УДК 61:681.518(075.8)
ББК (Р)51.1(2)
С 81

Столбов А.П., Кузнецов П.П. **Автоматизированная обработка и защита персональных данных в медицинских учреждениях.** – М.: ИД «Менеджер здравоохранения», 2010. – 176 с.

ISBN 978-5-903834-10-5

В книге приведены основные понятия в области автоматизированной обработки и защиты персональных данных в учреждениях здравоохранения. Рассмотрены основные принципы организации обработки персональных данных. Перечислены основные нормативно-методические и нормативно-технические документы, регламентирующие эти процессы. Даны методические рекомендации по реализации установленных требований к обеспечению конфиденциальности медицинской информации при ее автоматизированной обработке. Приведен перечень необходимых организационно-распорядительных и иных документов с соответствующими пояснениями. Книга представляет практический интерес для руководителей медицинских организаций, а также других учреждений здравоохранения и системы обязательного медицинского страхования и призвана оказать методическую помощь при организации автоматизированной обработки медицинской информации в соответствии с требованиями закона «О персональных данных».

УДК 61:681.518(075.8)
ББК (Р)51.1(2)

ISBN 978-5-903834-10-5

ОГЛАВЛЕНИЕ

Приложения

ПРЕДИСЛОВИЕ

Предлагаемая Вашему вниманию книга посвящена одной из очень актуальных сегодня для медицинских учреждений проблем – организации защиты информации о пациентах при её компьютерной обработке в соответствии с требованиями Федерального закона «О персональных данных».

Сегодня компьютеры все более активнее и шире используются в здравоохранении. Руководством страны поставлена задача в течение двух-трех лет подключить к Интернету все государственные и муниципальные учреждения и обеспечить гражданам возможность получения с помощью современных информационных и коммуникационных технологий информации о расписании работы поликлиник, записи на прием к врачу и других государственных услугах. Уже сейчас во многих регионах России реализуются проекты по ведению в поликлиниках и больницах электронных медицинских документов, предоставлению услуг «электронной регистратуры», созданию территориальных медицинских регистров и информационных систем здравоохранения.

Однако эта качественно новая технологическая среда информационного взаимодействия между врачами и пациентами создает также и множество новых проблем, связанных с обеспечением конфиденциальности медицинской информации и сохранением врачебной тайны. Реализация требований принятого в 2006 году закона «О персональных данных» предполагает создание в медицинском учреждении комплексной системы обеспечения безопасности информации, для чего нужны и специальные знания, и ресурсы, и время.

Последние дни 2009 года были отмечены двумя важными событиями: во-первых, 26 декабря на сайте Минздравсоцразвития России были опубликованы методические документы по организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости; во-вторых, было принято решение о переносе до 1 января 2011 года срока приведения всех информационных систем в соответствие с требованиями закона № 152-ФЗ «О персо-

нальных данных» от 27.07.2006 (Федеральный закон от 27.12.2009 № 363-ФЗ). В то же время проблемы с практическим выполнением всех положений и норм этого закона в здравоохранении по-прежнему остаются очень актуальными.

Поэтому полагаю, что представляемая книга, в которой описаны общие требования к защите персональных данных при использовании компьютеров для автоматизации учета медицинской помощи и даны рекомендации по их выполнению на практике будет весьма полезной и интересной как для организаторов здравоохранения и руководителей лечебно-профилактических учреждений, так и для других категорий медицинских работников, специалистов ИТ-подразделений, студентов и аспирантов соответствующих специальностей.

Директор Центрального научно-исследовательского института организации и информатизации здравоохранения, академик РАМН, доктор медицинских наук, профессор В.И. Стародубов

ВНИМАНИЕ!

Приказом Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 05.02.2010 № 58 утверждено «Положение о методах и способах защиты информации в информационных системах персональных данных» (далее — Положение). Приказ зарегистрирован в Минюсте РФ 19.02.2010 № 16456, опубликован 5 марта 2010 г. в «Российской газете», вступил в действие с 15 марта 2010 г.

Одновременно с этим в связи с изданием Приказа ФСТЭК России от 5 февраля 2010 г. № 58 объявлено решение ФСТЭК от 05.03.2010 не применять с 15.03.2010 следующие методические документы ФСТЭК:

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах (ИС) персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.;

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, утвержденные заместителем директора ФСТЭК России 15 февраля 2008 г.

Ссылки на указанные документы в тексте книги обозначены как [24] и [25], соответственно.

В связи с этим определение класса ИС персональных данных осуществляется только в соответствии с «Порядком проведения классификации информационных систем персональных данных», который утвержден совместным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 (ссылки на него в тексте книги обозначены как [23]). При этом класс системы определяется независимо от того, является ли она типовой или специальной, — таблица классов систем, приведенная в [23], относится и к типовым, и к специальным системам.

По сравнению с требованиями указанного выше методического документа «Основные мероприятия ...» в соответствии с новым Положением объем обязательных требований по защите персональных данных в ИС существенно сокращен, в том числе:

1. Отменены обязательные требования по: а) получению лицензии на техническую защиту информации, б) аттестации системы на соответствие требованиям безопасности информации, в) использованию средств криптографической защиты информации, г) управлению потоками информации с помощью меток конфиденциальности. Ранее лицензия была необходима для операторов систем классов К1, К2 и распределенных систем класса К3, аттестация была обязательной для систем классов К1 и К2, применение средств криптозащиты и меток конфиденциальности было предусмотрено для систем класса К1.

2. Отменены явные требования по обязательному использованию сертифицированных средств защиты информации, за исключением обязательного контроля отсутствия недекларированных возможностей в программном обеспечении средств защиты информации для ИС персональных данных класса К1.

3. Исключены требования по обязательному использованию специальных средств защиты от утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН), что было предусмотрено ранее для систем классов К1 и К2. Необходимость использования указанных средств защиты определяется оператором, исходя из модели актуальных угроз безопасности персональных данных в каждом конкретном случае (на усмотрение оператора).

Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных ИС через сеть связи общего пользования или Интернет в Положении предусмотрено:

— создание канала связи, обеспечивающего защиту передаваемой информации;

— осуществление аутентификации взаимодействующих ИС и проверки подлинности пользователей и целостности передаваемых данных.

При межсетевом взаимодействии ИС разных операторов персональных данных, кроме того, предусмотрено дополнительно обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю и(или) факта их получения от другого пользователя («учетность и неотказуемость»).

Поскольку приказ ФСТЭК от 05.02.2010 № 58 был опубликован уже после того, как книга была полностью сверстана и подготовлена к печати, а также учитывая актуальность представленного в книге материала, издательство признало возможным не изменять текст книги и дать только следующие пояснения:

1. Все ссылки в тексте книги на документ [24] и приведенные из него цитаты при чтении можно пропускать (не обращать на них внимания).

2. Поскольку теперь требования к системе и средствам защиты персональных данных в ИС в соответствии с их классом изложены не в [25], а в новом Положении, при описании этих требований все ссылки в тексте книги на документ [25], за исключением тех требований, которые не являются теперь обязательными (см. выше), следует считать ссылками на это Положение.

Издательство и авторы благодарят читателей за понимание.