



О.А. ФОХТ,

старший научный сотрудник Института программных систем им. А.К. Айламазяна РАН,
г. Переславль-Залесский, Россия, oaf@interin.ru

АНАЛИЗ ПРИНЯТЫХ ПОПРАВК К ФЕДЕРАЛЬНОМУ ЗАКОНУ №152-ФЗ «О ПЕРСОНАЛЬНЫХ ДАННЫХ»

УДК 61:658.011.56

Фохт О.А. Анализ принятых поправок к Федеральному закону №152-ФЗ «О персональных данных» (Учреждение Российской академии наук Институт программных систем им. А.К. Айламазяна РАН, г. Переславль-Залесский, Россия)

Аннотация: Большой пакет поправок к Федеральному закону №152-ФЗ «О персональных данных» вступил в силу 27 июля 2011 г. В статье анализируются принятые изменения Закона и рассматриваются отдельные наиболее интересные для применения в медицинских информационных системах положения.

Ключевые слова: персональные данные, защита персональных данных, информационная безопасность, информационные системы, медицинские информационные системы, внедрение информационных систем

UDC 61:658.011.56

Vogt O.A. State-of-the-Art Review on amendments to the law «On personal data protection» (Program Systems Institute, RAS, Pereslavl-Zalessky, Russia)

Abstract: The amendments to the Law «On personal data protection» were inured on 27.07.2011. Article gives the amendments to the Law state-of-the-art review. It considers a number of the positions most interesting to application in healthcare information systems.

Keywords: personal records, personal data protection, information security, information systems, healthcare information systems, information system deployment

В 4-м номере журнала «Врач и информационные технологии» опубликована статья «Динамика формирования и текущее состояние требований по защите персональных данных пациентов», рассказывающая об истории формирования требований по защите персональных данных применительно к медицинским информационным системам. В статье упоминалось об ожидании в скором времени принятия поправок к 152-ФЗ, и вот 27 июля 2011 года изменения в Федеральный закон № 152-ФЗ «О персональных данных» [1] были внесены и вступили в силу. В сегодняшней статье анализируются принятые поправки и рассматривается ряд наиболее интересных для применения в медицинских информационных системах положений обновленного Закона.

Сам закон «О персональных данных» [2] был принят еще в 2006 году и вызвал массу вопросов и споров в широких кругах. Вступление 152-ФЗ в силу повлекло выпуск целого ряда подзаконных актов и нормативных документов, регулирующих защиту персональных данных, которые неоднократно менялись и уточнялись [3]. Претензии и замечания социума к закону в конце 2009 года оформились в солидный пакет поправок [4], предложенных депу-

© О.А. Фохт, 2011 г.



татом Государственной Думы Резником В.М. (Проект № 282499-5). Поправки обсуждались и находились на рассмотрении более полутора лет, и вот, наконец, спорный Закон получил новую форму (изменено более 70% текста).

Надо отметить, что поправки приняты совсем не в том виде, в котором подавались. Так, например, весьма характерным для всего пакета «поправок Резника» предложением было свести случаи обработки персональных данных (а в исходном тексте 152-ФЗ перечислено 7 случаев обработки, не считая «с согласия субъекта» и специальных категорий) к трем универсальным: обязательная по требованиям федеральных законов (особенности обработки определяются законами), в ходе реализации договорных отношений (особенности обработки определяются договорными отношениями) и в личных целях. В принятом же сейчас тексте Закона количество случаев обработки, напротив, увеличилось до 11, и идея определять требования к защите персональных данных договоренностями между оператором и субъектами принята не была. Остались в тексте и противоречия, и невыполнимые требования, просматриваются интересы отдельных госструктур и выделенных направлений деятельности.

Так или иначе, поправки приняты и, вероятно, в таком виде Закон просуществует уже длительное время, что позволит руководствоваться им в работе, не оглядываясь на неустойчивость нормативной базы. Возможно, в связи с принятием новой редакции Закона будут пересмотрены и соответствующие нормативные акты. Но может быть этого и не произойдет, так как, несмотря на объем поправок по тексту, принципиальных изменений не так уж и много — в основном принятые изменения уточняют формулировки и выводят отдельные частные случаи из-под «общих» требований закона. В частности, положение об установлении определенных Правительством РФ уровней защищенности и требований к защите персональных данных

при их обработке в информационных системах персональных данных, исполнение которых эти установленные уровни защищенности обеспечивает, осталось. В то же время, ряду структур и ведомств дано право определять угрозы безопасности персональных данных с учетом своей специфики, что делает полностью легитимными как методические указания Минздравсоцразвития по обеспечению информационной безопасности в медицинских информационных системах [5], так и типовую модель угроз, разработанную Минздравсоцразвития для ЛПУ [6].

Требование про обеспечение информационной безопасности «применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации» в Законе также осталось. Это относится к продуктам, позиционирующим себя в качестве средства защиты информации — они должны иметь сертификаты. При этом следует иметь в виду, что сертифицируются заявленные возможности средства по защите данных. Так, например, наличие сертификата у «антивирусного средства» не сделает возможным его использование в качестве сертифицированного межсетевого экрана, несмотря на то, что МЭ будет входить в его состав.

В новой редакции 152-ФЗ хочется отметить наиболее интересные, с точки зрения применения в медицинских информационных системах, положения:

1. Оператор до начала обработки персональных данных обязан уведомить уполномоченный орган о своем намерении осуществлять их обработку. Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 года, обязаны представить уведомления, не позднее 1 января 2013 года.

2. Уведомление не требуется в случаях обработки данных в соответствии с трудовым законодательством (отделы кадров); получения и использования данных в связи с заключением договора, стороной которого является субъект персональных данных; обработки





общественным объединением или религиозной организацией информации о членах организации; обработки персональных данных, содержащих только ФИО; обработки в целях однократного пропуска субъекта на охраняемую территорию; а также в специальных случаях, предусмотренных законодательством Российской Федерации (здесь речь идет в основном о противодействии правонарушениям и терроризму).

3. Оператор обязан назначить лицо, ответственное за организацию обработки персональных данных, которое будет осуществлять внутренний контроль соблюдения требований к защите информации, доводить эти требования до сведения сотрудников, организовывать прием и обработку обращений и запросов субъектов персональных данных. Сведения об указанном лице подаются оператором в составе уведомления об обработке персональных данных.

4. Если персональные данные получены не от субъекта персональных данных, оператор, за исключением некоторых специальных случаев, до начала обработки таких персональных данных обязан уведомить субъекта о намерении их обработки.

5. Согласие субъекта персональных данных на их обработку принимается только в письменном виде или в виде электронного документа, сопровождаемого ЭЦП (в «поправках Резника» предлагался вариант присоединения — например, путем выставления соответствующей отметки «Согласен» на сайте, но этот вариант не прошел), за некоторыми исключениями (например, электронные госуслуги).

6. Для обработки персональных данных с целью защиты здоровья пациента в общем слу-

чае требуется получение его согласия (за исключением случаев, когда получение согласия субъекта персональных данных невозможно или когда обработка производится в рамках договорных отношений). Но при отзыве пациентом своего согласия оператор теперь не обязан прекратить обработку его персональных данных, так как «обработка персональных данных в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну», относится к специальным категориям, право обработки которых, согласно новой редакции Закона, сохраняется у оператора и после отзыва согласия субъекта.

7. Оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях по защите персональных данных.

8. Значительно усложнен пункт о поручении обработки персональных данных другому лицу (должно быть получено согласие субъекта и конкретно определены условия обработки). Ответственность за безопасность персональных данных при этом все равно несет оператор.

Следует также учитывать, что в нынешней редакции Закона немного изменены требования к содержанию уведомлений, запросов, согласий и пр., в результате чего организациям, уже использующим такие документы, придется их откорректировать.

ЛИТЕРАТУРА

- 1.** Федеральный закон Российской Федерации от 25 июля 2011 г. № 261-ФЗ г. Москва «О внесении изменений в Федеральный закон «О персональных данных»//Российская газета. —Федеральный выпуск №5538 от 27 июля 2011 г.



2. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»//Российская газета. — Федеральный выпуск № 4131 от 29 июля 2006 г.
3. Фохт О.А., Козадой Ю.В. Динамика формирования и текущее состояние требований по защите персональных данных пациентов//Врач и информационные технологии. — 2011. — № 4. — С. 6–22.
4. Обсуждение Законопроекта Резника. URL: <http://www.fz-152.org/forum/viewforum.php?f=2> (дата обращения: 17.08.2011).
5. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (включая «Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости» и Приложения (26 шт.)) <http://www.minzdravsoc.ru/docs/mzsr/informatics/5> (дата обращения: 17.08.2011).
6. Модель угроз типовой медицинской информационной системы (МИС) типового лечебно-профилактического учреждения (ЛПУ) http://www.minzdravsoc.ru/docs/mzsr/informatics/4/Modely_ugroz_MIS_LPU_2009_all.pdf (дата обращения: 17.08.2011).

Органайзер



CNEWS CONFERENCES И CNEWS ANALYTICS ПРОВЕДУТ 22 НОЯБРЯ 2011 Г. В МОСКВЕ КОНФЕРЕНЦИЮ «НОВЫЕ МЕДИЦИНСКИЕ ТЕХНОЛОГИИ»

Утвержденной 28 апреля 2011 г. Приказом № 364 Минздравсоцразвития России Концепцией создания единой государственной информационной системы в сфере здравоохранения предусмотрено выделение на информатизацию отечественного здравоохранения 19,6 млрд. руб. из федерального и 9,6 млрд. руб. из региональных бюджетов, то есть всего 29,2 млрд. рублей. Очевидно, что построение такой системы потребует в первую очередь целого ряда комплексных подготовительных мероприятий, таких как оснащение ЛПУ необходимой компьютерной техникой, развитие телекоммуникационной инфраструктуры, создание необходимых вычислительных мощностей как регионального, так и федерального уровня.

- Каких ИТ-решений ждет российское здравоохранение?
- Что могут предложить ему отечественные разработчики?
- Насколько применимы на российском рынке западные решения?
- Как решить проблему ИТ-поддержки медицинских учреждений?
- Готовы ли врачи к широкому использованию новейших технологий или они предпочитают работать по старинке?

Эти и многие другие вопросы будут рассмотрены в рамках круглого стола «Новые медицинские технологии».

Подробная информация http://events.cnews.ru/events/22_11_11.shtml.

По дополнительным вопросам обращайтесь по телефонам:

+7-495-363-11-57 доб. 50-35, 50-77, 50-78, 50-87. E-mail: events@cnews.ru,

Четвернин Алексей, Айвазов Армен, Серова Елена и Крысина Ольга.

