УДК 004.056

В.Д. Зыков, К.О. Беляков, Ю.П. Ехлаков

Методика по приведению медицинских информационных систем к требованиям законодательства в области защиты персональных данных

Рассмотрена разработанная методика по приведению медицинских информационных систем к требованиям законодательства в области защиты персональных данных, основанная на технологии типовых решений.
Ключевые слова: информационная безопасность, медицинские информационные системы, персональные данные.

В последние годы остро встал вопрос защиты персональных данных (ПДн) граждан, обрабатываемых в информационных системах персональных данных (ИСПДн). Этому способствует бурное развитие рынка самих ИСПДн, рост количества преступлений в сфере высоких технологий и требования законодательства.

Особое место среди ИСПДн занимают медицинские информационные системы (МИС), поскольку в них обрабатываются персональные медицинские данные (ПМДн) – сведения о состоянии здоровья граждан, которые относятся к врачебной тайне.

В соответствии с требованиями действующего законодательства [1–3], каждое учреждение – владелец МИС должно провести необходимые организационные и технические мероприятия для защиты ПМДн от неправомерных действий (рис. 1) [4].

Среди этих этапов наиболее важным является предпроектное обследование, поскольку является отправной точкой для последующих мероприятий. Наибольшую сложность для учреждений системы здравоохранения на этапе предпроектного обследования составляет процесс построения модели угроз, т.к. он требует проведения обследования специалистами по защите информации (рис. 2).

Практика организаций-операторов ПДн показывает высокую эффективность разработки типовых решений по защите ИСПДн для больших территориально распределенных систем, например для типовых региональных филиалов организации. Такой подход позволяет снизить временные и финансовые затраты при внедрении системы защиты ПДн в территориально распределенные ИСПДн, в том числе при их последующем расширении (например, открытии новых филиалов), а также привести систему защиты к унифицированному виду.

Целесообразным для обеспечения защиты ПМДн представляется создание моделей и средств обеспечения управления информационной безопасностью МИС, основанных на технологии типовых решений (типизации).

Согласно Положению об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных [2] выбор и реализация методов и способов защиты информации в ИСПДн осуществляются на основе модели угроз и класса ИСПДн. Это подтверждает необходимость и достаточность того, чтобы с использованием технологии типовых решений, модели МИС с точки зрения защиты ПМДн содержали:

1. Классификацию МИС на типы.
2. Модели угроз для выявленных типов МИС.

Средства обеспечения управления информационной безопасностью МИС должны содержать методику по приведению МИС к требованиям законодательства в области защиты ПДн, основанную на типизации.

В ходе исследования было выявлено 56 типов МИС по критерию защиты ПМДн и сформировано 56 моделей угроз. Модели угроз содержат перечень угроз для МИС конкретного типа с определением вероятности реализации, опасности и актуальности каждой угрозы. Для каждой из актуальных угроз были предложены одно или несколько рекомендуемых мероприятий по их предотвращению. Для упрощения процесса классификации МИС и выбора соответствующей модели угроз разработано программное обеспечение «Модели угроз медицинских информационных систем».

Особенностью разработанной методики является использование в ней предложенной классификации МИС на типы сформированных моделей угроз и рекомендаций по нейтрализации угроз (рис. 2). Указанная особенность позволяет снизить временные и финансо-

вые затраты как при реализации мероприятий по защите ПМДн в МИС, так и при осуществлении контроля соответствия требованиям.

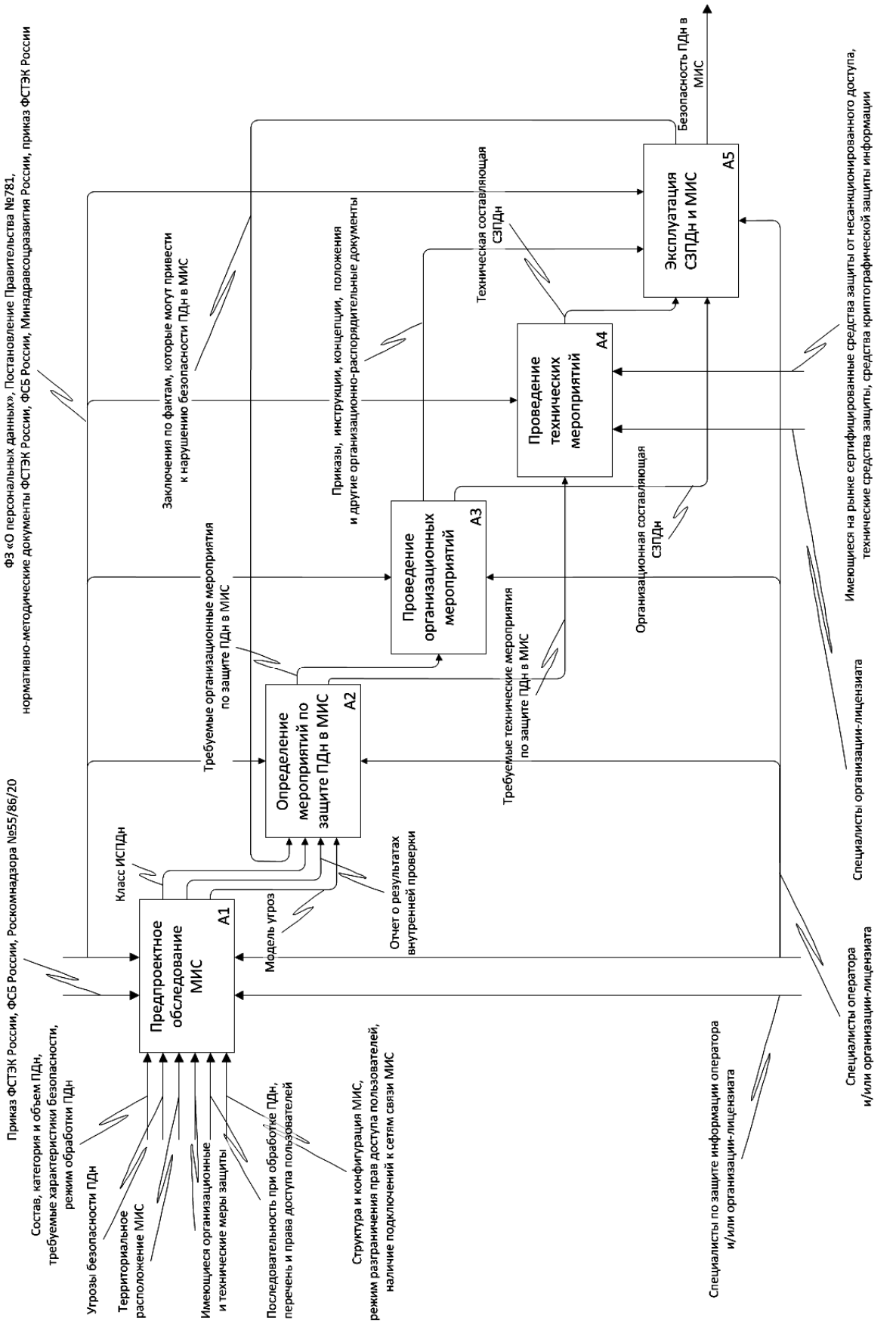

Рис. 1. Мероприятия по приведению МИС к требованиям законодательства по защите ПДн

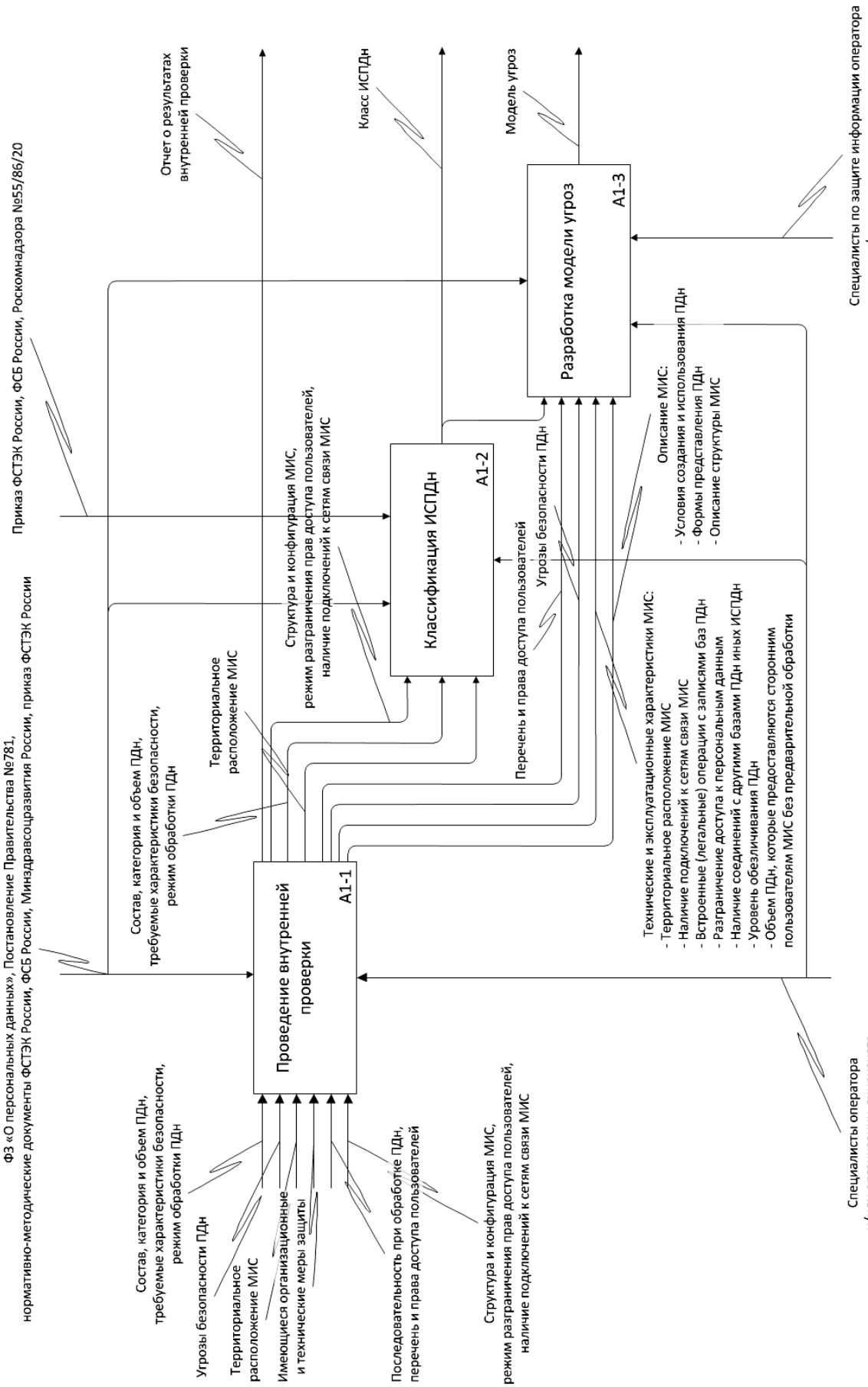

Рис. 2. Этапы проведения предпроектного обследования МИС

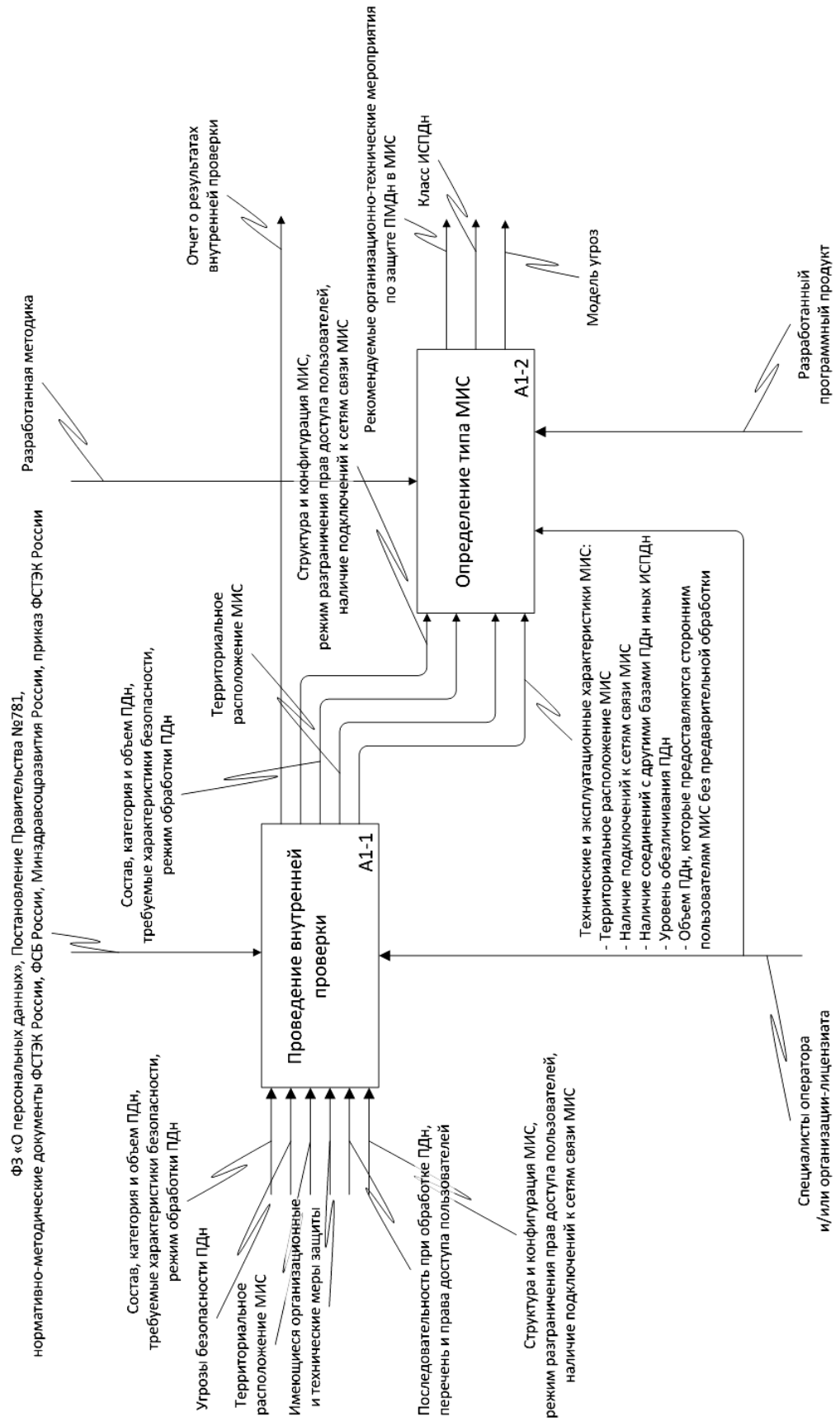

Рис. 2. Этапы проведения предпроектного обследования МИС по разработанной методике

Процедура контроля соответствия требованиям заключается в последовательном выполнении действий:

1) проведение классификации МИС с целью определения ее типа;

2) выбор соответствующей типовой модели угроз, с целью определения множества $A=\{a_1,a_2,\ldots,a_z\}$ – множества актуальных угроз; z – количество актуальных угроз и множества $B=\{b_1^{a_1},b_2^{a_1},\ldots,b_x^{a_1},\ldots,b_y^{a_z}\}$ – множества рекомендуемых мероприятий по их предотвращению; x – количество рекомендуемых мероприятий по предотвращению угрозы a_1; y – количество рекомендуемых мероприятий по предотвращению угрозы a_z;

3) определение множества $C=\{c_1,c_2,\ldots,c_u\}$ – множества реализованных мер по защите ПМДн в МИСС; u – количество реализованных мер;

4) сравнение множеств B и C и вывод о степени соответствия требованиям.

Оценка эффективности разработанной методики в ряде учреждений системы здравоохранения Томской области показала значительное сокращение времени выполнения этапа построения модели угроз при предпроектном обследовании. Одновременно отсутствовала необходимость привлечения сторонних специалистов и дополнительных финансовых затрат [5]. Оставшиеся этапы по выбору и реализации организационных и технических мероприятий выполнялись с привлечением сторонних специалистов и потребовали равные затраты, а также подтвердили отсутствие необходимости доработки моделей угроз, полученных с использованием разработанной методики.

Литература

1. Федеральный закон Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html, свободный (дата обращения: 21.05.2010).

2. Постановление Правительства Российской Федерации от 17 ноября 2007 г. №781, г. Москва «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». http://www.rg.ru/2007/11/21/personalnye-dannye-dok.html

3. Нормативно-методический документ Минздравсоцразвития России «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» от 23 декабря 2009 г. http://www.minzdravsoc.ru/docs/mzsr/informatics/5/Metodicheskie_rekomendatcii.doc

4. Зыков В.Д. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах лечебно-профилактических учреждений Томской области // Матер. докл. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2009». Томск, 12–15 мая 2009 г.: В 5 ч. – Ч. 3.– Томск: В-Спектр, 2009. – С. 255–256.

5. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 350 с.

Зыков Владимир Дмитриевич
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: (382-2) 41-25-00
Эл. адрес: zvd@udcs.ru

Беляков Константин Олегович
Финансовый директор ООО «Элекард-Мед», г. Томск
Тел.: (382-2) 49-21-98
Эл. адрес: konstantin.Belyakov@elecard.ru

Ехлаков Юрий Поликарпович
Проректор по информатизации и управлению ТУСУРа
Тел.: (382-2) 51-05-30
Эл. адрес: up@tusur.ru

V.D. Zykov, K.O. Belyakov, U.P. Ehlakov

Technique by reduction of medical information systems to requirements of the law in the field of protection of the personal data

The developed technique by reduction of medical information systems to requirements of the law in the field of protection of the personal data based on technology of typical solutions is considered in article.
Keywords: information security, medical information systems, personal data.