УДК 347:681.324

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ: ТЕНДЕНЦИИ ОСЕНИ-2009

В. В. Ульянов, руководитель аналитического центра Perimetrix; vladimir.ulyanov@perimetrix.com

***Ключевые слова**: персональные данные, информационная безопасность, информационные системы персональных данных, сертификация, программные средства для защиты персональных данных.*

Введение. В августе 2008 г. компания Perimetrix совместно с медиа-партнерами провела специализированное исследование, посвященное проблемам защиты персональных данных (ПДн), которое привлекло внимание как специалистов по информационной безопасности (ИБ), так и представителей компаний различных отраслей. Ведь вопросы, связанные с выполнением ФЗ № 152 «О персональных данных», актуальны сегодня для всех без исключения организаций.

Цель нового исследования «Персональные данные в России 2009» — показать текущее состояние дел в области защиты ПДн и практические сдвиги, произошедшие за последний год.

Методология оценки операторов ПДн. Исследование проводилось в августе-сентябре 2009 г путем интернет-опроса 287 специалистов и руководителей преимущественно подразделений ИТ и ИБ, поскольку именно эти подразделения чаще всего назначаются ответственными за выполнение ФЗ № 152 на местах (почему так происходит — это вопрос отдельный, и к нему мы еще вернемся).

Большую часть участников исследования составили представители ИТ- и телекоммуникационных компаний (36 % общего числа), финансовых институтов (35 %). Среди прочих отраслей заметную долю составляют медицинские учреждения и органы власти (по 8 %), т. е. организации, которые работают с большим числом субъектов ПДн.

Что касается распределения операторов ПДн по масштабам бизнеса, то в опросе были представлены небольшие организации (до 100 сотрудников), средние компании и даже крупные корпорации (свыше 10 тыс. человек).

Исследование охватывало следующие вопросы:

- портрет респондента (профиль участников описан выше);
- особенности обработки ПДн (сколько данных хранится, как они защищаются, кто имеет доступ и т. д.);
- вопросы, касающиеся законодательного регулирования;
- практические аспекты защиты ПДн.

Что влияет на вероятность утечки ПДн. Внимание компаний к проблеме защиты ПДн неоднородно и зависит от целого ряда факторов. Один из важнейших — объем обрабатываемых ПДн. (По поводу того, что относить к ПДн, сломано немало копий — список только классов ПДн может занять несколько полос. Этот вопрос выходит за рамки данной статьи; примем за ПДн некий набор сведений, идентифицирующих личность.) И чем больше записей ПДн обрабатывает компания, тем выше ее ответственность за их защиту. Ведь с ростом количества записей растут и риски операторов, которые с этими записями связаны.

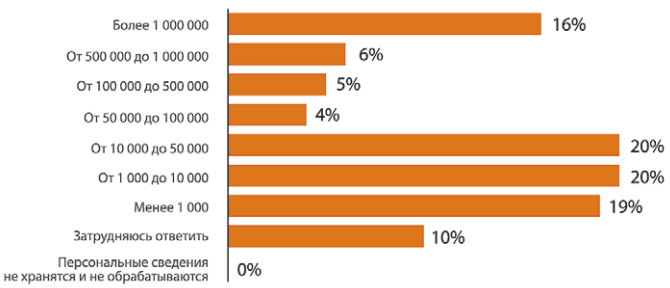

Рис. 1

На рис. 1 приведено количество записей ПДн в компаниях (сумма долей может не равняться 100 %из-за погрешностей математического округления). Из ответов видно, что свыше половины (51 %) респондентов обрабатывают ПДн более 10 тыс. человек. Последствия утечки такого количества информации могут быть весьма печальны: прямые финансовые издержки, штрафы регуляторов, ухудшение репутации, падение стоимости акций...

Следующий вопрос, непосредственно связанный с защищенностью субъектов ПДн, касается культуры обработки персональных данных. Ведь вероятность их утечки, при прочих равных условиях, тем выше, чем больше работников имеют доступ к массивам данных (на рис. 2 показано, кто имеет доступ к ПДн). В идеале такая возможность должна быть только у сотрудников службы безопасности. Однако на практике это встречается очень редко (4 %); в большинстве случаев (41 %) доступ к информации имеет и ИТ-персонал организации.

Рис. 2

ИТ-персонал — не единственная угроза безопасности ПДн. Часто доступ к информации предоставляется топ-менеджерам (18 %), ограничить в правах которых, хотя они действуют подчас весьма халатно, довольно трудно.

Что касается служб технической поддержки и call-центров, то подобные подразделения, как известно, комплектуются не самыми квалифицированными сотрудниками, отсюда высокий уровень текучести кадров. Операторы контактных центров практически всегда имеют доступ к ПДн, что необходимо им для обслуживания клиентов. Однако при грамотном подходе, в случае алгоритмизированного или с разграничением функций доступа, когда работник может лишь просматривать сведения, и то «поштучно», риски утечки относительно невелики. Базу данных миллиона человек украсть не так просто.

О нормативно-правовой защите ПДн. С момента своего принятия ФЗ «О персональных данных», нацеленный на сохранение конфиденциальности приватных данных, упорядочение процедур обработки ПДн и устранение такого явления, как общедоступные «базы» физических лиц, подвергался справедливой критике за недостаток конкретики. Совершенно не ясно было, как защищать права субъектов ПДн. Поэтому сегодня, помимо самого ФЗ № 152, существует множе-

ство подзаконных актов, правительственных постановлений и министерских приказов, также регулирующих эту сферу деятельности.

На рис. 3 показано влияние различных нормативных актов на защищенность ПДн. Рейтинг популярности здесь возглавляет, естественно, ФЗ «О персональных данных» (54%). Причем закон упрочил свое лидерство по сравнению с прошлым годом, когда у него было только 45%. Второе место, как и год назад, прочно занимают отраслевые нормативы. Напомним, что значительную часть участников исследования составляют кредитные организации — для них, в частности, важную роль играет стандарт Банка России «СТО БР ИББС», новая редакция которого вышла весной 2009 г.

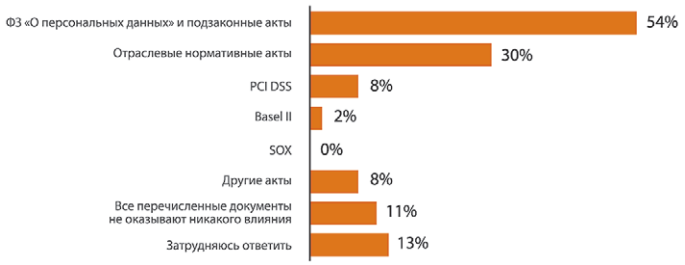

Рис. 3

Зарубежные стандарты, не имевшие большой доли и в прошлом году, еще более ослабили свои позиции. И это можно понять. Раньше, когда своих стандартов не хватало, ориентироваться приходилось на «лучшие западные практики». С развитием отечественной законодательной базы нет смысла слепо следовать чужим стандартам. Тем более что действительно лучшие из иностранных документов включаются и в отечественные нормативы. В частности, в уже упоминавшемся стандарте Банка России встречаются ссылки на ISO/IEC 17799:2005, ISO/IEC 13335—1:2004, ISO/IEC 27001:2005, CobIT и др.

Говоря о законодательном регулировании, необходимо отметить, что в нормативных актах, в частности требованиях ФСТЭК, отсутствуют в явном виде положения об обязательном использовании систем защиты данных (СЗДн) от компрометации со стороны собственных сотрудников. В то же время в большинстве документов четко говорится, что наиболее опасны именно инсайдеры — сотрудники, имеющие легальный доступ к конфиденциальным сведениям. Например, в п. 5.4. стандарта Банка России «СТО БР ИББС-1.0—2008» написано: «Наибольшими возможностями для нанесения ущерба организации БС РФ обладает ее собственный персонал... Внешний злоумышленник, как правило, имеет сообщника (сообщников) внутри организации...». Обязательность таких СЗДн, с одной стороны, можно расценить как давление на организацию, однако и польза была бы очевидной. Ведь только «полицейские» системы смогут обеспечить защиту и минимизировать риск утечки — как по злому умыслу, так и из-за халатности.

Насколько выполняются требования ФЗ «О персональных данных»? Мнение респондентов, безусловно, субъективно: пока еще очень мало организаций провели независимый внешний аудит. Тем не менее сравнение ответов участников на вопрос о соответствии их систем требованиям закона (рис. 4) с данными прошлогоднего анкетирования позволяет сделать интересные выводы.

Прежде всего бросается в глаза снижение доли (с 20% в 2008 г. до 14% в 2009 г.) «образцовых» компаний, которые соответствуют всем требованиям. Очевидно, что в компани-

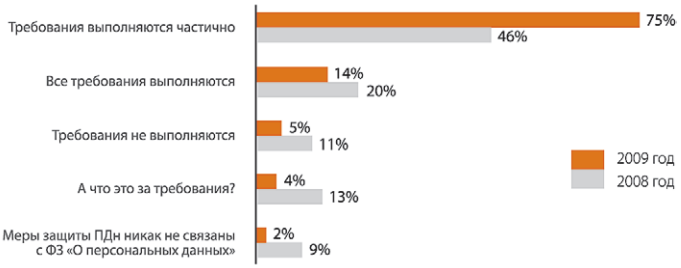

Рис. 4

ях хуже обращаться с ПДн не стали — там просто сняли «розовые очки». Нельзя не отметить и значительно возросшее (с 46 до 75%) число фирм, которые реализуют положения ФЗ № 152 частично. Как следствие, до 5% уменьшилось число организаций, вообще не выполняющих требования. А кроме того, практически пропали респонденты, считающие, что защита ПДн на практике и ФЗ «О персональных данных» никак не связаны. Эти результаты говорят о действительном улучшении дел.

Чем грозят реалии. Ознакомившись с ответами респондентов, насколько полно в их компаниях выполняются требования ФЗ № 152, подойдем к этому вопросу с другой стороны: что говорят факты, ведь общее мнение может быть и субъективным. Определить, ведутся проекты по улучшению защищенности ПДн или нет, гораздо проще — на рис. 5 приведена статистика проектов по повышению защищенности ПДн за последний год.

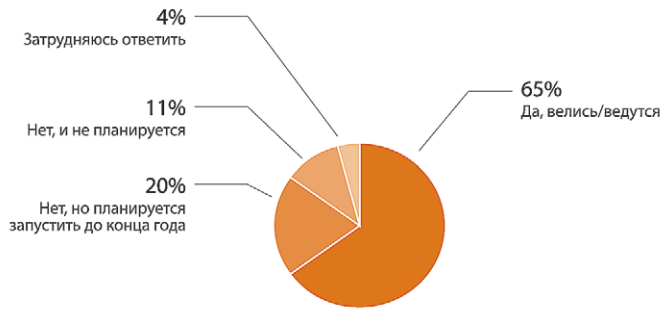

Рис. 5

Таким образом, значительная доля компаний (65%) уже реализовала на практике или внедряет подобные проекты сейчас. А что же оставшаяся треть фирм? Некоторые из них планируют заняться защитой ПДн до конца года, что неудивительно: в 2010 г. Роскомнадзор активизирует работу по проверке операторов. В то же время часть организаций вообще не собирается запускать проекты, связанные с ПДн.

Основные препятствия на пути реализации проектов в сфере защиты ПДн представлены на рис. 6.

Главная проблема — отсутствие квалифицированных кадров. Здесь, наверное, стоит вернуться к заданному в начале статьи вопросу о том, почему ФЗ № 152 занимаются специалисты по ИТ и ИБ. Ведь ПДн совсем не обязательно обрабатываются в электронных системах — случаются утечки и на бумажных носителях. И меры защиты ПДн не ограничиваются техническими решениями, но включают также организационные и правовые моменты. Однако, как можно предположить, заниматься ПДн просто некому. Не будет же юрист или разработчик корпоративных регламентов думать о том, как, скажем, «прикрутить» к базе клиентов какое-нибудь шифрование. В то же время айтишник должен иметь в виду и юридические аспекты, и новую анкету для клиентов, в которой будет

Рис. 6

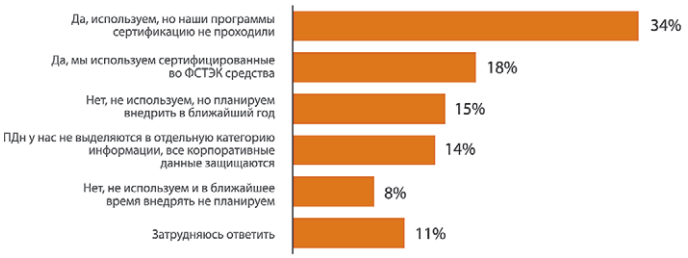

Рис. 7

пункт о том, что физическое лицо предоставляет компании право обрабатывать свои ПДн. И все же приходится констатировать: большинство нынешних специалистов по защите ПДн, независимо от образования, самоучки. Профессионалов или хотя бы опытных сотрудников, прошедших несколько тренингов, катастрофически не хватает.

Еще один практический вопрос затрагивал тему программных средств, используемых для защиты ПДн (рис. 7). Что применяют фирмы, хотя бы частично соответствующие ФЗ № 152? Как выяснилось, доля сертифицированных в ФСТЭК средств довольно мала (18%). Причин тому несколько. Конечно, это и «естественные» сложности — нехватка бюджета, недостаточная расторопность исполнителей и т.д. Однако часть вины лежит и на вендорах: спрос опережает предложение.

Процесс сертификации программы в ФСТЭК весьма сложен и продолжителен. Не все производители успели вовремя сертифицировать свои решения. Скажем, первый антивирус получил сертификат ФСТЭК только в середине октября 2009 г. (см. *www.fstec.ru*).

Другой аспект проблемы связан с тем, что информационные системы, обрабатывающие ПДн (ИСПДн), делятся на классы: К4–К1. И не всякое сертифицированное решение (в отличие, например, от Perimetrix SafeSpace) подходит для использования во всех ИСПДн. Стоит оговориться, что в ответах на данный вопрос различия в классах сертификатов не делались. Тем не менее большинство организаций пока использует несертифицированные, в том числе самописные, средства. А часть фирм при защите ПДн вообще обходится без каких-либо программных продуктов.

Заключение. Какие же подвижки произошли в 2009 г.? Прежде всего это рост числа компаний, которые занялись систематизацией ПДн (65%). Трудностей тоже немало: нехватка квалифицированного персонала, бюджетные ограничения, недостаток сертифицированных средств.

Заинтересованность в действии закона демонстрирует государство. Как всегда, не обходится без случаев административного рвения, как, например, публичное привлечение к ответственности мэра одного из городов Пермского края за разглашение ПДн неплательщиков коммунальных платежей.

Однако все свидетельствует о том, что работа в направлении защиты ПДн — не временный популистский проект, а выходит в разряд действительно важных задач. Согласно планам Роскомнадзора на 2010 г., количество проверок по поводу исполнения ФЗ № 152 возрастет в разы, а это значит, что и компании будут заниматься этим вопросом более плотно.

В прошлые годы, когда ФЗ «О персональных данных» только приняли, основной темой разговоров вокруг него было то, что закон есть, но он не работает. Постепенно выходили уточняющие подзаконные акты, и сегодня можно констатировать: закон заработал. Наверное, это главное.

Получено 18.11.09