А. Г. Сабанов, В. Д. Зыков, Р. В. Мещеряков, С. П. Рылов, А. А. Шелупанов

Защита персональных данных в организациях здравоохранения

Москва
Горячая линия – Телеком
2012

УДК 004.056.5
ББК 32.973.2-018.2
З-40

А в т о р ы : А. Г. Сабанов, В. Д. Зыков, Р. В. Мещеряков, С. П. Рылов, А. А. Шелупанов

З-40 **Защита** персональных данных в организациях здравоохранения / А. Г. Сабанов, В. Д. Зыков, Р. В. Мещеряков и др.; Под ред. А. Г. Сабанова. – М.: Горячая линия–Телеком, 2012. – 206 с., ил.

ISBN 978-5-9912-0243-5.

Книга посвящена вопросам защиты конфиденциальной информации и, в первую очередь, персональных данных, в учреждениях (организациях – согласно Федеральному закону от 21 ноября 2011 г. № 323-ФЗ) здравоохранения и социальной защиты. Анализируется современное состояние медицинских информационных систем применительно к перспективам внедрения средств защиты информации. Обсуждаются требования к защите информации, составляющей врачебную тайну и персональные данные пациентов. Рассматриваются основные способы и методы защиты информации применительно к типовым бизнес-процессам среднестатистического лечебно-профилактического учреждения. Обсуждаются вопросы снижения категории хранимых и обрабатываемых персональных данных. Анализируются перспективы развития медицинских информационных систем и систем защиты информации.

Для работников медицинских учреждений и специалистов по защите информации, также может быть полезна студентам, аспирантам и преподавателям вузов соответствующих специальностей.

ББК 32.973.2-018.2

Адрес издательства в Интернет WWW.TECHBOOK.RU

Научное издание

Сабанов Алексей Геннадиевич, **Зыков** Владимир Дмитриевич, **Мещеряков** Роман Валерьевич, **Рылов** Сергей Павлович, **Шелупанов** Александр Александрович

Защита персональных данных в организациях здравоохранения

Обложка художника В. Г. Ситникова

Подписано в печать 20.01.12. Формат 60×90/16. Усл. печ. л. 12,88. Тираж 500 экз. (1 завод – 250 экз.)

ISBN 978-5-9912-0243-5

Предисловие

Уважаемый читатель! Книга, которую Вы открыли, представляет собой весьма интересное исследование и содержит практические рекомендации, сделанные авторами на основании своего богатого опыта в области защиты информации. Приложение этого опыта к проблематике защиты информации в области информатизации здравоохранения представляется чрезвычайно важным в период реализации проекта модернизации отрасли здравоохранения. Такого полного, интересного и содержащего практические рекомендации издания, посвященного информационной безопасности систем, обрабатывающих медицинскую информацию, еще не было в нашей практике.

Информатизация здравоохранения становится одним из трех основных направлений модернизации, наряду с ремонтом и обновлением зданий, переоснащением учреждений новой медицинской техникой и стимулированием специалистов отрасли. Без внедрения информационных технологий переход на качественно иной уровень оказания медицинской помощи вред ли возможен в сроки, предусмотренные для решения задач модернизации здравоохранения. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ» прямо ставит в зависимость качество оказание медицинской помощи в учреждениях и их информатизацию. Но внедрение информационных систем в здравоохранении в значительной мере связано с реализацией фундаментальных прав пациентов на защиту их приватной информации, так как оказание медицинской помощи всегда персонифицировано. Одно из основных опасений, а иногда и возражений граждан по поводу новейших информационных технологий, связано с возможностью утечки конфиденциальной информации и ее неправомерного использования. Однако часто эти опасения возникают из-за того, что данная сфера знаний недостаточно изучена, да и практическое использование информационных систем показывает их весьма высокую уязвимость. Особенно это касается информационных систем, связанных с обработкой персональных данных, регулируемых, широко известным, 152-ФЗ. Сложность поставленной авторами перед собой задачи видна даже из того факта, что введение основных положений 152-ФЗ «О защите персо-

нальных данных» переносилось три раза и наконец, принято в полном объеме, с учетом ряда поправок, Закон заработал с 01.07.2011. Практика показывает, что во многих организациях, в том числе и медицинских, есть еще проблемы с его практической реализацией. Поэтому многим практическим специалистам данное издание будет очень полезным путеводителем в реализации комплекса мероприятий по обеспечению информационной безопасности.

Отрадно, что авторы подошли к работе классическим путем и посвятили первую главу книги анализу медицинских информационных систем. Конечно, бурно развивающаяся и фактически, несмотря на почти сорокалетнюю историю, только формирующаяся и в части терминологии и методологии, медицинская информатика трудный объект для исследований. Поэтому ряд определений и положений могут показаться спорными, например приведенная авторами в параграфе 1.2 классификация медицинских информационных систем. Дискуссионными являются и ряд положений параграфов 1.3 и 1.6, но это ни в коей мере не умаляет ценность работы, так как только в обсуждениях различных мнений мы сможем выработать общий подход и практически перейти в 2012 году к созданию единой государственной автоматизированной информационной системы (ЕГАИС) в сфере здравоохранения.

Чрезвычайно интересен взгляд авторов на формирование требований по защите информационных систем, где сосредоточены различные виды защищаемой информации: данные пациентов, сотрудников медицинских учреждений, соотношение персональных и конфиденциальных данных, коммерческой и врачебной тайны и их сложное пересечение, которое должно быть защищено как от разрушения, так и от несанкционированного использования. При этом возникает вопрос реализации 152-ФЗ в части обеспечения прав пациента на определение тех фрагментов данных, которые могут быть доступны конкретным сотрудникам учреждений. В довершение всего нельзя забывать о медицинской науке, которая не может развиваться без анализа и обработки данных территориально-популяционных регистров или выборок из учетных информационных систем.

В работе на основе методики Минздравсоцразвития России по проведению медицинских информационных систем к требованиям законодательства по защите персональных данных (утверждена в декабре 2009 г.) даны практические рекомендации по созданию модели угроз как медицинской информационной системы (МИС), так и медицинского учреждения, использующего такую систему. Главы

3 и 4, которые посвящены этим вопросам, могут стать эффективным подспорьем организаторам здравоохранения и медицинским информатикам по практическому выполнению требований законодательства в части защиты персональных данных. На наш взгляд, развитие положений методических рекомендаций в части детализации методики по приведению МИС к требованиям законодательства и определение содержания контроля соответствия требований поможет медицинским организациям в кратчайшие сроки качественно завершить эти работы. Предлагаемые в 5 главе пути построения защиты информации в медицинских учреждениях являются не только предельно детализированными, но и комплексными, что обеспечивает существенную экономию средств при реализации средств защиты в практике работы учреждений.

Отрадно, что авторам удалось не только предложить практические пути решения задачи защиты информации в текущей модели функционирования учреждений, но и дать рекомендации по перспективному развитию этих систем в соответствии с утвержденной «Концепцией создания единой государственной информационной системы в сфере здравоохранения», утвержденной приказом Министра здравоохранения и социального развития Российской Федерации Т.А. Голиковой 28.04.2011 г. В заключительной главе книги рассмотрены проблемы информационной безопасности в «облачной» модели построения ряда федеральных и региональных сервисов, а также юридические и технологические аспекты перехода на электронный документооборот и вопросы придания электронным документам юридической значимости.

Актуальность и фундаментальный подход к рассмотрению предмета исследования авторами позволяет надеяться на практическую пользу данной работы для широкого круга читателей от студентов медицинских ВУЗов до практиков организации здравоохранения и медицинской информатики.

Директор по ИТ МИАЦ РАМН,
к.т.н., с.н.с., доцент НИУ ВШЭ
действительный государственный советник 3 класса
О.В. Симаков

ŋqddʎǝɐʎ bƎ dǝdƎbʎɜǝ b ǝɐɔqɐɔʎ Ɉqddʎqʎǝ̀

ОГЛАВЛЕНИЕ

Предисловие 3

Предисловие авторов 6

Основные понятия, используемые в книге 8

Введение 15

1. Предмет исследования. медицинские информационные системы 19

1.1. Краткая история развития информатизации медицинских учреждений 19

1.2. Виды медицинских информационных систем 21

1.3. Электронная медицинская карта и МИС 23

1.4. Необходимость интеграции информационных систем . 31

1.5. Электронная история болезни 37

2. Требования по защите медицинских информационных систем 41

2.1. Основные источники медицинской информации как информации ограниченного доступа 41

2.2. Классификация типов информации в МИС ЛПУ с точки зрения информационной безопасности 43

2.2.1. Информация пациента 43

2.2.2. Информация сотрудника ЛПУ 48

2.2.3. Информация блока ИТ 49

2.3. Виды конфиденциальной информации в типовом ЛПУ 49

2.4. Требования по защите коммерческой тайны 52

2.5. Требования законодательства по защите врачебной тайны 55

2.6. Требования законодательства по защите персональных данных 58

2.7. Соотношение требований 60

3. Защита информации в ЛПУ: подготовительный этап 66

3.1. Выделение основных потоков информации — где и как появляются персональные данные и другие виды конфиденциальной информации 68

3.2. Методика Минздравсоцразвития России по приведению медицинских информационных систем к требованиям законодательства по защите персональных данных 73
3.3. Определение мероприятий по защите персональных медицинских данных в медицинской информационной системе 86
3.4. Организационные мероприятия по защите персональных медицинских данных в медицинской информационной системе 87
3.5. Роль руководства ЛПУ и кадровые вопросы 89

4. Учет специфики МИС для приведения ее в соответствие требованиям законодательства 94
4.1. Базовые критерии классификации медицинских информационных систем 94
4.2. Формирование полного перечня угроз безопасности персональных данных 98
4.2.1. Классификация угроз безопасности персональных данных 98
4.2.2. Содержание модели угроз верхнего уровня 105
4.2.3. Категории и возможности нарушителей 105
4.2.4. Полный перечень возможных угроз безопасности для медицинских информационных систем 108
4.3. Определение уровня исходной защищенности 111
4.4. Расширенные критерии классификации медицинских информационных систем 112
4.5. Определение вероятности реализации, коэффициентов реализуемости и показателей опасности угроз 113
4.6. Определение перечня актуальных угроз 118
4.7. Методика по приведению МИС к требованиям законодательства 121

5. Построение системы защиты информации в ЛПУ . . . 129
5.1. Основной объект защиты, типовой состав системы защиты информации 129
5.2. Использование типовых решений при защите информационных систем персональных данных ЛПУ 132
5.3. Некоторые типовые решения по защите ПДн в МИС . 133
5.4. Защита баз данных, содержащих персональные данные 143

6. Перспективы развития МИС и систем защиты информации . . . 163
6.1. Проблема информационной безопасности в «облаках» 164
6.2. Вопросы архитектуры и состава средств защиты информации для Системы и «облачных» вычислений . . 165
6.3. Вопросы обеспечения юридической значимости первичных медицинских документов . . . 168
6.3.1. Юридическая значимость бумажного документооборота . . . 168
6.3.2. Правовые аспекты электронного взаимодействия . 172
6.4. Вопросы идентификации и аутентификации . . . 179
Заключение . . . 189
Нормативная документация . . . 190
Литература . . . 196