станет точно понятно, как именно регуляторы трактуют «точное исполнение закона». Пока это непонятно, в том числе и им самим.

Тимур Аитов, вице-президент Ассоциации региональных банков

В законе остался ряд дыр, которые потенциально могут оказаться мощными источниками утечки ПД, например, социальные сети, электронные платежные системы — нерезиденты (около 10 миллионов паспортов клиентов). Отдельного внимания требуют системы резервирования. Так, 85 процентов данных российских авиаперевозчиков, включая «Аэрофлот», хранятся в базах зарубежных систем бронирования. То есть информация о перемещениях россиян доступна для бесконтрольного анализа.

Игорь Ляпунов, директор центра информационной безопасности «Инфосистемы Джет»

Для выполнения требований нормативной базы нужен скорее кнут, чем пряник. Но для фактической защиты ПД законодательство нуждается в определении ответственности за утечку данных. И должны заработать рыночные механизмы: когда репутационные риски, связанные с потерей данных, станут нашей реальностью, клиенты будут выбирать банк или оператора связи, думая в том числе и об отсутствии их клиентских баз на рынке или в Интернете.