О.А. ФОХТ,
старший научный сотрудник Института программных систем им. А.К. Айламазяна РАН,
oaf@interin.ru
Ю.В. КОЗАДОЙ,
инженер-исследователь Института программных систем им. А.К. Айламазяна РАН,
yvk@interin.ru

ДИНАМИКА ФОРМИРОВАНИЯ И ТЕКУЩЕЕ СОСТОЯНИЕ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ.

Вопросы соответствия медицинских информационных систем требованиям законодательства РФ

УДК 61:658.011.56

Фохт О.А., Козадой Ю.В. ***Динамика формирования и текущее состояние требований по защите персональных данных пациентов. Вопросы соответствия медицинских информационных систем требованиям законодательства РФ*** *(Институт программных систем им. А.К. Айламазяна РАН)*

Аннотация: Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных» регулирует деятельность по обработке (использованию) персональных данных. Закон принят Государственной Думой 26 июля 2006 года и вступил в силу 26 января 2007 г. Однако до настоящего момента нет полной ясности, каким именно образом организации, работающие с персональными данными, должны их защищать. Еще больше вопросов возникает относительно применения данного закона в прикладных областях — например, при информатизации учреждений здравоохранения, где большое значение приобретает специфика персональных данных и работы с ними.

В статье рассматривается динамика формирования требований по защите персональных данных и вопросы соответствия информационных систем лечебно-профилактических учреждений законодательству РФ. Данная тематика прежде всего представляет интерес для ИТ-специалистов широкого профиля (не специалистов в области защиты информации) самих лечебно-профилактических учреждений (ЛПУ), а также организаций, разрабатывающих и внедряющих информационные системы в медицинских учреждениях, для общего понимания сути проблемы.

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

UDC 61:658.011.56

Vogt Olga A., Kozadoy Yuriy V. ***Changes and current state of the patient personal data security requirements. Questions about applying Russian Federation legal system to healthcare information systems*** *(Program Systems Institute, RAS)*

Abstract: The law of 27.07.2006 «On personal data protection» regulates personal records processing (usage) activity. The law was inured on 26.01.2007. Still, it's not clear how exactly must institutions processing personal records protect it. The more vague is the law effect in application areas — for example, in the healthcare institutions informatization where specific personal records and its processing becomes significantly important.

The article describes the personal records protection requirements dynamics and the questions about the healthcare information systems correspondence to the legal system. This subject is first of all interesting to common IT specialists (not the information security specialists) of healthcare institutions and also to institutions developing and setting information systems in healthcare institutions — to understand the crux of the problem.

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

История вопроса

В 2006-м году были приняты Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2] и Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». И если первый не привлек особенного внимания, то второй всколыхнул сферу информационных технологий и держит ее в напряжении до сих пор.

Между тем необходимость защиты информации декларировалась и ранее, эти вопросы регулировали Федеральный закон от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» [3] и ряд других нормативно-правовых актов. Требования по защите конфиденциальной информации определялись документом Гостехкомиссии России «Специальные требования и рекомендации по технической защите конфиденциальной информации» (известном как «СТР-К») [4].

Данный документ определяет конфиденциальную информацию как информацию с ограниченным доступом, за исключением сведений, отнесенных к государственной тайне и персональным данным, содержащуюся в государственных (муниципальных) информационных ресурсах, накопленную за счет государственного (муниципального) бюджета и являющуюся собственностью государства. При этом указывается, что для защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, данный документ носит рекомендательный характер. Однако четкого определения «государственному информационному ресурсу» документ не дает, что породило многочисленные толкования данного вопроса: к государственным информационным ресурсам относили то любые хранилища информации в бюджетном учреждении, то лишь информационные хранилища органов управления государством (или муниципальным субъектом), организованные в интересах осуществления их полномочий.

Документ «СТР-К» устанавливал требования к классификации автоматизированных информационных систем (АС), обрабатывающих конфиденциальную информацию, по уровню защищенности, после чего необходимость применения тех или иных средств защиты для системы определенного класса определялась руководящим документом (РД) Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [5]. Именно здесь появились названия классов (устанавливалось девять классов защищенности АС от НСД к информации, классы подразделялись на три группы, отличающиеся особенностями обработки информации в АС, — 3Б, 1Г и пр.), которые до сих пор повсеместно используются в области защиты информации.

До принятия ФЗ «О персональных данных» обязательность применения средств защиты информации не декларировалась широко, документ «СТР-К» оставался документом для служебного пользования, серьезный учет организаций, обрабатывающих конфиденциальную информацию, не велся. А значит, санкции надзорных органов за несоблюдение требований по защите данных не грозили обыкновенному учреждению (школе или больнице), не имеющему по роду своей деятельности дел с секретными сведениями. Вступление же в силу 152-ФЗ предъявляло ряд требований практически к любой организации, обрабатывающей самую простую информацию: Ф.И.О. граждан и какие-то дополнительные сведения о них, называя такую организацию «оператором обработки персональных данных». Всем операторам обработки персональных данных предписывалось уведомить уполномоченный орган о своем намерении осуществлять обработку таких данных и защищать такие данные надлежащим обра-

зом. Таким образом, новый закон затронул очень многих.

Уполномоченным органом по защите прав субъектов персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Регуляторами в сфере защиты персональных данных при их обработке выступают также Федеральная служба по техническому и экспортному контролю (ФСТЭК России) и Федеральная служба безопасности Российской Федерации (ФСБ России).

Динамика формирования нормативной базы

Далее события развивались следующим образом:

1. Издание совместного приказа ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, утверждающего «Порядок проведения классификации информационных систем персональных данных» [6].

Указанный порядок вводил классификацию информационных систем не по уровню защищенности (как ранее определялось РД Гостехкомиссии России), а по виду обрабатываемых персональных данных и параметрам их обработки — так появилась другая система классов от К1 до К4. Классы в терминах этой классификации и классы, введенные ранее РД Гостехкомиссии России, — это совершенно разные классы и друг с другом они не соотносятся.

2. Выпуск в феврале 2008-го года комплекта нормативно-методических документов ФСТЭК (так называемого «четверокнижия»), регламентирующих защиту персональных данных при их обработке в информационных системах (ИС).

Документы изначально носили статус ДСП и не получили широкого распространения. Комплект включал:

— документ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», утв. зам. директора ФСТЭК России 15.02.08 [7];

— документ «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утв. зам. директора ФСТЭК России 15.02.08 [8];

— документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утв. зам. директора ФСТЭК России 15.02.08 [9];

— документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утв. зам. директора ФСТЭК России 14.02.08 [10].

«Основные мероприятия...» определяли список мероприятий, которые должны были быть выполнены для защиты информации. Мероприятия привязывались к классу системы, определенному в соответствии с «Порядком проведения классификации информационных систем персональных данных», и уточнялись для различных режимов использования ИС (многопользовательский/однопользовательский, с разными правами доступа пользователей/с одинаковым доступом).

«Рекомендации по обеспечению...» разъясняли положения «Основных мероприятий» и также привязывались к классам ИС.

Эти документы были достаточно объемными — представляли определенные трудности для изучения и понимания — и достаточно жесткими по составу требований.

Остальные две книги относились к модели угроз, представляя базовую модель и методику построения на ее основе частной модели угроз для конкретной ИС в конкретном учреждении, — и это было в определенной степени новшество, предыдущие документы (например, «СТР-К») упоминали о модели угроз как-то «вскользь» и особого внимания

ей не придавали. Но что было удивительно, базовые модели угроз предлагались для различных групп ИС (АРМ, локальные ИС, распределенные ИС, имеющие/не имеющие подключение к сетям общего пользования). И эти группы никоим образом не соотносились с классами ИС, а значит, и с первыми двумя книгами четверокнижия. То есть модель моделью, а требуемый комплекс мероприятий комплексом мероприятий, от модели угроз этот комплекс никак не зависел.

3. Изменение статуса документов «четверокнижия». Решением ФСТЭК России от 16 ноября 2009 г. с документов снята пометка «для служебного пользования» и они признаны общедоступными. При этом документы немного подправили, но не принципиально.

4. Выпуск 24 декабря 2009 года Минздравсоцразвития России совместно со ФСТЭК ряда рекомендательных документов, касающихся обеспечения защиты информации в ЛПУ. Сюда вошли:

— «Модель угроз типовой медицинской информационной системы (МИС) типового лечебно-профилактического учреждения (ЛПУ)»,

— «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.)» [11, 12].

Документы выложены на сайте Минздравсоцразвития в общий доступ. Работа проведена грандиозная. Стараниями Минздравсоцразвития рекомендуемый класс медицинских информационных систем понижен с ранее бесспорного и очень жесткого К1 («персональные данные, касающиеся состояния здоровья», в соответствии с «Порядком проведения классификации информационных систем персональных данных») до более-менее приемлемого в обеспечении защиты К3.

Основные моменты, которые позволили это сделать, изложены в выводах к «Модели угроз»: отнесение ИС к специальной (что позволило более «вольно» обращаться с классификацией), утверждение, что в МИС не предусмотрено принятие решений, порождающих юридические последствия в отношении субъекта персональных, на основании исключительно автоматизированной обработки персональных данных, а также весьма спорный тезис: «нарушение безопасности персональных данных, обрабатываемых в МИС, может привести к незначительным негативным последствиям для субъектов персональных данных».

Безусловно, все это небесспорно. Однако «Методические рекомендации...» утверждены не только Минздравсоцразвития, на них стоит и согласование ФСТЭК, «Модель угроз» с вышеуказанными формулировками идет как бы в комплекте с Рекомендациями, что придает этим выводам определенную легитимность.

Дополнительно опубликованный комплект содержит огромное количество приложений, представляющих собой типовые документы по обеспечению информационной безопасности в ЛПУ. Адаптировав их для себя, ЛПУ сможет довольно уверенно себя чувствовать в области организационных мер по защите информации, а это уже значительно облегчает его участь.

5. Внесение в декабре 2009 года изменений в статьи 19 и 25 Федерального закона «О персональных данных», в части исключения требования об использовании криптографических средств защиты персональных данных и продления срока, в течение которого ранее созданные информационные системы персональных данных подлежат приведению в соответствие с Федеральным законом.

Требования по использованию криптографических средств защиты персональных данных сняты. Срок приведения ИС в соответствие Закону о персональных данных продлен до 1 января 2011 г.

6. Выпуск 5 февраля 2010 года Приказа № 58 ФСТЭК «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» и самого Положения, являющегося на момент подготовки статьи последним выпущенным документом в этой сфере [13, 14].

Соответствующее Положение четко определяет, что деятельность по защите персональных данных должна базироваться на модели угроз: «Выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности». Приложение данного документа содержит список мер и способов защиты для ИС различных классов с уточнениями по количеству пользователей и режиму доступа. Как эти меры соотносятся с моделью угроз по-прежнему непонятно, но формулировка: «применяются следующие основные методы и способы защиты информации» (в отличие от «должны быть применены») и «определяются оператором (уполномоченным лицом)» дает основания считать, что из приведенного списка следует выбрать те методы и способы, которые необходимы для нейтрализации актуальных угроз. Впрочем как этот пункт будут толковать надзорные органы, неизвестно.

Положение и в части списка мер и средств защиты значительно мягче (а главное — короче!) предыдущих «Основных мероприятий» и «Рекомендаций» ФСТЭКа. Отменена обязательная аттестация оператора обработки персональных данных. Отменено требование по обязательному контролю недекларированных возможностей для систем класса ниже К1. Список применяемых мер очень сильно сокращен.

7. Отмена 15 марта 2010 г. действия документов «четверокнижия» «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» и «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Документы далее не применяются в связи с изданием Приказа ФСТЭК № 58, утвердившего заменившее их Положение.

8. Внесение 27.07.2010 в Федеральный закон «О персональных данных» изменений о признании равнозначности письменного согласия субъекта персональных данных и согласия в форме электронного документа.

9. Ответ Федеральной службы по техническому и экспортному контролю (Письмо №240/2/2520 от 18 июня 2010 г.) на запрос Минздравсоцразвития о необходимости получения лечебно-профилактическими учреждениями лицензии на деятельность по технической защите информации, если эта деятельность осуществляется ЛПУ исключительно в собственных нуждах [15].

Ответ ФСТЭК заключался в разъяснении, что деятельность по технической защите информации подлежит обязательному лицензированию независимо от того, в чьих интересах эта деятельность осуществляется. Таким образом, попытка Минздравсоцразвития увести учреждения здравоохранения от необходимости лицензирования по защите информации не удалась в полной мере. Однако ЛПУ может не иметь лицензии само (для обработки персональных данных она теперь не требуется), оно лишь должно заключать договоры на разработку и сопровождение средств защиты информации для своих МИС с организациями, имеющими такую лицензию.

10. Внесение 10 декабря 2010 года изменений в статью 25 Федерального закона «О персональных данных» в части продления срока, в течение которого ранее созданные информационные системы персональных данных подлежат приведению в соответствие с Федеральным законом.

Срок приведения ИС в соответствие Закону о персональных данных продлен до 1 июля 2011 г.

Что происходит сейчас и каковы дальнейшие перспективы?

На момент подготовки статьи (май 2011 г.) в Государственной Думе на рассмотрении находится законопроект № 282499-5 В.М. Резника «О внесении изменений в Федеральный закон «О персональных данных» (в части уточнения условий и правил обработки персональных данных)» [16, 17].

Законопроект содержит массу поправок, которые, с одной стороны, делают закон более внятным и логичным, а с другой, содержат довольно революционные отступления от первоначальной концепции. Так, например, предлагается явно озвучить возможность разработки и применения отраслевых стандартов по обработке и хранению персональных данных, при этом не оговаривается, что требования по защите должны быть не ниже, чем государственные. Предлагается также разделить случаи обработки персональных данных на обязательные (субъект не может отказаться от обработки своих персональных данных, и в этих случаях оператор должен будет соответствовать требованиям регуляторов по защите данных) и производимые по соглашению субъекта персональных данных с оператором, причем такое соглашение может быть офертой неограниченному кругу лиц (и в этих случаях основные параметры обработки и защиты персональных данных определяются этим самым соглашением, а требования регуляторов являются всего лишь рекомендательными).

Если законопроект будет принят, то вполне возможно, что обработка персональных данных в медицинских информационных системах попадет под случай «по соглашению», и оператор получит гораздо большую свободу маневра.

Однако последняя запись в электронной регистрационной карте законопроекта от 5.05.2010: «Принять законопроект в первом чтении; представить поправки к законопроекту в тридцатидневный срок со дня принятия постановления». Как можно заметить, с момента этого решения прошло больше года, а законопроект так и числится «находящимся на рассмотрении» (включен в примерную программу решением Государственной Думы на май 2011), что является лучшим подтверждением незрелости вопроса на сегодня.

Сравнительный анализ требований при защите ИСУ по классам К1-К3

Ниже приведена сравнительная таблица требований при защите ИСУ для разных классов [14].

Таблица 1

Сравнительная таблица требований при защите МИС по классам К1-К3

Защита по классу К3	*Защита по классу К2*	*Защита по классу К1*
Управление доступом		
Идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов	То же, что и по К3	То же, что и по К3. Дополнительно: В процессе идентификации и подлинности пользователя участвует идентификатор (код)
Не предъявляются	Не предъявляются	Идентификация терминалов, технических средств, узлов сети, каналов связи, внешних устройств по логическим именам
Не предъявляются	Не предъявляются	Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам

Таблица 1, продолжение

Защита по классу К3	*Защита по классу К2*	*Защита по классу К1*
Не предъявляются	Не предъявляются	Контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа
Регистрация и учет		
Регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа	То же, что и по К3	То же, что и по К3. Дополнительно: В параметрах регистрации указывается код или пароль, предъявленный при неуспешной попытке
Учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме)	То же, что и по К3	То же, что и по К3
Не предъявляются	Не предъявляются	Регистрация выдачи печатных (графических) документов на бумажный носитель. В параметрах регистрации указываются дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи (логическое имя (номер) внешнего устройства), краткое содержание документа (наименование, вид, шифр, код), идентификатор пользователя, запросившего документ
Не предъявляются	Не предъявляются	Регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор пользователя, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный)

Таблица 1, продолжение

Защита по классу К3	*Защита по классу К2*	*Защита по классу К1*
Не предъявляются	Не предъявляются	Регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого файла
Не предъявляются	Не предъявляются	Регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа (терминалам, техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей). В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор пользователя, спецификация защищаемого объекта (логическое имя (номер))
Не предъявляются	Не предъявляются	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти информационной системы и внешних накопителей
Обеспечение целостности		
Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по контрольным суммам компонентов системы защиты, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения персональных данных	То же, что и по К3	То же, что и по К3

Таблица 1, продолжение

Защита по классу К3	*Защита по классу К2*	*Защита по классу К1*
Физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации	То же, что и по К3	То же, что и по К3
Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа	То же, что и по К3	То же, что и по К3
Наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности	То же, что и по К3	То же, что и по К3
Безопасное межсетевое взаимодействие		
Фильтрация на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов)	То же, что и по К3	То же, что и по К3
Фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств	То же, что и по К3	То же, что и по К3
Не предъявляются	Фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов	То же, что и по К2
Не предъявляются	Фильтрация с учетом любых значимых полей сетевых пакетов	То же, что и по К2
Не предъявляются	Не предъявляются	Фильтрация на транспортном уровне запросов на установление виртуальных соединений с учетом транспортных адресов отправителя и получателя

Таблица 1, продолжение

Защита по классу К3	*Защита по классу К2*	*Защита по классу К1*
Не предъявляются	Не предъявляются	Фильтрация на прикладном уровне запросов к прикладным сервисам с учетом прикладных адресов отправителя и получателя
Не предъявляются	Не предъявляются	Фильтрация с учетом даты и времени
Идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия	То же, что и по К3	То же, что и по К3
Не предъявляются	Не предъявляются	Идентификация и аутентификация администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации
Не предъявляются	Не предъявляются	Аутентификация входящих и исходящих запросов методами, устойчивыми к пассивному и (или) активному прослушиванию сети
Регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана)	То же, что и по К3	То же, что и по К3
Не предъявляются	Регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации)	То же, что и по К2
Не предъявляются	Регистрация запуска программ и процессов (заданий, задач)	То же, что и по К2
Не предъявляются	Не предъявляются	Регистрация и учет запросов на установление виртуальных соединений
Не предъявляются	Не предъявляются	Регистрация действия администратора межсетевого экрана по изменению правил фильтрации
Контроль целостности собственной программной и информационной части средства, обеспечивающего безопасное межсетевое взаимодействие	То же, что и по К3	То же, что и по К3. / Дополнительно: / Целостность контролируется по контрольным суммам

Таблица 1, продолжение

Защита по классу К3	*Защита по классу К2*	*Защита по классу К1*
Восстановление свойств межсетевого экрана после сбоев и отказов оборудования	То же, что и по К3	То же, что и по К3
Регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления	То же, что и по К3	То же, что и по К3
Не предъявляются	Регламентное тестирование процесса регистрации	То же, что и по К2
Не предъявляются	Не предъявляются	Регламентное тестирование процесса идентификации и аутентификации запросов
Не предъявляются	Не предъявляются	Локальная сигнализация попыток нарушения правил фильтрации
Не предъявляются	Не предъявляются	Предотвращение доступа неидентифицированного пользователя или пользователя, подлинность идентификации которого при аутентификации не подтвердилась
Не предъявляются	Не предъявляются	Возможность дистанционного управления своими компонентами, в том числе возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации
Контроль отсутствия недекларированных возможностей		
Необходимость проведения контроля отсутствия недекларированных возможностей программного обеспечения средств защиты информации, применяемых в информационных системах К2 и К3 классов, определяется оператором (уполномоченным лицом).		Программное обеспечение средств защиты информации, применяемых в информационных системах класса К1, проходит контроль отсутствия недекларированных возможностей. Для информационных систем класса К1 применяется программное обеспечение средств защиты информации, соответствующее 4-му уровню контроля отсутствия недекларированных возможностей.

Таблица 1, окончание

Защита по классу К3	*Защита по классу К2*	*Защита по классу К1*
Защита от утечки по техническим каналам		
Защита речевой информации и информации, представленной в виде информативных электрических сигналов и физических полей, осуществляется в случаях, когда при определении угроз безопасности персональных данных и формировании модели угроз применительно к информационной системе являются актуальными угрозы утечки акустической речевой информации, угрозы утечки видовой информации и угрозы утечки информации по каналам побочных электромагнитных излучений и наводок		
	В информационных системах класса К2 для обработки информации используются средства вычислительной техники, удовлетворяющие требованиям национальных стандартов по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам средств вычислительной техники.	Для исключения утечки персональных данных за счет побочных электромагнитных излучений и наводок в информационных системах класса К1 могут применяться следующие методы и способы защиты информации: — использование технических средств в защищенном исполнении; — использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия; — размещение объектов защиты в соответствии с предписанием на эксплуатацию; — размещение понижающих трансформаторных подстанций электропитания и контуров заземления технических средств в пределах охраняемой территории; — обеспечение развязки цепей электропитания технических средств с помощью защитных фильтров, блокирующих (подавляющих) информативный сигнал; — обеспечение электромагнитной развязки между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы охраняемой территории, и информационными цепями, по которым циркулирует защищаемая информация.
Размещение устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.		

Что делать ЛПУ

Нормативно-правовая база в области защиты персональных данных до сих пор находится в постоянном движении. Принятие же полного комплекса мер по обеспечению информационной безопасности в соответствии с нынешней редакцией требований требует значительных вложений. При этом существует вероятность, что принятые сейчас меры в итоге окажутся либо недостаточно соответствующими изменившейся нормативной базе, либо, напротив, значительно превзойдут ее, а значит, произведенные затраты окажутся неоправданно высокими. В то же время, не дожидаясь окончательного формирования согласованной позиции всех заинтересованных сторон, ФСТЭК уже проводит проверки юридических лиц и индивидуальных предпринимателей по вопросам контроля обеспечения безопасности персональных данных (план проведения плановых проверок выложен на сайте ФСТЭК).

С учетом вышесказанного любому ЛПУ целесообразно уже сейчас предпринять ряд не слишком затратных мер, чтобы не оказаться в числе отъявленных нарушителей. Это следующие действия:

1. Утверждение перечня конфиденциальной информации ЛПУ. Обязательно.

Информационная система медицинского учреждения (далее — медицинская информационная система, МИС) может содержать различную информацию ограниченного доступа, при этом следует иметь в виду, что защита разных видов конфиденциальной информации регулируется различными нормативными документами. Статус конфиденциальности информации присваивается на уровне самого учреждения, и оно имеет определенную свободу в этом вопросе. Удобнее считать, что вся конфиденциальная информация ЛПУ подпадает исключительно под действие закона «О персональных данных» (выполнять требования которого в любом случае придется) и никак не соотносится с дополнительными требованиями того же «СТР-К». Для этого в Перечне все нуждающиеся в охране данные о пациентах и их лечении следует объявить «персональными данными, содержащими информацию о здоровье субъекта персональных данных», а не коммерческой или служебной тайной.

2. Проведение классификации ИС с оформлением соответствующего Акта. Обязательно.

В соответствии с методическими документами Минздравсоцразвития [11, 12] можно порекомендовать классифицировать МИС как специальную информационную систему обработки персональных данных, в основном класса К3.

3. Уведомление надзорных органов о своем намерении осуществлять обработку персональных данных пациентов. Обязательно.

Уведомление следует подавать в территориальный орган Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (территориальный орган Роскомнадзора).

4. Формирование комплекта документов ЛПУ по обеспечению информационной безопасности на основе типовых документов, разработанных Минздравсоцразвития (Приложения к документу «Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сфере труда и занятости») [11]. Обязательно.

Состав комплекта должен быть по возможности полный. С особенным вниманием следует отнестись к формированию модели угроз и ее ограничений, так как это основополагающий документ, определяющий в дальнейшем направления и степени защиты. При формировании модели угроз следует проанализировать возможные

риски и стоимость защиты от них — ряд угроз, цена защиты от которых значительно превосходит возможный ущерб, будет правильнее объявить неактуальными и не рассматривать. Модель угроз может также содержать различные допущения (ограничения), принимаемые оператором обработки персональных данных. Например, модель нарушителя может допускать сговор персонала ЛПУ со сторонними лицами, но исключать сговор между собой (по причине тщательного отбора персонала). Модель может содержать ограничение «не рассматривать угрозы утечки информации по каналам побочных электромагнитных излучений и наводок» и пр.

5. Организация и регулярное выполнение регламентных мероприятий, означенных в сформированном комплекте документов.

6. Введение в ЛПУ процедуры получения согласия пациентов на обработку их персональных данных при заведении медкарты (или при первом обращении в ЛПУ, начиная с определенного момента времени). Крайне желательно.

Способы оформления такого согласия могут быть любыми: от автоматизированного формирования согласий в МИС до заполнения заранее напечатанных бланков данными субъекта обработки персональных данных.

7. Введение в ЛПУ процедуры обезличивания персональных данных пациентов по их требованию. Обязательно.

Возможность обезличивания должна быть реализована в МИС.

8. Выполнение требований нормативных документов по защите данных. В меру возможностей.

Может выполняться согласно разделу данной статьи «Легкий» вариант для защиты персональных данных». Указанные в разделе меры в каких-то случаях могут оказаться не вполне удобными или не полностью соответствующими требованиям нормативно-правовых документов. Зато они доступны.

«Легкий» вариант для защиты персональных данных (для класса К3)

В соответствии с актуальным на момент подготовки статьи Положением «О методах и способах защиты информации в информационных системах персональных данных» [14] для систем класса К3 рекомендуются меры:

а) управление доступом:

— идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Может быть реализовано как средствами операционной системы, так и средствами прикладного программного обеспечения (самой МИС).

б) регистрация и учет:

— регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации указываются дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная), идентификатор (код или фамилия) пользователя, предъявленный при попытке доступа.

Может быть реализовано как средствами операционной системы, так и средствами прикладного программного обеспечения (самой МИС), а также организационными мерами (ведение соответствующих журналов);

— учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме).

Может быть реализовано организационными мерами (должен быть разработан соответствующий регламент, должны вестись соответствующие журналы).

в) обеспечение целостности:

— обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.

Это самое сложное требование, обычно соответствие ему обеспечивается установкой на каждый компьютер программно-аппаратных средств защиты информации от несанкционированного доступа — СЗИ от НСД (Secret Net, Аккорд, Dallas Lock, Панцирь-К, Фикс и пр.), что при большом количестве компьютеров в ЛПУ требует довольно значительных затрат. В качестве «промежуточной» меры можно порекомендовать использование СЗИ от НСД только на серверах (при условии, что МИС в ЛПУ построена на клиент-серверной архитектуре) с дополнительным вводом регламента на установку и использование средств модификации объектного кода программ на компьютерах, где обрабатываются персональные данные (при этом необходимо обратить внимание, что к «средствам модификации объектного кода» относятся не только средства разработки, но и такие «безобидные» прикладные программы, как Microsoft Office или Microsoft Internet Explorer), а также ведением паспортов серверов и рабочих станций, где будет перечислено установленное на них ПО. Обязательно использование антивирусного программного обеспечения. Обязательна организация регулярного резервного копирования данных и самой МИС;

— физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации.

Может быть реализовано организационными мерами;

— периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа.

Автоматическое тестирование при помощи тест-программ может быть обеспечено только использованием СЗИ от НСД, предоставляющих такой функционал. Но в качестве «облегченной» меры можно предложить регламент периодического «ручного» прогона МИС по «Программе и методике испытаний» (в части обеспечения защиты информации), которая должна быть разработана для ввода ИС в действие. Регламент должен предусматривать проверки как после установки обновлений МИС, так и плановые (периодические) проверки или проверки при изменении условий функционирования МИС. Как вариант (при отсутствии такого документа) может быть разработан список контрольных примеров, прохождение по которому обеспечивает проверку соответствия МИС требованиям безопасности;

— наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонент средств защиты информации, их периодическое обновление и контроль работоспособности.

Может быть реализовано разработкой регламента восстановления работоспособности МИС и всей системы защиты после сбоев или аварийных ситуаций. Ведение двух копий программных компонент средств защиты информации в минимальном варианте может быть обеспечено хранением в двух экземпля-

рах дистрибутивов программных средств и файлов с описанием настроек.

г) обеспечение безопасного межсетевого взаимодействия.

Достигается применением средств межсетевого экранирования. При выборе следует исходить из наличия сертификата ФСТЭК и оптимальной цены для требуемого количества пользователей.

Следует заметить, что рекомендуемые для защиты ИС по классу К2 мероприятия отличаются от рассмотренных выше только в части обеспечения безопасного межсетевого взаимодействия. Его же в любом случае (в объеме, достаточном для К3 и К2) обеспечит применение межсетевого экрана.

Обстоятельством, осложняющим организацию защиты данных, является требование «использования средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия». Положение не уточняет, какая именно процедура соответствия должна быть пройдена и какие именно сертификаты должны иметь средства защиты. Тем не менее, для защиты информации лучше использовать средства, имеющие сертификаты. В первую очередь это относится к специализированным средствам — чье единственное назначение в обеспечении информационной безопасности (межсетевой экран, СЗИ от НСД, антивирусное программное обеспечение).

Операционная система (при декларации ее использования и в качестве средства защиты данных) тоже может иметь сертификат. Имея официальную версию ОС (например, Microsoft Windows XP), можно поднять ее до уровня сертифицированной ФСТЭК.

Использование прикладного программного обеспечения (МИС), имеющего сертификат, довольно проблематично, так как процедура сертификации чрезвычайно трудоемка, требует больших затрат и вряд ли будет широко применяться производителями медицинских информационных систем.

ЛИТЕРАТУРА

1. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации».

4. Документ Гостехкомиссии России «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К).

5. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации».

6. Порядок проведения классификации информационных систем персональных данных, утвержденный Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 (зарегистрирован Минюстом России 03.04.2008, регистрационный № 11 462).

7. Нормативно-методический документ «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных», утв. зам. директора ФСТЭК России 15.02.08.

8. Нормативно-методический документ «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утв. зам. директора ФСТЭК России 15.02.08.

9. Нормативно-методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утв. зам. директора ФСТЭК России 15.02.08.

10. Нормативно-методический документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утв. зам. директора ФСТЭК России 14.02.08.

11. «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости», утверждены директором Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации 23.12.2009 с приложениями.

12. 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, утвержденные директором Департамента информатизации Министерства здравоохранения и социального развития Российской Федерации 23.12.2009, согласованные начальником 2-го управления ФСТЭК России 22.12.2009.

13. Приказ № 58 Федеральной службы по техническому и экспортному контролю «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» от 5 февраля 2010 г., подписанный директором Федеральной службы по техническому и экспортному контролю.

14. Положение «О методах и способах защиты информации в информационных системах персональных данных» (Приложение к Приказу № 58 Федеральной службы по техническому и экспортному контролю «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных» от 5 февраля 2010 г.).

15. Ответ Федеральной службы по техническому и экспортному контролю (Письмо № 240/2/2520 от 18 июня 2010 г.) на запрос Минздравсоцразвития о необходимости получения лечебно-профилактическими учреждениями лицензии на деятельность по технической защите информации, если эта деятельность осуществляется ЛПУ исключительно в собственных нуждах.

16. Законопроект № 282499-5 «О внесении изменений в Федеральный закон «О персональных данных» (в части уточнения условий и правил обработки персональных данных).

17. Электронная регистрационная карта на законопроект № 282499-5 «О внесении изменений в Федеральный закон «О персональных данных» (в части уточнения условий и правил обработки персональных данных).