О.А. ФОХТ,
старший научный сотрудник, Институт программных систем им. А.К. Айламазяна РАН, г. Переславль-Залесский, Россия, oaf@interin.ru
А.А. ЦВЕТКОВ,
главный специалист по информационной безопасности, ООО «Интерин сервис», г. Переславль-Залесский, Россия, sio@interin.com

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ. НОВОЕ В ЗАКОНОДАТЕЛЬСТВЕ: ТЕНДЕНЦИИ, ВОПРОСЫ ПРАКТИЧЕСКОГО ПРИМЕНЕНИЯ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

УДК 61:658.011.56
Фохт О.А., Цветков А.А. ***Защита персональных данных. Новое в законодательстве: тенденции, вопросы практического применения в медицинских информационных системах*** *(ФГБУН Институт программных систем им. А.К. Айламазяна Российской академии наук, г. Переславль-Залесский, Россия)*
Аннотация: В статье дается обзор вышедших нормативных документов, анализируются тенденции, складывающиеся в области защиты информации, а также рассматривается ряд наиболее интересных для применения в медицинских информационных системах вопросов практического применения требований регуляторов.
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., Tsvetkov A.A. ***Protection of Personal Data. New Legislation: Trends, Issues of Practical Application in Medical Information Systems*** *(Program Systems Institute, RAS, Pereslavl-Zalessky, Russia)*
Abstract: This article provides an overview of published regulatory documents, analyzes trends developing in the field of information security, and examines some of the most interesting for applications in healthcare information systems, the practical implementation of the requirements of regulators.
Keywords: *personal records, personal data protection, information security, information systems, healthcare information systems, information system deployment*

Введение

Закон «О персональных данных» [1] был принят в 2006 году. История формирования соответствующей ему нормативно-методической базы рассматривалась нами в 4-м номере журнала за 2011 год [2]. Здесь выделим лишь основные моменты.

Подзаконными актами и нормативными документами были определены требования по классификации обрабатывающих ПДн информационных систем (классификация регулировалась документом «Порядок проведения классификации информационных систем персональных данных» [3]) и требования к необходимым мероприятиям по защите ПДн (требования зависели от класса ИС и определялись Положением «О методах и способах защиты информации в информационных системах персональных данных» [4]).

Летом 2011 года в закон были внесены поправки (Федеральный закон № 261-ФЗ от 25 июля 2011 г. «О внесении изменений в Федеральный закон «О персональных данных»» [5]), при этом изменилось более 70% текста закона — мы писали об этом в 5-м номере журнала за 2011 год [6].

Вслед за вводом в действие обновленного закона последовали изменения и в подзаконных актах, нормативных и методических документах. Основными стали:

— Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [7], определяющее, в частности, новую схему классификации ИС для обработки ПДн;

— Приказ ФСТЭК России № 21 от 18.05.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [8], вводящий, как это видно из названия, список обязательных мер, которые должны обеспечивать защиту ПДн.

Рассмотрим эти документы подробнее.

Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее Постановление) заменило Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» [8].

Основное влияние документа на практическую организацию защиты ПДн оказывает новая классификация, которую вводит Постановление.Взамен утвержденных ранее приказом [2] для ИС обработки ПДн (далее ИСПДн) классов К1–К4, в зависимости от которых для защиты данных должны были применяться определенные для каждого класса ИСПДн меры, новое Постановление вводит понятие «уровни защищенности персональных данных» *(см. таблицу 1).*

Именно эти уровни и определяют теперь набор мер, которые необходимо применять для защиты информации.

Согласно *таблице 1,* для выбора необходимого уровня защищенности (далее УЗ) ПДн вначале требуется зафиксировать категорию ПДн, которые будет обрабатывать/обрабатывает ИС. При этом различают следующие категории ПДн:

- специальные категории ПДн (данные о здоровье, расовой принадлежности, политических взглядах и пр.);
- биометрические категории ПДн;
- иные категории ПДн;
- общедоступные категории ПДн.

Таким образом,МИС относятся к ИСПДн, обрабатывающим специальные категории ПДн (данные о здоровье).

На следующем этапе нужно определить, чьи ПДн будет обрабатывать/обрабатывает ИС (внешних субъектов или собственных сотрудников оператора обработки ПДн), а также количество внешних субъектов, ПДн которых будут обрабатываться/обрабатываются.

Далее следует определить тип актуальных для рассматриваемой ИСПДн угроз. В Постановлении рассматриваются угрозы трех типов:

— для ИСПДн считаются актуальными угрозы 1-го типа в том случае, когда для нее актуальны угрозы, связанные с наличием недокументированных возможностей (далее — НДВ) в системном программном обеспечении, используемом в ИСПДн;

Таблица 1

Определение уровня защищенности для ИС, обрабатывающих ПДн

Категории ПДн		*Специальные*			*Биометрические*	*Иные*			*Общедоступные*		
Собственные работники		*Нет*	*Нет*	*Да*		*Нет*	*Нет*	*Да*	*Нет*	*Нет*	*Да*
Количество субъектов		*Более 100 тыс.*	*Менее 100 тыс.*			*Более 100 тыс.*	*Менее 100 тыс.*		*Более 100 тыс.*	*Менее 100 тыс.*	
Тип актуальных угроз	1	1-й УЗ	1-й УЗ	1-й УЗ	1-й УЗ	1-й УЗ	2-й УЗ	2-й УЗ	2-й УЗ	2-й УЗ	2-й УЗ
	2	1-й УЗ	2-й УЗ	2-й УЗ	2-й УЗ	2-й УЗ	3-й УЗ	3-й УЗ	2-й УЗ	3-й УЗ	3-й УЗ
	3	2-й УЗ	3-й УЗ	3-й УЗ	3-й УЗ	3-й УЗ	4-й УЗ	4-й УЗ	4-й УЗ	4-й УЗ	4-й УЗ

— для ИСПДн считаются актуальными угрозы 2-го типа в том случае, когда для нее актуальны угрозы, связанные с наличием НДВ в прикладном программном обеспечении, используемом в ИСПДн;

— для ИСПДн считаются актуальными угрозы 3-го типа в том случае, когда вышеперечисленные угрозы для нее не актуальны.

Постановление не регламентирует порядок определения актуальности перечисленных угроз для конкретной ИСПДн («определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится оператором с учетом оценки возможного вреда ... и в соответствии с нормативными правовыми актами»).Определить тип актуальных угроз — задача оператора обработки ПДн. В настоящее время складывается практика (см., например, «Материалы с вебинара обсуждения приказа ФСТЭК по защите персональныхданных» [9]) определять тип актуальных угроз, исходя из принципа оценки затрат на организацию защиты данных в сравнении с возможным ущербом от разглашения охраняемой информации. При этом все чаще высказывается мнение, что данные прикладных информационных систем (не банковских ИС, не ИС, обслуживающих выборы, и пр.) в общем случае не являются настолько ценными для возможных злоумышленников, чтобы они пошли на внедрение вредоносных закладок в прикладное, а тем более в системное программное обеспечение для таких ИС можно выбирать 3-й тип возможных угроз.

Определив категорию обрабатываемых персональных данных и тип актуальных для ИСПДн угроз, можно установить необходимый уровень защищенности для рассматриваемой системы. Постановлением вводится четыре уровня защищенности. Для МИС (ИСПДн, обрабатывающих специальные категории персональных данных) интересны следующие:

— Первый уровень защищенности необходимо обеспечить тем МИС, для которых актуальны угрозы 1-го типа, либо тем МИС, для которых актуальны угрозы 2-го типа и которые обрабатывают данные более чем ста тысяч пациентов.

— Второй уровень защищенности необходимо обеспечить тем МИС, для которых актуальны угрозы 2-го типа и которые обрабатывают данные менее чем ста тысяч пациентов, а также тем МИС, для которых актуальны угрозы 3-го типа и которые обрабатывают данные более чем ста тысяч пациентов.

— Третий уровень защищенности необходимо обеспечить тем МИС, для которых актуальны угрозы 3-го типа и которые обрабатывают данные менее чем ста тысяч пациентов.

— Четвертый уровень для МИС не подходит, так как не применяется при обработке специальных категорий персональных данных.

Постановление вводит также некоторые требования по обеспечению указанных УЗ.

Так, для обеспечения 3-го уровня защищенности необходимо принять следующие меры:

— организация режима обеспечения безопасности помещений, в которых размещена МИС, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

— обеспечение сохранности носителей ПДн;

— утверждение руководителем оператора (лечебно-профилактического учреждения) документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в МИС, необходим для выполнения ими служебных обязанностей;

— использование СЗИ, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

— назначение должностного лица, ответственного за обеспечение безопасности ПДн в МИС.

Для обеспечения защиты по 2-му уровню к вышеуказанным мерам добавляется:

— предоставление доступа к содержанию электронного журнала сообщений исключительно для должностных лиц, оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных обязанностей (при этом нигде не поясняется, что такое «электронный журнал сообщений»).

Необходимость обеспечения защиты по 1-му уровню добавляет меры:

— автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе;

— создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.

Контроль соблюдения этих требований находится в зоне ответственности оператора, который должен провести его сам либо привлечь для этого на договорной основе исполнителей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Такой контроль должен проводиться не реже одного раза в 3 года.

Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Приказ ФСТЭК России № 21 от 18.05.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее — Приказ) заменил Приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» [4].

Приказ вводит состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн для каждого из УЗ для ПДн, установленных в «Требованиях к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных Постановлением [7]. Перечень мер серьезно увеличен по сравнению с действующими ранее [4]. Следует отметить, что в Приказе для названия мер теперь используется общая профессиональная терминология, принятая в области защиты информации (см., например, описание классических угроз в [10]).

Общий перечень мер по обеспечению безопасности ПДн включает следующие группы:

— идентификация и аутентификация субъектов доступа и объектов доступа;

— управление доступом субъектов доступа к объектам доступа;

— ограничение программной среды;

— защита машинных носителей информации, на которых хранятся и (или) обрабатываются ПДн;

— регистрация событий безопасности;

— антивирусная защита;

— обнаружение (предотвращение) вторжений;

— контроль (анализ) защищенности ПДн;

— обеспечение целостности ИС и ПДн;

— обеспечение доступности ПДн;

— защита среды виртуализации;

— защита технических средств;

— защита ИС, ее средств, систем связи и передачи данных;

— выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС и (или) к возникновению угроз безопасности ПДн, и реагирование на них;

— управление конфигурацией ИС и системы защиты ПДн.

В Приложении Приказа в наглядном табличном представлении показано, какая мера должна применяться для обеспечения каждого их четырех УЗ. Наряду с обязательными мерами, входящими в базовый набор для соответствующего УЗПДн, представлены меры, которые могут применяться при адаптации или уточнении базового набора, а также при разработке компенсирующих мер. Таблица большая, поэтому приводить ее здесь мы не будем. Хочется лишь отметить, что если принять число обязательных для применения мер базового набора для защиты ИСПДн 1-го уровня за 100%, то меры базового набора для защиты ИСПДн 2-го уровня составляют около 96%, а меры, необходимые для обеспечения 3-го уровня защиты около 60% от этого количества.

То есть классификация ИСПДн не по 2-му, а по 3-му уровню защищенности значительно упрощает схему защиты данных, а вот классификация по 1-му УЗ в сравнении со 2-м уровнем не принципиально усложнит ситуацию, добавив к списку необходимых мер только следующие:

— установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов;

— контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование;

— разделение в ИС функций по управлению (администрированию) ИС, управлению (администрированию) системой защиты ПДн, функций по обработке ПДн и иных функций ИС.

Если сравнивать вышедший Приказ с проектом этого документа, опубликованным для обсуждения в декабре 2012 года, то заметным делается следующий интересный факт: формулировка проекта «Для обеспечения безопасности персональных данных при их обработке в информационных системах применяются средства защиты информации, прошедшие в соответствии с законодательством Российской Федерации оценку соответствия ***в форме обязательной сертификации*** на соответствие требованиям по безопасности информации» в конечной версии документа заменена следующей: «Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке ***процедуру оценки соответствия***, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных». Таким образом, требование использования для защиты ПДн только сертифицированных средств защиты исчезло. Теперь оператор может сам (или с привлечением на договорной основе исполнителя, имеющего лицензию на осуществление деятельности по

технической защите конфиденциальной информации) оценить эффективность и соответствие используемых средств защиты требованиям регуляторов.

Основные тенденции, формирующиеся в области защиты персональных данных

Из достойных внимания тенденций, формирующихся в области защиты персональных данных, мы отметили три:

1. Сфера защиты персональных данных перемещается в компетенцию профессионалов. И само содержание, и формулировки новых документов стали значительно более профессиональными и узкоспециальными. Теперь они приближены к документам Гостехкомиссии, регламентирующим защиту конфиденциальной информации еще до выделения ПДн для отдельного рассмотрения. Документы стали более формальными и (особенно из-за использования принятой в этой области терминологии) более понятными профессионалам в области защиты информации, но в то же время менее содержательными и понятными неподготовленному человеку. Таким образом, мы отмечаем, что, хотя за защиту ПДн по-прежнему отвечает оператор, их обрабатывающий, единственное, что он может сделать, — пригласить профессионалов и положиться на их квалификацию, самому разобраться в тонкостях требований регуляторов все менее реально.

2. Ответственность переходит от сертифицирующих органов к лицензированным организациям. ФСТЭК не может рассмотреть и сертифицировать все используемые средства защиты информации, так как их поток слишком велик. Невозможно и аттестовать на соответствие требованиям по обработке ПДн все установленные экземпляры ИСПДн. Очевидно, по этой причине принято решение делать упор на лицензирование деятельности по обеспечению информационной безопасности, причем эти лицензии теперь стали бессрочными. И уже лицензированная организация (профессионалы) разрабатывает средства защиты информации, строит комплексные системы защиты у конечного пользователя (оператора обработки ПДн) и оценивает адекватность принимаемых для защиты данных мер.

3. Сертифицированные тиражируемые средства защиты информации имеет смысл использовать для нейтрализации угроз, не зависящих от специфики ИСПДн (антивирусное программное обеспечение, межсетевые экраны и пр.). При разработке производителем МИС (ИСПДн) встроенных средств защиты информации, специфичных для данной МИС, их сертификация во ФСТЭК не требуется. Достаточно, чтобы разработчик имел лицензию на деятельность по разработке и производству средств защиты конфиденциальной информации, а исполнитель работ по развертыванию системы защиты МИС в лечебно-профилактическом учреждении — лицензию на деятельность по технической защите конфиденциальной информации. После чего оператор обработки ПДн (лечебно-профилактическое учреждение), очевидно, при помощи организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации, должен сформировать пакет документов для Роскомнадзора, которые будут описывать установленную в МИС и используемые средства защиты. Та же организация может привлекаться для помощи при проведении оператором внутренних проверок или при прохождении им внешних проверок надзорных органов.

Проблемы защиты персональных данных

Сфера защиты ПДн по-прежнему остается довольно проблематичной областью. Мы посчитали возможным особо выделить следующие проблемы:

1. Документы, регламентирующие деятельность по защите ПДн, до сих пор не слишком

согласованы друг с другом и не представляют целостный и взаимосвязанный комплект. Так, например, Приказ [8] содержит список мер, которые должны обеспечить защиту ПДн в зависимости от необходимого уровня защищенности ИСПДн. В то же время ряд необходимых мер перечислен в Постановлении [7] (в том числе про тот самый никому не ведомый «электронный журнал сообщений»), а ряд мер (например, необходимость получения в тех или иных случаях согласия субъекта на обработку его ПДн, требование возможности обезличивания ПДн, требование опубликовать на сайте принимаемые по защите данных меры и пр.) содержится в самом законе «О персональных данных» [5]. Единого ясного документа с исчерпывающим списком необходимых для «правильной» обработки персональных данных мероприятий нет.

2. Нормативные документы утверждают, что защита должна быть организована, исходя из частной модели угроз, специфичной для ИСПДн. В то же время Приказ [8] содержит список «обязательных» мер, а значит, формально их следует применять независимо от частной модели угроз. Например, среди обязательных мер есть целая группа, посвященная защите среды виртуализации, которую использует далеко не всякая ИСПДн. Также список обязательных мер по защите информации не зависит от того, подключена ИСПДн к сети Интернет или представляет собой автономную систему, а ведь всем понятно, что это совсем разные с точки зрения потенциальных угроз ситуации. Есть и другие нестыковки.

3. Нормативные документы оставляют нерегламентированными довольно сложные вопросы, исходя из которых должна строиться система защиты. Например: оценка вреда, который может быть причинен субъекту персональных данных в случае нарушения требований к обеспечению их безопасности; определение актуальности типа угрозы для установления необходимого уровня защищенности ИСПДн. Остается надеяться, что Министерство здравоохранения выпустит согласованный со ФСТЭК пакет методических документов, в которых эти вопросы будут рассмотрены с учетом специфики МИС.

4. Проблема защиты ПДн при использовании сетевых сервисов (хранение медицинских данных пациента, единая электронная медицинская карта, удаленные врачебные консультации и пр.) находятся практически вне зоны рассмотрения вопросов защиты ПДн, обеспечить для них защиту в соответствии с принятыми требованиями невозможно. И как только внимание регуляторов к этой сфере будет привлечено — движение в таком перспективном и передовом направлении в информатизации медицины будет очень сильно затруднено.

5. «Вне закона» находятся и подключаемые в МИС приборы (лабораторные анализаторы, МРТ, рентгеновские аппараты и пр.). Используемое ими программное обеспечение, как правило, «закрыто», а то и «прошито» — неразрывно связано с аппаратным обеспечением, приспособить его к требованиям регуляторов не представляется возможным.

6. Здравоохранение — сфера деятельности, обладающая огромным багажом учетной документации. Многим имеющим до сих пор хождение документам по нескольку десятков лет. Ни они, ни даже разрабатываемые в настоящее время новые формы документов никак не относятся ни к вопросам обработки в МИС, ни к вопросам защиты персональных данных, что опять же сильно затрудняет работу с ними в соответствии с требованиями регуляторов.

Начатая в России с 2006 года работа по защите персональных данных медленно, но верно начинает переходить во все более профессиональное русло, и новые требования законодательства этому способствуют. Тем не менее, при общей позитивной тенденции нельзя не отметить остающийся пласт нерешенных вопросов в части защиты ПДн при работе МИС ЛПУ, которые, мы надеемся, тоже будут решены в обозримом будущем.

ЛИТЕРАТУРА

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»//Российская газета, Федеральный выпуск № 4131 от 29 июля 2006 г.

2. *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.

3. Порядок проведения классификации информационных систем персональных данных, утвержденный Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20. Утратил силу.

4. 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.). Утратило силу.

5. 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.

6. *Фохт О.А.* Анализ принятых поправок к Федеральному закону № 152-ФЗ «О персональных данных»//Врач и информационные технологии. — 2011. — № 5. — С. 56–59.

7. Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

8. Приказ ФСТЭК России № 21 от 18.02.2013 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

9. RISSPA. Материалы с вебинара — обсуждения приказа ФСТЭК по защите персональных данных//http://www.risspa.ru/masterclass/new-fstek-order (дата обращения: 22.06.2013).

10. *Киреенко А.Е.* Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения//Молодой ученый. — 2012. — № 3. — С. 40–46.