

Врач

и информационные
ТЕХНОЛОГИИ



Научно-
практический
журнал

№ 1
2010



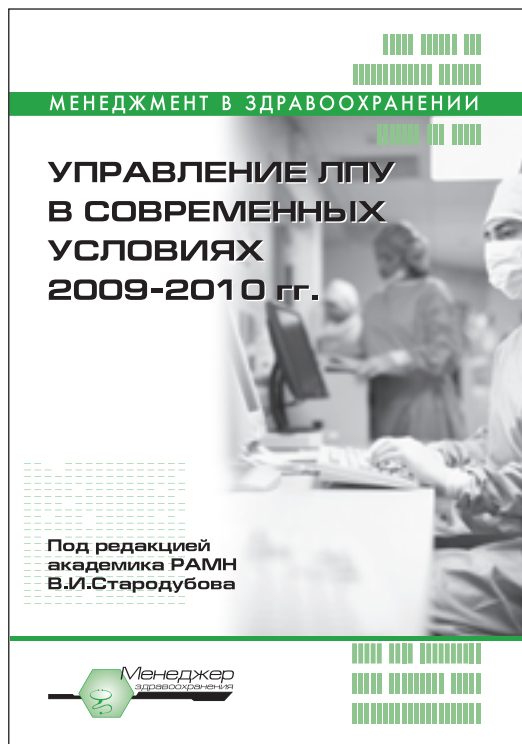
Врач

и информационные
ТЕХНОЛОГИИ

ISSN 1811-0193



9 771811 019000 >



Управление ЛПУ в современных условиях 2009-2010 гг.

Продолжающееся, ежегодно актуализируемое издание

Оглавление:

Раздел 1. *Механизмы стабилизации финансового состояния медицинских учреждений.*

Новые системы оплаты труда в здравоохранении, и перспективы замены ЕСН на страховые взносы в фонды ОМС, перевод отрасли на одноканальное финансирование через систему ОМС, введение механизмов хозяйственного расчета и «условного фондодержания» — раздел содержит анализ первых результатов апробирования на практике и оценку эффективности различных механизмов стабилизации финансового состояния медицинских учреждений.

Раздел 2. *Платные услуги в государственных (муниципальных) учреждениях здравоохранения*

В разделе даны экспертные оценки конституционности платных медицинских услуг, предложены ответы на вопросы, иско-

ренимы ли причины, вызывающие необходимость оказания платных услуг и как возможные запреты скажутся на финансовом положении медицинских учреждений.

Раздел 3. *Аутсорсинг как форма взаимодействия бюджетных медицинских учреждений со сторонними организациями*

В разделе публикуются консультации экспертов, разъясняющие суть аутсорсинга в здравоохранении, примеры практического применения аутсорсинга, методические рекомендации о порядке выведения обеспечивающих функций органов исполнительной власти и бюджетных учреждений на аутсорсинг, методика расчетов целесообразности перевода отдельных функций на аутсорсинг и расчеты на примерах конкретных бюджетных учреждений.

Раздел 4. *Обеспечение населения Российской Федерации специализированной, в том числе высокотехнологической медицинской помощью*

Предложен анализ новых тенденций и организационных мероприятий в вопросах обеспечения населения РФ высокотехнологической медицинской помощью для комплексного структурного анализа деятельности больничных учреждений и их ресурсного обеспечения, а также для решения задач повышения медицинской и социальной эффективности систем здравоохранения регионов.

Раздел 5. *Информатизация ЛПУ*

Создание государственной информационной системы персонифицированного учета оказания медицинской помощи гражданам, типовое программное обеспечение ЛПУ, правоприменительная практика в здравоохранении Федерального закона от 27.07.2006 № 152 ФЗ «О персональных данных» (далее — ФЗ № 152) — эти три актуальных вопроса информатизации ЛПУ в 2009–2010 гг. предмет рассмотрения настоящего отдела.

Раздел 6. *Антикризисное управление в здравоохранении*

В разделе рассматриваются такие элементы антикризисных мероприятий, как оптимизация затрат на оплату труда, приобретение медикаментов, перевязочных средств и других расходных материалов, организация и финансирование обновления основных фондов здравоохранения.

По вопросам приобретения обращаться: (495) 618-07-92, idmz@mednet.ru



УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Первый номер в этом году открывает большая обзорная статья Андрея Павловича Столбова, посвященная, пожалуй, одной из самых обсуждаемых и трудных проблем — исполнением федерального закона о защите персональных данных. Весь прошлый год, особенно к его концу, все находились в напряжении — что будет с уже сделанными проектами информатизации ЛПУ, что делать с запланированными и т.д. Нас пугали карательными акциями, тяжелейшими и мало кому понятными процедурами сертификации и т.д. Закон не отменили и, по большому счету, мало что в нем поправили радикально, но дали дополнительное время на подготовку. Этот материал позволит Вам окунуться в мир существующей нормативной базы и ясно представить для себя объем организационно-технических мер, которые нужно предпринимать.

Интересная статья Д. Романова и А. Борейко рассказывает об опыте внедрения медицинской информационной системы с решением проблем наличия унаследованного и устаревшего программного обеспечения. Эти проблемы, пожалуй, актуальны сейчас для очень многих проектов, так как практически не осталось ЛПУ, где бы информатизация приходила на «пустое место». Сейчас практически везде есть либо какие-то отдельные системы, либо результаты «лоскутной информатизации» — и последствия, в их самых острых проявлениях, кроются как раз в необходимости сохранения накопленных данных и переобучения пользователей. Опыт такой работы и делятся авторы в своей статье «Внедрение промышленной медицинской информационной системы с заменой морально устаревших программных решений».

Героиней нашей традиционной рубрики «Интервью с профессионалом» стала Зоя Борисовна Рахманова, руководитель Медицинского информационно-аналитического центра в составе Московского областного научно-исследовательского института (МОНИКИ) им. М.Ф. Владимирского.

Завершают номер традиционные репортажи — на этот раз с заседаний рабочей группы РАМН по вопросам создания и внедрения медицинских информационных технологий и с II Всероссийской учебно-методической конференции по преподаванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования. Материалы с этой конференции будут постепенно публиковаться на страницах «Врач и информационные технологии», так как представлены результаты, исследования и наблюдения заслуживают пристального внимания профессионального сообщества и наших читателей.

Александр Гусев, ответственный редактор

ГЛАВНЫЙ РЕДАКТОР:

Стародубов В.И., академик РАМН, профессор

ШЕФ-РЕДАКТОР:

Куракова Н.Г., д.б.н., главный специалист ЦНИИОИЗ Росздрава

ЗАМЕСТИТЕЛИ ГЛАВНОГО РЕДАКТОРА:

Зарубина Т.В., д.м.н., профессор, заведующая кафедрой медицинской кибернетики и информатики Российского ГМУ

Столбов А.П., д.т.н., заместитель директора МИАЦ РАМН

ОТВЕТСТВЕННЫЙ РЕДАКТОР:

Гусев А.В., к.т.н., заместитель директора по развитию, компания «Комплексные медицинские информационные системы»

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Виноградов К.А., профессор кафедры управления, экономики здравоохранения и фармации Красноярской государственной медицинской академии

Гасников В.К., д.м.н., профессор, директор РМИАЦ Министерства здравоохранения Удмуртской Республики, академик МАИ и РАМТН

ПЕРСОНАЛЬНЫЕ ДАННЫЕ

А.П. Столбов

Аннотированный перечень организационно-распорядительных документов по защите персональных данных в медицинском учреждении

4-20

ТЕЛЕМЕДИЦИНСКИЕ СИСТЕМЫ

В.И. Перхов, В.М. Кураева, С.А. Киреев, Е.Е. Балугев

О необходимости использования телеконсультаций при организации оказания высокотехнологичной медицинской помощи

21-29

МЕДИЦИНСКИЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Д.Н. Романов, А.А. Борейко

Внедрение промышленной медицинской информационной системы с заменой морально устаревших программных решений

30-35

Э.Ш. Салихова, М.А. Красиков, Т.Б. Шустикова, С.А. Шевченко

Информатизация здравоохранения регионального уровня на основе типовых медицинских информационных систем

36-41

Н.В. Кобляков

Разработка и внедрение дистанционной технологии социального и медицинского обслуживания пожилых людей как пример частно-государственного партнерства в системе здравоохранения

42-44

ПРЕПОДАВАНИЕ МЕДИЦИНСКОЙ ИНФОРМАТИКИ

Итоги II Всероссийской учебно-методической конференции по преподаванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования

45-46

Т.В. Зарубина, Е.Н. Николаиди

Анализ динамики преподавания медицинской информатики в учреждениях высшего и дополнительного образования Российской Федерации

47-55

Гулиев Я.И., к.т.н, директор Исследовательского центра медицинской информатики Института программных систем РАН
Емелин И.В., к.ф.-м.н., заместитель директора Главного научно-исследовательского вычислительного центра Медицинского центра Управления делами Президента Российской Федерации

Кобринский Б.А., д.м.н., профессор, руководитель Медицинского центра новых информационных технологий МНИИ педиатрии и детской хирургии МЗ РФ

Красильников И.А., д.м.н., заведующий кафедрой информатики и управления в медицинских системах Санкт-Петербургской медицинской академии последипломного образования

Кузнецов П.П., д.м.н., директор МИАЦ РАМН

Шифрин М.А., к.ф.-м.н., руководитель медико-математической лаборатории НИИ нейрохирургии им. академика Н.Н.Бурденко

Чеченин Г.И., д.м.н., профессор, член-корр. РАЕН, директор Кустового медицинского ИВЦ, заведующий кафедрой медицинской кибернетики и информатики ГИДУВ

Цветкова Л.А., к.б.н., зав. сектором отделения научно-информационного обслуживания РАН и регионов России ВИНТИ РАН

Щаренская Т.Н., к.т.н., заместитель директора по информатизации НПЦ экстренной медицинской помощи

Читатели могут принять участие в обсуждении статей, опубликованных в журнале «Врач и информационные технологии» и направить актуальные вопросы на «горячую линию» редакции.

Журнал зарегистрирован Министерством Российской Федерации по делам печати, телерадиовещания и средств массовых коммуникаций. Товарный знак и название «Врач и информационные технологии» являются исключительной собственностью ООО Издательский дом «Менеджер здравоохранения». Авторы опубликованных материалов несут ответственность за подбор и точность приведенных фактов, цитат, статистических данных и прочих сведений, а также за то, что в материалах не содержится данных, не подлежащих открытой публикации. Материалы рецензируются редакционной коллегией.

Мнение редакции может не совпадать с мнением автора. Перепечатка текстов без разрешения журнала «Врач и информационные технологии» запрещена. При цитировании материалов ссылка на журнал обязательна.

За содержание рекламы ответственность несет рекламодатель.

Издатель — ООО Издательский дом «Менеджер здравоохранения»

Адрес редакции:

127254, г.Москва,
ул. Добролюбова, д. 11, офис 406
idmz@mednet.ru
(495) 618-07-92

Главный редактор:

академик РАМН,
профессор В.И.Стародубов
idmz@mednet.ru

Зам. главного редактора:

д.м.н. Т.В.Зарубина
t_zarubina@mail.ru
д.т.н. А.П.Стоялов
stolbov@mcrarn.ru

Ответственный редактор:

к.т.н. А.В.Гусев
alexgus@onego.ru

Шеф-редактор:

д.б.н. Н.Г.Куракова
kurakov.s@relcom.ru

Директор отдела распространения и развития:

к.б.н. Л.А.Цветкова
(495) 618-07-92
idmz@mednet.ru, idmz@yandex.ru

Автор дизайн-макета:

А.Д.Пугаченко

Компьютерная верстка и дизайн:

ООО «Допечатные технологии»

Администратор сайта:

А.В.Гусев, alexgus@onego.ru

Литературный редактор:

Л.И.Чекушкина

Подписные индексы:

Каталог агентства «Роспечать» — 82615

Отпечатано в типографии
ООО «КОНТЕНТ-ПРЕСС»:
127206, Москва, Чуксин туп., 9.

© ООО Издательский дом «Менеджер здравоохранения»

ИНТЕРВЬЮ С ПРОФЕССИОНАЛОМ

Информатизация должна стать неотъемлемой частью инфраструктуры медицинского учреждения

Интервью с З.Б. Рахмановой, руководителем МИАЦ Московского областного научно-исследовательского клинического института (МОНКИ) им. М.Ф.Владимирского

56-65

КНИЖНАЯ ПОЛКА

А.П.Стоялов, П.П.Кузнецов
Автоматизированная обработка персональных данных

66

ПРОФЕССИОНАЛЬНОЕ СООБЩЕСТВО

Закон «О персональных данных»:
типовые угрозы для ЛПУ 2010 года
Репортаж о 39 заседании Рабочей группы РАМН (3 декабря 2009 г.)

67-70

Информационные системы в здравоохранении: новые видение, функции и требования
Репортаж о 40 заседании Рабочей группы РАМН (17 декабря 2009 г.)

71-73

ДИССЕРТАЦИОННЫЙ СОВЕТ
Проект Краткого паспорта научной специальности ОЗ.01.09 — «Математическая биология, биоинформатика» (физико-математические, биологические, медицинские науки)

74-75

АКТУАЛЬНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ И СТАНДАРТЫ

76-78

ПОЛЕЗНАЯ ССЫЛКА
Открыт официальный блог Минздравсоцразвития
Открыта электронная версия общественной приемной Минздравсоцразвития

79-80



А.П. СТОЛБОВ,

заместитель директора Медицинского информационно-аналитического центра РАМН,
г. Москва, stolbov@miacramn.ru

АННОТИРОВАННЫЙ ПЕРЕЧЕНЬ ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫХ ДОКУМЕНТОВ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКОМ УЧРЕЖДЕНИИ

УДК 614.2

Столбов А.П. Аннотированный перечень организационно-распорядительных документов по защите персональных данных в медицинском учреждении (Медицинский информационно-аналитический центр РАМН).

Аннотация: Представлен перечень приказов, положений, инструкций, журналов и других документов, которые должны быть разработаны в медицинском учреждении для защиты персональных данных пациентов.

Даны пояснения и рекомендации по использованию данных документов.

Ключевые слова: персональные данные, защита, медицинское учреждение, организационно-распорядительные документы

UDC 614.2

Stolbov A.P. An annotated list of organizational and administrative documents for the protection of personal data in a medical institution (Medical Information and Analytical Center of RAMS).

Abstract: We present a list of orders, regulations, instructions, journals and other documents that must be developed in a medical institution for the protection of personal data of patients. An explanation and recommendations on the use of these instruments are given.

Keywords: personal data protection, medical facility, organizational and administrative documents

Реализация требований принятого в 2006 году федерального закона «О персональных данных» предполагает создание в медицинском учреждении комплексной системы обеспечения защиты и безопасности информации. При этом необходимо подготовить и издать целый ряд организационно-распорядительных документов. Ниже представлен примерный перечень приказов, положений, инструкций, журналов и других документов, которые должны быть разработаны в учреждении, с некоторыми пояснениями и рекомендациями. Материал подготовлен на основе опыта работы и документов Медицинского информационно-аналитического центра РАМН (www.micramn.ru).

В квадратных скобках указаны нормативные ссылки на документы, их разделы, пункты и статьи, перечень которых приведен в



разделе «Нормативные ссылки». Знаками (!!!) помечены документы, которые, как это указано в [16], должны быть обязательно разработаны и утверждены в учреждении.

Используются следующие сокращения: АВС — антивирусные средства (средства обнаружения вредоносных программ-вирусов); АС — автоматизированная система; ВТСС — вспомогательные технические средства и системы, не предназначенные для передачи, обработки и хранения ПДн, устанавливаемые совместно с ТС, предназначенными для обработки ПДн, или в помещениях, в которых установлены ИС ПДн; ИС — информационная система; ОБИ — обеспечение безопасности информации; ОТСС — основные технические средства связи; ПДн — персональные данные; СВТ — средства вычислительной техники; СЗИ — средства защиты информации; ТД — техническая документация; ТС — технические средства и системы; ФСБ — Федеральная служба безопасности; ФСТЭК — Федеральная служба по техническому и экспортному контролю; ЭД — эксплуатационная документация; К1, К2 и К3 — классы информационных систем ПДн в соответствии с [3], [4].

1. Приказы

1.1. *О назначении комиссии для проведения обследования и классификации информационной системы обработки персональных данных в учреждении (!!!).*

Приказом утверждается состав комиссии, цели, задачи и сроки проведения обследования в соответствии с [3] и [4]. Основными задачами комиссии являются: **а)** инвентаризация всех информационных ресурсов в учреждении, обрабатываемых с помощью компьютеров, их категорирование — отнесение к открытой или конфиденциальной информации, в том числе к различным категориям ПДн [3], **б)** выделение всех отдельных ИС ПДн, **в)** определение класса ИС ПДн в соответствии с [3] и оформление акта классификации. См. ниже пп. 2.1, 2.3.

1.2. *Об организации автоматизированной обработки и защиты персональных данных в учреждении (!!!).*

Должен включать в том числе следующие основные пункты:

1.2.1. О назначении структурного подразделения (должностного лица), ответственного за обеспечение безопасности информации (в том числе персональных данных) в учреждении.

Назначение подразделения или должностного лица, ответственного за обеспечение безопасности ПДн, предусмотрено [2, п. 13]. Приказом должны быть утверждены положение об этом подразделении, должностные инструкции ответственного лица и администраторов безопасности информации, в которых должны быть перечислены их функции, права и обязанности, определены их подчиненность, подотчетность, и особые полномочия (статус) в части осуществления контроля за безопасностью информации по отношению к остальным пользователям ИС учреждения (см. далее пп. 3.3; 3.4; 3.5).

1.2.2. О допуске сотрудников учреждения к обработке конфиденциальной информации.

Приказом утверждается список сотрудников [2, п. 12(ж), п. 14], [5, п. 3.10] с указанием полномочий их доступа к различным категориям информации, в том числе персональным данным пациентов и работников учреждения. Для каждого сотрудника целесообразно указать его роли (их может быть несколько). Это необходимо для формирования матрицы доступа пользователей к ресурсам ИС (см. ниже п. 2.6). Внесение изменений в список также должно проводиться приказом.

1.2.3. О закреплении компьютеров, предназначенных для обработки персональных данных.

С учетом работы компьютеров в составе разных ИС ПДн (например, подсистемы учета кадров и подсистемы учета медицинской помощи/пациентов). Требования к средствам защиты информации для компьютеров (ресурсов ИС), входящих в ИС ПДн разного класса (К1, К2 и К3), различные [5].





1.2.4. Об утверждении (определении) границ контролируемой зоны, закреплении помещений, предназначенных для обработки персональных данных (в том числе, для хранения машинных носителей с ПДн).

Контролируемая зона — это пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств. Границей контролируемой зоны может быть: периметр охраняемой территории учреждения, ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения. См. ниже пп. 3.6, 4.4, 5.1.

1.2.5. Об утверждении Плана мероприятий по обеспечению безопасности информации в учреждении.

План мероприятий разрабатывается по результатам обследования ИС учреждения в части выполнения установленных требований к безопасности информации (см. выше п. 1.1). План должен быть комплексным и включать как однократно выполняемые организационные и технические мероприятия по созданию системы защиты информации, так и постоянно и периодически выполняемые мероприятия по ее эксплуатации, контролю (аудиту) безопасности, поддержанию, совершенствованию и развитию (модернизации) системы, обучению персонала по вопросам ОБИ и работе с СЗИ [2, п. 12(д)] и т.д. Должно быть предусмотрено обеспечение мероприятий плана необходимыми ресурсами, в том числе выделение соответствующих финансовых средств. Должно быть определено должностное лицо, на которое возлагается контроль за выполнением плана, например, заместитель главного врача (см. [4, раздел 4]).

1.2.6. О допуске лиц к работе с криптографическими средствами защиты информации.

Издается при использовании в учреждении сертифицированных ФСБ средств криптографической защиты информации в соответствии

с [9] и [10]. Следует заметить, что законом от 27.12.2009 № 363-ФЗ из текста первоначальной редакции закона «О персональных данных» исключено требование об обязательности применения оператором шифровальных (криптографических) средств для защиты ПДн (в ст. 19). См. также ниже пп. 3.19, 4.18, 4.19.

1.2.7. Об утверждении положений, инструкций, регламентов, форм учетных документов (журналов, ведомостей).

Примерный перечень указанных документов приведен ниже в разделах 3 (положения, инструкции) и 4 (журналы, ведомости).

1.3. *О проведении (приемочных) испытаний системы защиты информации в учреждении.*

Приказом должна быть назначена комиссия для проведения испытаний, определены сроки испытаний. В приказе должно быть указано, что испытания проводятся в соответствии с утвержденной руководителем учреждения программой и методикой испытаний системы защиты информации. По результатам испытаний оформляется протокол (см. ниже пп. 2.8, 3.20).

1.4. *О вводе в эксплуатацию системы защиты информации в учреждении.*

Издается по результатам приемочных испытаний системы, на основе протокола (акта) испытаний, содержащего заключение о готовности средств защиты информации к использованию [2, п. 12(в), (г)]. В приказе должны быть назначены ответственные за организацию технической эксплуатации системы и предусмотрено выделение необходимых ресурсов и финансовых средств. См. также п. 2.8.

1.5. *О проведении (утверждении плана) проверки выполнения мероприятий по обеспечению безопасности информации в учреждении (!!!).*

Издается в случае, если возникает необходимость проведения внеплановой проверки, не предусмотренной планом мероприятий (см. п. 1.2.5). В приказе должны быть определены



состав комиссии, цели, перечень проверяемых вопросов (программа проверки) и сроки выполнения проверки (см. также п. 2.12).

2. Отчеты, акты, перечни

2.1. Отчет (акт) о результатах обследования информационной системы учреждения (!!!).

Готовится специальной комиссией, назначаемой приказом руководителя учреждения. Должен включать перечень и основные характеристики (см. [3], [4, раздел 3]) всех информационных (под)систем, в которых обрабатываются персональные данные, — отдельных ИС ПДн, обрабатывающих ПДн разной категории и(или) с разными целями, например, о сотрудниках учреждения (данные кадрового и бухгалтерского учета, категория 3) и о пациентах (данные о состоянии здоровья, категория 1). Отчет должен содержать также: **а)** перечень сведений конфиденциального характера, обрабатываемых в учреждении (см. п. 2.2); **б)** общее, краткое описание потоков данных как внутри учреждения, так и передаваемых и получаемых в(из) внешних ИС — кто, что, кому, каким образом (как, по каким каналам, на каких носителях) и когда (с какой периодичностью) передает (получает), как учитывается (документируется) факт передачи-приема и т.д. (см. [5, п. 3.6]), в том числе возможно в виде ссылок на соответствующие документы, содержащие эту информацию (регламенты, инструкции, описание рабочих процессов и т.д.).

2.2. Перечень сведений конфиденциального характера, обрабатываемых в учреждении (!!!).

Документ разрабатывается в соответствии с требованиями [8, приложение 6] по результатам инвентаризации и категорирования информационных ресурсов учреждения, которые проводятся в рамках обследования ИС учреждения (см. п. 1.1). Должен включать перечень персональных данных сотрудников и пациентов учреждения, подлежащих защите

от несанкционированного доступа. Утверждается руководителем учреждения.

2.3. Акт классификации информационной системы персональных данных учреждения (!!!).

Утверждается руководителем учреждения. Определение класса ИС ПДн осуществляется по результатам обследования ИС учреждения в соответствии с требованиями [3], [4]. Может включать в качестве приложения отчет о результатах обследования информационной системы учреждения (см. выше п. 2.1). При наличии в учреждении нескольких ИС ПДн, обрабатывающих данные разной категории, ИС ПДн в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем [3, п. 17], [4, раздел 3]. Следует отметить, что согласно [4, раздел 3], применительно к специальным информационным системам (к ним, в том числе относятся ИС, в которых обрабатываются персональные данные о состоянии здоровья), после определения класса системы должна быть разработана модель угроз безопасности ПДн с использованием методических документов ФСТЭК и ФСБ [4], [5], [6], [7], [9] и [10], и проведена оценка актуальности угроз (см. далее п. 2.4). В специальных ИС ПДн, помимо требований конфиденциальности, предъявляются также требования целостности (защиты от уничтожения и искажения) и(или) постоянной доступности данных для использования.

2.4. Модель угроз безопасности персональных данных и иной конфиденциальной информации в учреждении (!!!).

Угрозы безопасности персональных данных — это совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информацион-



ной системе персональных данных. Модель угроз — это перечень возможных угроз безопасности информации. Исходными данными для разработки модели является отчет по результатам обследования ИС, методической основой для разработки модели являются [4, раздел 4], [6], [7], [15], [16] и [17]. Следует подчеркнуть, что согласно [15] медицинская информационная система в лечебно-профилактическом учреждении при количестве пациентов (субъектов ПДн) менее 100 тысяч может быть отнесена к специальной ИС ПДн с требованиями по обеспечению безопасности ПДн, в основном соответствующими классу КЗ (полагается, что: **а**) принятие юридически значимых решений осуществляется исключительно только на основе бумажных медицинских документов; **б**) нарушение безопасности обрабатываемых ПДн может привести к незначительным негативным последствиям для пациентов). Модель угроз утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации.

2.5. Требования по обеспечению безопасности информации (персональных данных).

Разрабатываются в соответствии с [4, раздел 4] и [5] на основе присвоенного ИС ПДн класса (К1, К2 или К3) и частной модели угроз безопасности ПДн (см. выше п. 2.4). Документ должен включать перечень организационных мер и требования к программным, и техническим средствам защиты информации в соответствии с [5, раздел 4], на основе которых определяется состав и осуществляется выбор средств защиты и(или) разрабатывается техническое задание на создание (модернизацию) системы защиты информации в учреждении. На основе этого документа осуществляется также оценка соответствия

ИС ПДн требованиям по безопасности информации. Документ утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации и включается в состав комплекта технической документации на систему защиты информации в учреждении (см. далее раздел 5).

2.6. Матрица доступа к ресурсам информационной системы учреждения* (!!!).

Ресурс ИС — это именованный элемент информационного, системного и прикладного программного, и аппаратного обеспечения информационной системы (объект доступа). Матрица доступа [5] должна разрабатываться на основе принятой в учреждении политики разграничения полномочий доступа пользователей к ресурсам ИС (при многопользовательском режиме и разными правами доступа). Для медицинских учреждений рекомендуется разрешительная политика ролевого разграничения прав доступа пользователей (субъектов доступа) к ресурсам ИС («запрещено все, что явно не разрешено»). В связи с этим матрица доступа обычно представляется в виде совокупности таблиц двух типов записей (все ресурсы ИС и субъекты доступа известны, идентифицированы и именованы): **а**) роль (должность) — ресурс ИС — полномочия (создание, изменение, удаление, чтение, запись, копирование, печать, пересылка, запуск приложения и т.д.); **б**) роль — пользователь (он может выполнять несколько ролей). Матрица утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации, ответственного за ведение матрицы. Является основой для настройки применяемых в ИС средств управления доступом к ресурсам ИС. Актуализация матрицы доступа осуществляется на основе

* В [16] рекомендуется разрабатывать «Положение о разграничении прав доступа к обрабатываемым персональным данным...» [16, приложение 10], которое представляет собой приказ о допуске персонала к обработке конфиденциальной информации, оформленный в виде таблиц матрицы ролевого доступа к ресурсам ИС при многопользовательском режиме и разными правами доступа [5] (см. выше п. 1.2.2).



приказа руководителя учреждения о допуске сотрудников к обработке конфиденциальной информации (см. выше п. 1.2.2).

2.7. Акт(ы) установки сертифицированных средств защиты информации в учреждении.

Документально подтверждает то, что сертифицированные средства защиты информации были установлены, настроены и введены в действие (эксплуатацию) организацией-лицензиатом ФСТЭК или ФСБ (для средств криптографической защиты).

2.8. Протокол (акт) приемочных испытаний системы защиты информации в учреждении.

См. выше п. 1.3. При положительных результатах испытаний является основанием для: **а)** издания приказа о вводе системы защиты информации учреждения в эксплуатацию (см. выше п. 1.4); **б)** оформления декларации подтверждения соответствия информационной системы учреждения требованиям по безопасности информации для систем класса КЗ (см. далее п. 2.11).

2.9. Технический паспорт на аттестуемую автоматизированную систему.

Необходим для проведения аттестации на соответствие требованиям по безопасности информации для ИС ПДн классов К1 и К2. Содержание и форма технического паспорта АС приведены в [8, приложение 5]. Утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации.

2.10. Аттестат соответствия информационной (автоматизированной) системы требованиям по безопасности информации.

Аттестация проводится для ИС ПДн классов К1, К2 уполномоченными организациями-лицензиатами ФСТЭК. Содержание и форма аттестата приведены в [8, приложение 2]. Устанавливается соответствие требованиям по безопасности информации согласно руководящему документу «Автоматизированные системы. Защита от несанкционированного

доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия РФ, 1992 г.). Аттестат может содержать запись о соответствии классу ИС ПДн. Для аттестации АС необходимо предъявить следующие основные документы: приемо-сдаточную документацию на объект информатизации (АС); акты категорирования выделенных помещений и объект информатизации; инструкции по эксплуатации СЗИ; технический паспорт на аттестуемый объект [8, приложение 5]; документы, регламентирующие организацию пропускного режима и допуска в служебные помещения учреждения; нормативные и организационно-распорядительные документы по защите информации и контролю ее эффективности в учреждении.

2.11. Декларация подтверждения соответствия информационной системы учреждения требованиям по безопасности информации.

Оформляется по результатам приемочных испытаний системы защиты информации для ИС ПДн класса КЗ. По форме и содержанию декларация аналогична аттестату соответствия информационной (автоматизированной) системы требованиям по безопасности информации (см. п. 2.10). Утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации.

2.12. Акт (отчет) по результатам внутренней проверки (внешнего аудита) выполнения мероприятий по обеспечению безопасности информации.

См. выше п. 1.5. В акте должны быть отражены результаты проверки (аудита) в соответствии с поставленными целями (программой) проверки. Аналогичный акт может быть составлен также по результатам разбирательства случаев нарушения (инцидентов) безопасности информации (см. п. 3.18). При этом в журнале учета инцидентов указывается ссылка на этот акт (см. п. 4.10).



2.13. Акт(ы) выполнения работ по техническому обслуживанию средств защиты информации.

Оформляется в случае, если указанные работы выполнялись организацией-лицензиатом ФСТЭК или ФСБ (для средств криптографической защиты). При этом делается также соответствующая запись в журнале учета мероприятий по техническому обслуживанию средств ИС учреждения. См. также ниже пп. 4.15, 4.16, 5.6–5.9.

2.14. Акт(ы) об уничтожении персональных данных.

Оформляется в случае отзыва пациентом согласия на обработку его ПДн в учреждении [1, ч. 5 ст. 21]. Процедура уничтожения ПДн пациента может быть описана в «Положении о защите персональных данных пациентов и работников учреждения» или в «Порядке оформления, учета и хранения письменного согласия пациента на обработку его персональных данных в медицинском учреждении» (см. ниже пп. 3.2, 3.7, 4.5).

2.15. Копия «Уведомления об обработке персональных данных», направленного учреждением (оператором) в территориальный орган Роскомнадзора* (!!!).

Копия уведомления должна быть зарегистрирована по принятым в учреждении правилам учета и хранения документов.

2.16. Выписка из Реестра операторов персональных данных*.

Порядок получения выписки определяется Приказом Роскомнадзора от 28.03.2008 № 154 «Об утверждении положения о ведении Реестра операторов, осуществляющих

обработку персональных данных» (п. 17 приказа). Выписку из Реестра операторов можно найти и скачать с сайта <http://pd.rsoc.ru>, распечатать и зарегистрировать по принятым в учреждении правилам учета и хранения документов.

2.17. Лицензия на техническую защиту информации.

Под технической защитой информации понимается комплекс мероприятий и(или) услуг по ее защите от несанкционированного доступа, в том числе и по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней [11, п. 2]. Лицензия необходима для операторов, эксплуатирующих ИС ПДн классов К1, К2, в также для распределенных систем класса К3 [5, п. 3.14]. Распределенными являются ИС, в которых взаимодействие между элементами ИС (компьютерами) осуществляется с использованием линий связи (сетей), выходящих за пределы контролируемой зоны и(или) по каналам связи (сетям) общего пользования. Лицензия выдается учреждению (оператору) уполномоченными организациями-лицензиатами ФСТЭК сроком на пять лет.

3. Положения, инструкции, регламенты

3.1. Положение (политика) об информационной безопасности в учреждении.**

Основной документ, в котором формулируются общие требования, принципы организации и подходы к обеспечению безопасности информации, порядок доступа различ-

* Копия уведомления и выписка из реестра операторов предъявляются при проведении внешнего аудита и контрольно-надзорных мероприятий за соблюдением требований к безопасности персональных данных. На портале Роскомнадзора www.rsoc.ru реализованы функции получения в электронном виде государственных услуг «Оформление уведомления об обработке (намерении осуществлять обработку) персональных данных» и «Получение выписки из реестра операторов персональных данных».

** В [16] наряду с «Положением (политикой) ...» рекомендуется разрабатывать также «Концепцию информационной безопасности ...». Нам представляется это излишним, поскольку все ключевые требования, основные организационные аспекты и принципиальные положения по обеспечению безопасности информации в учреждении, то есть концепцию информационной безопасности, можно изложить в одном документе — Положении (политике).



ных категорий пользователей к конфиденциальным данным и ресурсам информационной системы в учреждении с учетом специфики его деятельности, меры ответственности за нарушение установленного режима обеспечения безопасности информации и т.д. В положении должно быть определено, когда, как и кем проводится инструктаж и доведение до сотрудников требований и документов по соблюдению установленных требований к защите информации, проведение контроля и т.п. Документ должен содержать перечень всех организационно-методических и учетных документов (инструкций, положений, журналов, ведомостей и др.), определяющих требования к защите информации и регламентирующих процессы обработки конфиденциальных данных в учреждении. Утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации. Политика безопасности информации в учреждении разрабатывается в соответствии с [5, п. 3.4] и [12, п. 2.4.4]. Рекомендации по содержанию документа приведены в [13, приложение А].

3.2. Положение о защите персональных данных пациентов и работников учреждения* (!!!).

В рекомендациях [4, раздел 4] этот документ назван как «Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИС ПДн». Разрабатывается в соответствии с требованиями нормативных правовых актов, определяющих требования к обеспечению прав и свобод граждан при обработке их персональных данных, в том числе при оказании медицинской помощи («Основы законодательства Российской Федерации об охране здоровья граждан» (ст. 61), закон «О меди-

цинском страховании граждан в Российской Федерации» (ст. 12) и др. — для пациентов), а также требований Трудового кодекса РФ (ст.ст. 85–90), нормативно-методических и распорядительных документов по организации ведения федерального регистра медицинских и фармацевтических работников, ведению кадрового и бухгалтерского учета (для работников учреждения). Должно содержать требование оформления письменного обязательства сотрудника учреждения о неразглашении конфиденциальной (служебной) информации (может оформляться в виде специального пункта в трудовом договоре). Утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации.

3.3. Положение о подразделении по защите информации в учреждении (!!!).

Разрабатывается, если такое подразделение предусмотрено в организационно-штатной структуре учреждения (см. выше п. 1.2.1). В ином случае функции по методическому обеспечению, организации технического обслуживания и администрированию средств защиты информации, технической поддержке и контролю пользователей возлагаются на подразделение, в состав которого включены сотрудники, выполняющие функции администраторов системы защиты информации, имеющие необходимую квалификацию и профессиональную подготовку.

3.4. Инструкция администратору безопасности информации (!!!).

Помимо должностных обязанностей администратора безопасности (функции, права, обязанности, ответственность) и требований к его компетенции (квалификации, знаниям и умениям), инструкция должна включать пере-

* Возможно также: а) включение (оформление) этого положения в виде соответствующего(их) раздела(ов) в Положение об (политике) информационной безопасности в учреждении (см. выше п. 3.1), б) разработка двух специальных, отдельных документов (положений) — по пациентам и по работникам (в нормативно-методических документах уполномоченных федеральных органов исполнительной власти явных требований и ограничений относительно этого нет).



чень применяемых мер и средств защиты информации, обслуживаемых администратором, с указанием ссылок на инструкции (руководства) по их эксплуатации, а также описание порядка его взаимодействия с пользователями ИС и руководством учреждения, в том числе возможно в виде ссылок на другие документы (инструкции, положения и т.д.). В инструкции должно быть явно описано (перечислено) все, что разрешено и запрещено делать администратору безопасности в различных ситуациях с ресурсами ИС и средствами защиты информации. Следует подчеркнуть, что в общем случае администратор безопасности не имеет полномочий для работы с персональными данными (их ввода, изменения, удаления). Он, в силу своих обязанностей, может выполнять с ними только чисто технологические операции (действия). Инструкция утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации (см. п. 1.2).

3.5. Инструкция пользователю информационной системы по защите информации* (!!!).

Для каждой отдельной ИС ПДн в учреждении целесообразно разработать свою инструкцию. Инструкция должна содержать: требования к компетенции (квалификации, знаниям и умениям), права, общие обязанности и правила работы пользователя ИС в части обеспечения безопасности информации; меры ответственности пользователя за несоблюдение установленных требований безопасности; перечень всех применяемых мер и средств защиты информации с указани-

ем их назначения и возможностей, а также ссылок на инструкции (руководства) по их эксплуатации (в том числе использованию паролей, средств антивирусной защиты, работы с внешними носителями данных, пользованию электронной почтой, Интернетом, ведению журналов учета и т.д.); описание порядка взаимодействия пользователя с администраторами безопасности информации. Для каждой категории (ролевой группы) пользователей ИС ПДн в инструкции должно быть явно описано (перечислено) все, что разрешено и запрещено делать пользователю в различных ситуациях с ресурсами ИС и средствами защиты информации. Инструкция должна быть согласована с администратором безопасности информации, утверждена руководителем учреждения и доведена (изучена) под подпись до каждого пользователя. Периодически необходимо проверять знание инструкции пользователями ИС.

3.6. Положение (инструкция) по организации пропускного режима и порядке допуска в служебные помещения в учреждении.

В документе должно быть определено, что помещения, в которых установлены компьютеры и хранятся машинные носители данных, предназначенные для обработки конфиденциальной информации (ПДн), должны охраняться, иметь замки и, возможно, средства сигнализации, решетки на окнах и т.д. Вскрытие и закрытие таких помещений должно осуществляться под подпись в журнале по спискам, утвержденным руководителем учреждения.

3.7. Порядок оформления, учета и хранения письменного согласия пациента на

* В должностные инструкции всех сотрудников учреждения должны быть включены требования по обеспечению конфиденциальности информации, в том числе, возможно, со ссылками на документы по защите информации в учреждении. В общем случае в учреждении целесообразно иметь специальный технологический регламент обработки данных в каждой ИС ПДн (см. [5, п. 3.6], а также п. 2.1). В инструкции по учету и хранению документов (делопроизводству) в учреждении должен быть определен порядок работы с документами, содержащими персональные данные (см. «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждено постановлением Правительства РФ от 15.09.2008 г. № 687).



обработку его персональных данных в медицинском учреждении*.

Инструкция должна содержать описание процедур получения (оформления), учета (регистрации) и порядка хранения письменного согласия пациента медицинского учреждения, образец оформления согласия пациента, а также порядок отзыва этого согласия в соответствии с требованиями закона [1, ст.ст. 6, 9, 10]. Должно быть предусмотрено ведение (формирование) ведомости пациентов, давших и отозвавших согласие на обработку их ПДн, а также регистрация фактов уничтожения ПДн по требованию пациента [1, ч. 5 ст. 21] (см. пп. 2.14, 4.5). Целесообразно автоматизировать формирование (заполнение реквизитов) и печать письменного согласия пациента на обработку его персональных данных в регистратуре или приемном отделении учреждения, а также формирование и печать ведомости пациентов, давших и отозвавших согласие на обработку их ПДн. В поликлинике письменное согласие можно оформлять при первом обращении пациента и оформлении амбулаторной карты, в стационаре — при каждом случае госпитализации в виде вкладыша в историю болезни.

3.8. Порядок информирования пациентов об обработке их персональных данных в медицинском учреждении.

Информирование пациентов об обработке их персональных данных (цели, способы и сроки обработки, список лиц, имеющих доступ к их ПДн) осуществляется по их запросам (обращениям) в соответствии с требованиями закона [1, ст.ст. 14, 20]. В документе должны быть определены порядок учета обращений и информирования пациентов, и ответственные за подготовку и предоставление указанных сведений пациентам (журнал учета, см. ниже п. 4.6). Целесообразно авто-

матизировать формирование и печать документа, содержащего указанные сведения, например, на основе приказа о допуске сотрудников к ПДн (см. п. 1.2.2) или матрицы доступа к ресурсам ИС (см. п. 2.6).

3.9. Инструкция по использованию электронной почты общего пользования в учреждении.

В инструкции должно быть указано, что использовать открытую (обычную) электронную почту для передачи ПДн без применения сертифицированных ФСБ средств криптографической защиты информации категорически запрещается.

3.10. Инструкция по использованию защищенной (корпоративной) сети передачи данных.

Разрабатывается при использовании защищенной корпоративной сети передачи данных (например, VPN, Virtual Private Network), в том числе электронной почты, например, «Деловой почты» в составе программного продукта ViPNet. В инструкции должен быть описан порядок передачи сообщений (файлов), в том числе ведение журнала приема/передачи сообщений, содержащих ПДн, и определена форма этого журнала (см. п. 4.7). Как правило, разрабатывается на основе типовой инструкции для данной корпоративной защищенной сети.

3.11. Инструкция по работе с Интернетом в учреждении.

Для упрощения и удешевления системы защиты информации доступ в Интернет рекомендуется осуществлять только со специально выделенных компьютеров, изолированных от сегментов локальной вычислительной сети (компьютеров) учреждения, в которых осуществляется обработка персональных данных и иной конфиденциальной информации, либо с компьютеров, связанных с этими сегментами

* Следующие два документа можно: а) объединить в один — «Положение об организации информирования, оформления, учета и хранения письменного согласия пациента на обработку его персональных данных в медицинском учреждении» либо б) включить в виде соответствующих разделов в «Положение о защите персональных данных пациентов и работников учреждения» (см. п. 3.2).





сети через специальные сертифицированные межсетевые экраны (см. [4], [5]).

3.12. Инструкция по использованию средств антивирусной защиты.

Требования к антивирусным средствам (АВС) изложены в [5, раздел 4]. Инструкция разрабатывается с учетом особенностей используемых АВС, способов и регламентов обмена данными как внутри учреждения, так и с внешними организациями, должна включать перечень используемых АВС и ссылки на инструкции по их эксплуатации, подготовленные их разработчиками (поставщиками). См. также ниже п. 4.13.

3.13. Инструкция по организации парольной защиты в информационной системе учреждения.

Разрабатывается в соответствии с утвержденной политикой безопасности и требованиями используемых программно-технических средств — подсистем управления доступом к ресурсам ИС. Инструкция должна содержать требования к учетным именам и паролям пользователей, определять порядок генерации паролей, периодичность их смены, а также порядок замены в случае их компрометации (см. [5, раздел 4]). См. также далее п. 4.14.

3.14. Инструкция по учету, хранению и использованию машинных носителей данных, содержащих сведения конфиденциального характера.

В инструкции должны быть определены правила маркировки и идентификации носителей, форма журнала учета носителей (см. ниже п. 4.11), предусмотрена систематическая проверка их наличия и работоспособности, порядок выдачи и ответственность пользователей за их сохранность и несанкционированное использование. В инструкции должно быть четко определено, какие данные могут быть записаны (выгружены) на носитель, в том числе указано, что данные, относящиеся к разным ИС ПДн, должны храниться на физически разных (отдельных) машинных носителях. Носители данных, содержащих

конфиденциальную информацию, должны храниться в сейфах и(или) специальных охраняемых помещениях (см. п. 1.2.4). Документ должен включать также описание процедуры (порядок) стирания информации, снятия с учета и утилизации носителей данных [8, п. 5.2.6, п. 5.3.6].

3.15. Инструкция по резервному копированию и восстановлению данных в информационной системе учреждения (!!!).

Документ должен определять, кем осуществляется резервное копирование (восстановление), включать график копирования, описание правил или ссылки на инструкции по эксплуатации используемых средств копирования/восстановления данных, а также порядок хранения и учета машинных носителей с резервными копиями, в том числе, возможно, в виде ссылок на инструкцию по учету и хранению машинных носителей данных (см. п. 3.14). В инструкции, помимо всего прочего, следует определить, что носители данных с резервными копиями должны храниться вне помещений, в которых размещены серверы (компьютеры) ИС, дабы при возникновении чрезвычайных ситуаций, в результате которых может произойти физическое разрушение носителей данных или серверов (компьютеров), например, при пожаре, затоплении и т.п., сохранилась хотя бы одна копия критически важных данных — на сервере (компьютере) или внешних машинных носителях. См. также п. 4.12.

3.16. Положение (инструкция) о порядке работы с электронным журналом регистрации и учета обращений (запросов) пользователей информационной системы учреждения к персональным данным (!!!).

Необходимость использования этого электронного журнала определена в [2, п. 15]. Порядок использования электронного журнала должен быть отражен в положении (политике) об информационной безопасности и инструкциях администраторам системы защиты информации (безопасности). В положении должно быть указано, кем, каким образом и с какой



периодичностью просматривается журнал, какие действия осуществляются при обнаружении инцидентов, связанных с нарушением режима защиты информации (см. ниже п. 3.18), а также каким образом проводятся работы по его техническому обслуживанию. Утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации. Электронный журнал автоматического учета обращений к персональным данным может быть реализован с помощью сертифицированных средств аутентификации пользователей, управления доступом, регистрации и учета, например, таких как «Панцирь-С», «Secret Net» и др. (реестр сертифицированных средств защиты информации опубликован на сайте ФСТЭК www.fstec.ru). В документе должны быть приведены также образцы экранных и печатных форм (отчетов), формируемых на основе учетных данных в журнале. См. п. 4.1.

3.17. Регламент (инструкция) учета записи на внешние носители информации и печати документов, содержащих персональные данные.

В соответствии с установленными требованиями автоматическая регистрация в электронном журнале действий, связанных с записью на внешние носители или печатью документов, содержащих персональные данные, должна выполняться только для систем классов К1 (см. [5, пп. 4.2.4(б), 4.2.7(б)]) и К2 при многопользовательском режиме обработки ПДн с разными правами доступа (см. [5, пп. 4.2.9(б)]). Для систем класса К3 это требование не обязательно. Поэтому Регламент в обязательном порядке разрабатывается только для указанных классов ИС ПДн, а для систем класса К3 — по усмотрению руководителя учреждения. Регламент должен содержать форму журналов учета печати документов и записи ПДн на внешние машинные носители информации (см. далее пп. 4.8, 4.9). Следует заметить, что при записи на внешние носители рекомендуется шифровать ПДн с

использованием сертифицированных ФСБ криптографических средств (см. далее п. 3.19). В тех случаях, когда внешние носители данных хранятся и передаются доверенным способом, исключающим их утрату (утерю) или несанкционированное использование, шифрование не требуется. Не надо также шифровать данные при записи на внешний носитель, выдаваемый на руки пациенту под его роспись в журнале учета (см. п. 4.8).

3.18. Инструкция по действиям в нестандартных ситуациях, связанных с нарушениями функционирования системы безопасности информации.

Документ должен содержать перечень, описание признаков и классификацию инцидентов, связанных с нарушением режима или изменением показателей функционирования системы безопасности информации, в зависимости от последствий, порядок учета инцидентов (ведение журнала, см. п. 4.10), а также описание действий по восстановлению нормального функционирования системы. Действия целесообразно сгруппировать по различным категориям пользователей и персонала (администраторов) ИС. Для каждой категории может разрабатываться отдельная инструкция. Документ должен включать описание процедуры (регламент) проведения разбирательств по фактам несанкционированного доступа (утечки) информации [4, раздел 4]. Утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации.

3.19. Инструкция по использованию средств криптографической защиты информации.

Разрабатывается при использовании в учреждении сертифицированных ФСБ средств криптографической защиты (шифрования) информации в соответствии с требованиями [9], [10]. Инструкция должна содержать также порядок работы с ключевой информацией. Обычно разрабатывается при участии организации-лицензиата ФСБ — поставщика





криптосредств. Утверждается руководителем учреждения с согласующей подписью ответственного за использование криптосредств. См. также пп. 1.2.6; 4.18; 4.19.

3.20. Программа и методика испытаний информационной системы учреждения по требованиям безопасности информации.

Разрабатывается в соответствии с [14, раздел 4]. Утверждается руководителем учреждения с согласующей подписью представителя подразделения (ответственного) по защите информации. В программе испытаний должны быть предусмотрены проверки всех подсистем и средств защиты информации, наличие необходимой эксплуатационной (технической) документации, а также критерии и способы оценки соответствия ИС ПДн установленным (заданным) требованиям безопасности информации (ПДн) при ее обработке в ИС учреждения. Программа может использоваться не только при проведении приемочных испытаний, но также и при выполнении плановых контрольных и проверочных мероприятий по оценке состояния системы защиты информации (в полном объеме или частично). См. также пп. 1.3, 2.8, 2.7.

4. Журналы, ведомости

Ведение журналов учета и ведомостей осуществляется в соответствии с положениями, инструкциями, должностными обязанностями и иными организационно-распорядительными документами, в которых должны быть определены форма журнала, кем он ведется, кем и когда проверяется, а также указаны средства автоматизированного ведения (формирования) и анализа (мониторинга) журнала.

4.1. Электронный журнал учета обращений (запросов) пользователей ИС учреждения к персональным данным (!!!).

См. пояснения к п. 3.16. Электронный журнал — это своего рода «черный ящик». Знание того, что все действия с защищаемыми ресурсами ИС авторизуются и регистрируются

в общем случае способствует созданию у пользователей мотивации к корректной работе и неукоснительному выполнению установленных правил и регламентов («фактор неотказуемости»).

4.2. Журнал учета мероприятий по обеспечению безопасности информации в учреждении (!!!).

В журнале учитываются как плановые, так и ситуационно выполненные мероприятия, учет которых не предусмотрен в других журналах, в частности, контрольные проверки (см. далее).

4.3. Журнал учета инструктажа сотрудников учреждения по обеспечению режима защиты информации.

В журнале учитываются как индивидуальные, так и коллективные формы инструктажа (занятия, семинары, тренинги, зачеты, допуск к работе с СЗИ и т.д.). В виде отдельного раздела в журнале ведется ведомость ознакомления сотрудников учреждения с документами по защите информации (под подпись).

4.4. Журнал(ы) учета сдачи под охрану и вскрытия служебных помещений.

Одновременно могут вестись несколько журналов — в зависимости от размещения помещений в здании(ях), организации охраны и пропускного режима в учреждении.

4.5. Ведомость учета пациентов, давших и отзывавших согласие на обработку их персональных данных.

См. пояснения к п. 3.7. В случае отзыва пациентом согласия на обработку ПДн [1, ч. 5 ст. 21] в журнале делается отметка об уничтожении оператором его ПДн, в порядке и на условиях, как это предусмотрено в согласии. Факт уничтожения ПДн пациента оформляется в виде акта (см. выше п. 2.14). В журнале должна быть также сделана запись об уведомлении пациента о прекращении обработки и уничтожении его ПДн [1, ч. 5 ст. 21], если иное не предусмотрено в согласии или в отзыве согласия пациента на обработку его ПДн.



4.6. Журнал учета обращений и информирования пациентов об обработке их персональных данных в учреждении (!!!).

См. пояснения к п. 3.8. По каждому случаю обращения (запроса) пациента должна быть сделана запись о факте его информирования (ответе). В этом же журнале могут учитываться также обращения органов Роскомнадзора в учреждение за аналогичной информацией об обработке персональных данных (см. [1, ст. 23]).

4.7. Журнал учета обмена электронными сообщениями (документами) по защищенной сети передачи данных.

См. пояснения к п. 3.10. Целесообразна автоматизация ведения, формирования и печати этого журнала.

4.8. Журнал учета записи (копирования) персональных данных на внешние машинные носители*.

См. пояснения в п. 3.17. Применяемые в ИС ПДн классов К1 и К2 подсистемы управления доступом, учета и регистрации действий с ресурсами ИС обеспечивают надежную аутентификацию пользователей и носителей информации, что делает возможным автоматическое ведение, просмотр и печать этого журнала (см. выше п. 3.16).

4.9. Журнал учета печати документов, содержащих персональные данные.

См. пояснения в п. 4.8 выше.

4.10. Журнал учета случаев нарушения режима (инцидентов) безопасности информации в учреждении.

Порядок ведения и форма журнала должны быть определены в Инструкции по действиям в нештатных ситуациях (см. п. 3.18). По каждому случаю (инциденту) необходимо, кроме всего прочего, указать, как осуществлялось разбирательство, какие сделаны заключения (выводы), приняты меры и выполнены действия. Возможно также ведение учета инцидентов в общем журнале учета

мероприятий по защите информации (см. выше п. 4.2).

4.11. Журнал учета внешних машинных носителей информации.

Должен включать: **1)** ведомость всех носителей с указанием их назначения, в том числе носителей данных: **а)** используемых для обмена данными, **б)** с резервными копиями; **2)** собственно журнал учета выдачи (движения) носителей (кому и когда выдан, принят, где хранится, отметки о стирании информации) с подписью пользователя или ответственного лица; **3)** раздел учета проверок наличия носителей. В журнале должно быть предусмотрено также ведение записей об уничтожении и(или) стирании информации с машинного носителя и его снятии с учета (утилизации). Должно быть предусмотрено ведение записей о проверке журнала должностными лицами учреждения. См. также пп. 3.14; 3.15.

4.12. Журнал учета резервного копирования и восстановления данных на программно-аппаратном комплексе ИС учреждения (!!!).

В журнале ведется учет копирования данных, записанных как на серверах, так и на отдельных рабочих станциях (компьютерах). Желательно использовать штатные возможности автоматизированного ведения журнала, имеющиеся в применяемых средствах копирования/восстановления данных в составе подсистем управления доступом, регистрации и учета, и проверки целостности сертифицированных СЗИ с выгрузкой текущей копии журнала на отдельный внешний носитель. См. также п. 3.15.

4.13. Журнал учета антивирусных проверок на программно-аппаратном комплексе ИС учреждения.

См. п. 3.12. Целесообразно использовать штатные средства журнализации в применяемых антивирусных средствах, рекомендуемых

* Возможно ведение одного журнала учета печати и записи ПДн на внешние носители информации. В журнале должна быть предусмотрена возможность учета записи на внешний носитель и выдачи на руки пациенту под его роспись копий медицинских документов.



(сертифицированных) ФСТЭК (DrWeb, Kaspersky и др.).

4.14. Журнал учетных записей пользователей информационной системы учреждения.

Форма журнала и порядок его ведения должны быть определены в Инструкции по организации парольной защиты в ИС учреждения (см. п. 3.13). Во всех современных средствах (подсистемах) управления доступом к ресурсам ИС, ведение, просмотр и печать журнала автоматизированы.

4.15. Журнал учета мероприятий по техническому обслуживанию программно-технических средств информационной системы учреждения.

При необходимости учет мероприятий по техническому обслуживанию средств защиты информации в тех случаях, когда они выполняются организациями-лицензиатами ФСТЭК и(или) ФСБ, может осуществляться в отдельных (специальных) журналах или оформляться в виде актов о выполнении соответствующих работ (см. пп. 2.13, 5.6–5.9).

4.16. Журнал(ы) учета настроек средств(а) защиты информации.

Ведется, если это требуется инструкцией по эксплуатации применяемого средства защиты информации. Учет настроек всех СЗИ может также вестись в одном журнале или в журнале учета работ по техническому обслуживанию СЗИ и(или) СВТ (см. выше п. 4.15).

4.17. Журнал учета заявок пользователей ИС на техническое обслуживание компьютеров.

В журнале должны учитываться обращения пользователей ИС в службу технической поддержки, в том числе связанных с работой средств защиты информации, заражением вирусами и т.д. Учет заявок пользователей может осуществляться также в журнале учета мероприятий по техническому обслуживанию (см. выше п. 4.15).

4.18. Журнал учета криптографических средств.

Ведется в соответствии с [9, пп. 3.3; 3.4; 3.5, приложение № 2] при использовании в системе сертифицированных ФСБ средств криптографической защиты информации (см. п. 1.2.6).

4.19. Технический (аппаратный) журнал криптографического средства.

Ведется в соответствии с [9, п. 3.6, приложение № 3] при использовании в системе сертифицированных ФСБ средств криптографической защиты информации. См. также п. 3.19.

4.20. Ведомость нормативно-методических, распорядительных и учетных документов по обеспечению безопасности информации в учреждении.

Помимо всего прочего, эта ведомость необходима при проведении аттестации ИС на соответствие требованиям безопасности информации, а также при получении лицензии ФСТЭК на деятельность по технической защите информации [11, п. 5]. См. также п. 3.19.

4.21. Ведомость учета средств защиты информации, технической эксплуатационной документации системы защиты информации.

Необходимость учета средств технической защиты информации определена [2, п. 12(е), п. 20] (см. далее).

5. Техническая документация

В учреждении необходимо обеспечить учет и иметь полный перечень (ведомость) всех технических (эксплуатационных) документов системы защиты информации [2, п. 12(е), п. 20]. Техническая документация (ТД) должна содержать описание системы защиты информации в учреждении [2, п. 12(к)]. Разработка комплекта ТД осуществляется в процессе проектирования и реализации (технорабочего проектирования) системы защиты информации в учреждении в соответствии с заданными требованиями к системе защиты (техническим заданием, см. п. 2.5).

Техническая документация на систему защиты информации должна включать:



5.1. План-схему контролируемой зоны (см. п. 1.2.4);

5.2. План-схему инженерных коммуникаций, электроснабжения и заземления с привязкой к границам контролируемой зоны (для систем классов К1, К2);

5.3. План-схему размещения основных технических средств связи (ОТСС) и вспомогательных технических средств и систем (ВТСС) и их кабельных линий с привязкой к границам контролируемой зоны (для ИС ПДн классов К1, К2); входит в состав технического паспорта АС (см. выше п. 2.9);

5.4. План-схему размещения технических средств информационной системы учреждения с привязкой к границам контролируемой зоны;

5.5. Перечень и спецификации используемых: **а)** средств вычислительной техники, **б)** общесистемного и прикладного программного обеспечения (с указанием их размещения (установки) на каждом компьютере/сервере);

5.6. Спецификации средств защиты информации (СЗИ) с указанием серийных (заводских) номеров изделий, реквизитов лицензий и сертификатов соответствия, а также перечней (реквизитов) эксплуатационной (технической) документации а СЗИ;

5.7. Инструкции по использованию аппаратных и программных СЗИ (в инструкции администратору ОБИ и пользователям ИС могут включаться ссылки на эти инструкции, их отдельные разделы и пункты);

5.8. Иную техническую документацию СЗИ (ведомость ЭД, описания, инструкции по установке, настройке и обслуживанию и т.д.);

5.9. Учетные эксплуатационные документы СЗИ (журналы учета настроек СЗИ, учета мероприятий по техническому обслуживанию СЗИ и др.);

5.10. Лицензии и копии сертификатов на используемые СЗИ, акты об их установке и вводе в действие (см. пп. 2.7, 2.13).

Комплект ТД используется при проведении испытаний и оценке соответствия ИС ПДн

учреждения установленным требованиям безопасности информации.

Нормативные ссылки

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (в ред. законов от 25.11.2009 № 266-ФЗ и от 27.12.2009 № 363-ФЗ).

2. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (утверждено Постановлением Правительства РФ от 17.11.2007 № 781).

3. Порядок проведения классификации информационных систем персональных данных (утвержден Приказом ФСТЭК, ФСБ и Мининформсвязи России от 13.02.2008 № 55/86/20).

4. Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены ФСТЭК 15.02.2008/11.11.2009 снят гриф «ДСП»).

5. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных (утверждены ФСТЭК 15.02.2008/11.11.2009 снят гриф «ДСП»).

6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена ФСТЭК 15.02.2008).

7. Методика определения актуальных угроз безопасности при их обработке в информационных системах персональных данных (утверждена ФСТЭК 14.02.2008/16.11.2009 снят гриф «ДСП»).

8. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К, утверждены Гостехкомиссией РФ 30.08.2002).

9. Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназна-





ченных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены ФСБ 21.02.2008).

10. Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (утверждены ФСБ 21.02.2008).

11. Положение о лицензировании деятельности по технической защите конфиденциальной информации (утверждено Постановлением Правительства РФ от 15.08.2006 № 504).

12. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

13. ГОСТ Р ИСО/МЭК 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий.

14. ГОСТ 34.603-92 Виды испытаний автоматизированных систем.

15. Модель угроз типовой медицинской информационной системы типового лечебно-профилактического учреждения (Минздравсоцразвития России, ноябрь 2009; согласована с ФСТЭК, письмо от 27.11.2009 № 240/2/4009 за подписью заместителя директора ФСТЭК А. Гапонова)*.

16. Методические рекомендации по организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (Минздравсоцразвития России, утверждены 23.12.2009 директором Департамента информатизации Минздравсоцразвития России О.В. Симаковым,

согласованы 22.12.2009 начальником 2-го управления ФСТЭК России А.В. Куц)*.

17. Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений и организаций здравоохранения, социальной сферы, труда и занятости (Минздравсоцразвития России, утверждены 23.12.2009 директором Департамента информатизации Минздравсоцразвития России О.В. Симаковым, согласованы 22.12.2009 начальником 2-го управления ФСТЭК России А.В. Куц)*.

Тексты перечисленных выше нормативных правовых документов опубликованы на сайтах Роскомнадзора www.rsoc.ru и ФСТЭК www.fstec.ru. Образцы некоторых организационно-распорядительных документов можно найти на сайте Минздравсоцразвития России по указанному выше адресу (приложения к [16]), на сайтах www.54.rsoc.ru, www.admin.smolensk.ru и сайтах МИАЦ Владимирской, Омской и Челябинской областей — www.medctaf.narod.ru, www.omskminzdrav.ru, www.miac74.ru. Много полезных материалов по вопросам защиты персональных данных, в том числе в медицинских учреждениях, размещено на сайте www.ispdn.ru.

В заключение следует отметить, что задача разработки в учреждении внутренних нормативных и методических документов по защите информации должна быть приоритетной. Первоочередность ее выполнения обеспечит разработку и внедрение эффективных и экономически оправданных организационных и технических решений по защите информации.

Автор будет признателен всем, кто пришлет свои замечания и предложения по электронной почте по адресу: ap100lbov@mail.ru или stolbov@mcramn.ru.

* Эти документы 26.12.2009 были опубликованы на сайте Минздравсоцразвития России (www.minzdravsoc.ru/docs/mzsr/informatics/). Основные положения «Модели угроз ...» были доложены директором Департамента информатизации Минздравсоцразвития России О.В. Симаковым и заместителем начальника отдела департамента С.П. Рыловым на заседании Рабочей группы РАМН по вопросам создания и внедрения медицинских информационных технологий 3 декабря 2009 г.

**В.И. ПЕРХОВ,**

д.м.н., ведущий научный сотрудник ФГУ «Центральный научно-исследовательский институт организации и информатизации здравоохранения Минздравсоцразвития России», г. Москва, finramn@mail.ru

В.М. КУРАЕВА,

аспирант ФГУ «Центральный научно-исследовательский институт организации и информатизации здравоохранения Минздравсоцразвития России» г. Москва, kuraeva095@mail.ru

С.А. КИРЕЕВ,

заместитель директора ФГУ «Эндокринологический научный центр Минздравсоцразвития России», г. Москва, s1381967@mail.ru

Е.Е. БАЛУЕВ,

консультант заместителя председателя Правительства Пермского края, г. Пермь, e.baluev@mail.ru

О НЕОБХОДИМОСТИ ИСПОЛЬЗОВАНИЯ ТЕЛЕКОНСУЛЬТАЦИЙ ПРИ ОРГАНИЗАЦИИ ОКАЗАНИЯ ВЫСОКОТЕХНОЛОГИЧНОЙ МЕДИЦИНСКОЙ ПОМОЩИ

УДК 614.2

Перхов В.И., Кураева В.М., Киреев С.А., Балувев Е.Е. О необходимости использования телеконсультаций при организации оказания высокотехнологичной медицинской помощи (ФГУ «Центральный научно-исследовательский институт организации и информатизации здравоохранения Минздравсоцразвития России», ФГУ «Эндокринологический научный центр Минздравсоцразвития России», г. Москва; Правительство Пермского края, г. Пермь).

Аннотация: Обеспечение равной доступности для населения разных регионов страны высоких медицинских технологий является сложной задачей по ряду причин, включая низкую эффективность отбора больных. В статье представлены фактические данные, обуславливающие необходимость расширения использования медицинских телекоммуникационных технологий в сфере обеспечения населения высокотехнологичной медицинской помощью, обоснован вариант перечня головных по профилю высокотехнологичной медицинской помощи федеральных медицинских учреждений.

Ключевые слова: высокотехнологичная медицинская помощь, медицинские телекоммуникационные технологии

UDC 614.2

Perkhov V.I., Kuraeva V.M. (FGU «The Central scientific research institute of the organization and information of public health services of Minzdravsotsrazvitiya of Russia»), Kireev S.A. (FGU «The Endocrinology centre of science of Minzdravsotsrazvitiya of Russia»), Baluev E.E. (The government of the Perm edge) The necessity of the use of teleconsultations at the organization of rendering of hi-tech medical aid

Abstract: Providing with equal availability to the population of different regions of the country of hi-tech medical technologies is a difficult task because of several reasons, including low efficiency of the patients selection. The fact data causing the necessity of the expansion of the use of medical telecommunication technologies in sphere of providing the population with hi-tech medical aid is presented in the article, the variant of the list of the head federal medical institutions in each profile of hi-tech medical aid is proved.

Keywords: hi-tech medical aid, medical telecommunication technologies

12 ноября 2009 года в своем Послании Федеральному Собранию Российской Федерации Президент России Дмитрий Медведев в числе основных направлений деятельности в сфере экономики и народного хозяйства, наряду с внедрением новейших медицинских, энергетических



и информационных технологий, назвал также развитие телекоммуникационных систем.

Актуальность развития и широкого практического внедрения телекоммуникационных технологий в медицине (телемедицины) в Российской Федерации обусловлена не только наличием проблем, являющихся общими для многих современных систем здравоохранения. Существуют и другие факторы, характерные только для Российской Федерации. Это — большая территория и низкая плотность населения во многих регионах, существенные различия между регионами в степени урбанизации, диспропорции в уровнях финансирования региональных систем здравоохранения из государственных источников на душу населения, существенные территориальные различия в уровне доступности специализированной, в том числе высокотехнологичной, медицинской помощи для населения различных регионов.

Высокотехнологичная медицинская помощь (ВМП) — это наиболее эффективная, приводящая к существенному и стойкому улучшению состояния здоровья и качества жизни пациента, пользующаяся высоким спросом у населения, но наименее доступная медицинская помощь.

Этот вид медицинской помощи предоставляется при жизнеугрожающих и (или) инвалидизирующих заболеваниях, оказывается на основе научно- и ресурсоемких медицинских технологий, имеющих законченное клиническое значение и которые не могут быть широко тиражированы ввиду: **а)** высокой стоимости оборудования и используемых изделий медицинского назначения, имплантируемых в организм человека (протезы суставов, слуховые аппараты, ликворошунтирующие системы, электростимуляторы, материалы для внутрисосудистых вмешательств и прочие), и (или) лекарственных средств; **б)** необходимости выполнения специалистами особо высокой квалификации (обученных по специальным программам, имеющих ученые степени и т.д.) в специально оборудованных (операционные микроскопы, ультразвуковые дезинтеграторы,

навигационные системы, сложная наркозно-дыхательная аппаратура и прочие) условиях. ВМП — это в основном хирургическая помощь, отличающаяся необходимостью проведения углубленного и комплексного предоперационного обследования и подготовки, а послеоперационное ведение сопряжено с потреблением большого количества дорогостоящих медикаментов.

Объемы высокотехнологичной медицинской помощи, предоставляемые за счет государственных источников финансирования, подлежат жесткому регулированию, доступ населения к этому виду медицинской помощи ограничен, что обуславливает актуальность использования в этой сфере телекоммуникационных технологий.

Ежегодно в амбулаторно-поликлинических подразделениях федеральных медицинских учреждений регистрируется свыше 5,7 млн. посещений пациентами врачей. При этом в среднем только каждое 12-е посещение завершается госпитализацией больного, в том числе только каждое 28-е посещение завершается госпитализацией для оказания высокотехнологичной медицинской помощи. Обращение пациентов в федеральные медицинские учреждения (ФМУ) для консультации, в том числе с целью решения вопроса об оказании высокотехнологичной медицинской помощи, сопряжено с высокими транспортными расходами. Только для консультаций в ФМУ, расположенных на территории Москвы, пациенты других регионов суммарно преодолевают свыше 250 млн. километров в год, при этом затраты на однократный проезд туда и обратно составляют не менее 700 млн. рублей в год.

С учетом общих объемов экстерриториально оказанной высокотехнологичной медицинской помощи, а также того, что значительная часть пациентов, направленных в ФМУ для получения ВМП, фактически не госпитализируются, общие затраты на проезд пациентов могут оказаться еще более значительными.



Другой стратегически важной в условиях финансово-экономического кризиса стала задача организации взаимодействия между лечебно-профилактическими учреждениями и специализированными федеральными государственными учреждениями, оказывающими населению высокотехнологичную медицинскую помощь. Оперативное и полноценное решение этой проблемы может быть реализовано только при использовании современных информационно-телекоммуникационных технологий, что позволит расширить использование интеллектуального потенциала ведущих медицинских центров различного профиля для повышения качества оказания медицинской помощи жителям всех регионов России, включая отдаленные, в условиях задачи сокращения коечного фонда при одновременном ускорении лечебно-диагностического процесса.

Развитие телемедицины для обеспечения дистанционной консультативной помощи экономически целесообразно и наглядно продемонстрировало свою жизнеспособность в высокоразвитых странах. Телеконсультации особенно важны в отношении социально значимых и трудно дифференцируемых заболеваний, диагностика и лечение которых представляют значительные трудности и зачастую сопровождаются ошибками. В то же время накопленный опыт позволяет эффективно использовать телемедицинские технологии в системе оказания высокотехнологичной медицинской помощи, которая получает в настоящее время все более широкое распространение.

Процесс формирования общероссийской телемедицинской сети, обеспечивающей доступ к высокотехнологичной помощи в ФМУ больным из территориально отдаленных лечебно-профилактических учреждений, находится на начальном этапе своего развития. На федеральном уровне телемедицинские центры созданы в НИИ хирургии им. А.В. Вишневого, Научном центре сердечно-сосудистой хирургии им. А.Н. Бакулева,

Московском НИИ педиатрии и детской хирургии, Российском научном центре хирургии, Эндокринологическом научном центре и в некоторых других федеральных учреждениях. С федеральными медицинскими учреждениями взаимодействуют телемедицинские центры, расположенные в республиках Мордовия, Якутия, в Нижегородской, Смоленской, Ростовской, Тюменской, Оренбургской областях, в Ставропольском крае и на некоторых других территориях. Однако говорить о том, что телемедицина широко используется в высокотехнологичном здравоохранении, пока преждевременно, а успех внедрения телемедицинских технологий на федеральном уровне оказания высокотехнологичной медицинской помощи определяется не только удачными техническими, но и организационными решениями.

Одним из таких организационных решений является распределение субъектов Федерации по профильным направлениям телемедицинских консультаций в федеральных медицинских учреждениях, которое может быть реализовано с учетом данных о частоте госпитализаций в каждое федеральное медицинское учреждение пациентов из разных регионов, за исключением региона, являющегося местом расположения федеральной клиники. Эти данные характеризуют маршруты пациентов, начинающиеся в регионе (специализированном медицинском учреждении субъекта Федерации или территориальном органе управления здравоохранением) и заканчивающиеся в федеральной клинике.

Анализ основной части годовых объемов оказываемой в ФМУ ВМП показал, что из 140,4 тыс. оказанных в 2007 году за счет средств федерального бюджета видов ВМП только 47,8 тыс. видов (34,0%) предоставлено жителям территории (субъекта Федерации), являющейся местом расположения самого ФМУ. При этом 92,6 тыс. видов ВМП предоставлено ФМУ жителям других регионов (таблица 1).





Таблица 1

Объемы территориальной и экстерриториальной высокотехнологичной медицинской помощи, оказанной в федеральных медицинских учреждениях за счет средств федерального бюджета в 2007 году

Наименование профилей ВМП	Объемы ВМП (число оказанных видов)			Удельный вес объемов ВМП, оказанных жителям собственной территории, %
	Жителям других территорий	Жителям собственной территории	Общий итог	
Абдоминальная хирургия	631	594	1225	48,5
Акушерство и гинекология	1316	1217	2533	48,0
Гастроэнтерология	186	142	328	43,3
Гематология	684	1409	2093	67,3
Дерматовенерология	485	879	1364	64,4
Комбустиология	210	195	405	48,1
Неврология	360	383	743	51,5
Нейрохирургия	2133	913	3046	30,0
Онкология	12 652	15 860	28 512	55,6
Оториноларингология	173	99	272	36,4
Офтальмология	42 726	2773	45 499	6,1
Педиатрия	2181	1627	3808	42,7
Ревматология	1912	1136	3048	37,3
Сердечно-сосудистая хирургия	17 861	13 126	30 987	42,4
Торакальная хирургия	448	380	828	45,9
Травматология и ортопедия	5180	3710	8890	41,7
Трансплантация	281	103	384	26,8
Урология	1172	1137	2309	49,2
Челюстно-лицевая хирургия	735	378	1113	34,0
Эндокринология	1319	1735	3054	56,8
Общий итог	92 645	47 796	140 441	34,0

Наибольший объем высокотехнологичной медицинской помощи жителям других территорий (более 50%) предоставляется в ФМУ по профилям: офтальмология (93,9%), трансплантация (73,2%), нейрохирургия (70,0%), челюстно-лицевая хирургия (66,0%), оториноларингология (63,6%), ревматология (62,7%), травматология и ортопедия (58,3%), сердечно-сосудистая хирургия (57,6%), педиатрия (57,3%), гастроэнтерология (56,7%), торакальная хирургия (54,1%), акушерство и гинекология (52,0%), комбустиология (51,9%), абдоминальная хирургия (51,5%), урология (50,8%).

Жители только 21 субъекта Федерации имеют возможность получить ВМП по месту своего жительства. В наибольшей степени нуждаемость в высоких и высокозатратных медицинских технологиях, оказываемых в ФМУ, по месту своего жительства удовлетворяют жители города Москвы (98,1% объемов оказанной ВМП), Томской области (83,7%), Ростовской области (80,4%), г. Санкт-Петербурга (76,0%), Новосибирской области (74,0%), Свердловской области (65,2%), Кемеровской области (62,9%), Кировской области (59,1%), Саратовской области (54,7%), Нижегородской области (50,8%).



С учетом численности населения регионов наиболее интенсивно потребляют объемы ВМП, оказываемые в ФМУ, расположенные не на территории, которая является местом постоянного жительства больного, в регионах: Республика Адыгея (37,4 оказанных видов ВМП на 10 000 населения), Чукотский АО (36,8), Корякский АО (27,0), Республика Алтай (21,6), Калужская область (21,5), Ленинградская область (19,5), Магаданская область (18,4), Московская область (17,9), Хабаровский край (17,5), Камчатский край (16,6), Иркутская область (15,6), Тамбовская область (15,4), Республика Калмыкия (14,9), Волгоградская область (14,2), Северная Осетия-Алания (12,8), Таймырский АО (12,5), Эвенкийский АО (11,2), Новгородская область (10,8), Усть-Ордынский Бурятский АО (10,7), Еврейская автономная область (10,2), Чеченская Республика (10,0), Сахалинская область (9,9), Оренбургская область (9,5), Республика Хакасия (9,4), Тверская область (9,2), Республика Тыва (9,1), Республика Ингушетия (9,0), Псковская область (8,9), Липецкая область (8,5), Карачаево-Черкесская Республика (8,4), Владимирская область (8,4), Приморский край (8,1), Рязанская область (8,0), Читинская область (8,0), Республика Саха (7,7).

Только в федеральных клиниках, расположенных на территории Москвы, жителям других территорий (не москвичам) оказано 72,9 тыс. видов ВМП (51,8% всех объемов ВМП, оказанных в федеральных клиниках за счет средств федерального бюджета в 2007 году).

Наибольшие объемы ВМП оказаны московскими федеральными клиниками жителям следующих регионов: Московская область (11,6 тыс. видов ВМП), Волгоградская область (3,6 тыс. видов ВМП), Иркутская область (3,4 тыс. видов ВМП), г. Санкт-Петербург (3,1 тыс. видов ВМП), Хабаровский край (2,2 тыс. видов ВМП), Краснодарский край (2,2 тыс. видов ВМП), Калужская область (2,2 тыс. видов ВМП), Новосибирская область (1,9 тыс. видов ВМП), Оренбургская область

(1,9 тыс. видов ВМП), Тамбовская область (1,6 тыс. видов ВМП), Приморский край (1,3 тыс. видов ВМП), Тверская область (1,2 тыс. видов ВМП), Республика Татарстан (1,1 тыс. видов ВМП), Тульская область (1,1 тыс. видов ВМП), Владимирская область (1,1 тыс. видов ВМП).

Таким образом, для целей планирования направлений (профилей) телемедицинских консультаций представляется целесообразным наибольшие объемы консультаций планировать для следующих профилей ВМП: офтальмология, трансплантация, нейрохирургия, челюстно-лицевая хирургия, оториноларингология, ревматология, травматология и ортопедия, сердечно-сосудистая хирургия, педиатрия, гастроэнтерология, торакальная хирургия, акушерство и гинекология, комбустиология, абдоминальная хирургия, урология.

Население, как городов, так и сельских районов разных регионов неравномерно обеспечено высокотехнологичной больничной помощью, предоставляемой в пределах территории субъекта Федерации — места жительства больных. Поэтому для целей планирования объемов телемедицинских консультаций представляется целесообразным наибольшие объемы консультаций планировать для субъектов Федерации с наибольшей интенсивностью потребления экстерриториальных объемов высокотехнологичной медицинской помощи.

ФМУ также значительно отличаются друг от друга по удельному весу объемов ВМП в общем объеме оказываемой больничной помощи. Потому целесообразно квалифицировать ФМУ по этому признаку и выделить федеральные клиники, предоставляющие населению наибольшие объемы ВМП, а также являющиеся ведущими (головными) по каждому из профилей ВМП. Предлагается использовать четыре квалификационные категории.

Высшая категория — федеральные клиники, выполняющие большие объемы ВМП (более 2% от всего объема государственного задания на ВМП).





Первая категория — федеральные клиники, выполняющие существенные объемы ВМП (от 1 до 2% от всего объема государственного задания на ВМП).

Вторая категория — федеральные клиники, выполняющие от 0,5 до 1% от всего объема государственного задания на ВМП).

Третья категория — федеральные клиники, выполняющие незначительные объемы ВМП (менее 0,5% от всего объема государственного задания на ВМП).

В 2009 году 102 федеральных медицинских учреждения (Приказ Министерства здравоохранения и социального развития Российской Федерации от 29 декабря 2008 г. № 786н) вошли в состав исполнителей государственного задания на оказание ВМП за счет средств федерального бюджета. Вместе с тем только 17 федеральных клиник из 102 можно отнести к высшей квалификационной категории с учетом установленных этим учреждениям объемов государственного задания на ВМП: ФГУ «Межотраслевой научно-технический комплекс «Микрохирургия глаза» им. акад. С.Н. Федорова», ГУ «Российский онкологический научный центр им. Н.Н. Блохина РАМН», ФГУ «Новосибирский научно-исследовательский институт патологии кровообращения им. академика Е.Н. Мешалкина», ГУ «Научный центр сердечно-сосудистой хирургии им. А.Н. Бакулева РАМН», ФГУ «Ростовский научно-исследовательский онкологический институт», Санкт-Петербургский государственный медицинский университет им. академика И.П. Павлова, Российская детская клиническая больница, ФГУ «Московский научно-исследовательский онкологический институт им. П.А. Герцена», ФГУ науки и здравоохранения «Московский научно-исследовательский институт глазных болезней им. Гельмгольца», ФГУ «Национальный медико-хирургический центр им. Н.И. Пирогова», ФГУ «Научно-исследовательский институт онкологии им. проф. Н.Н. Петрова», ГУ «Гематологический научный центр РАМН»,

ГУ «Научный центр здоровья детей РАМН», ФГУ «Российский научный центр радиологии и хирургических технологий», ФГУ «Федеральный центр сердца, крови и эндокринологии им. В.А. Алмазова», ФГУ «Научный центр акушерства, гинекологии и перинатологии им. акад. В.И. Кулакова», Государственное образовательное учреждение высшего профессионального образования «Московская медицинская академия им. И.М. Сеченова».

К первой категории можно отнести 15 федеральных клиник: ФГУ здравоохранения «Всероссийский центр глазной и пластической хирургии», ФГУ «Лечебно-реабилитационный центр», ГУ «Научно-исследовательский институт нейрохирургии им. академика Н.Н. Бурденко РАМН», ФГУ «Российский научно-исследовательский институт травматологии и ортопедии им. Р.Р. Вредена», Саратовский государственный медицинский университет, ГУ «Российский научный центр хирургии РАМН», ФГУ «Эндокринологический научный центр», ГУ «Медицинский радиологический научный центр РАМН», ФГУ «Российский научный центр рентгенорадиологии», ФГУ «Московский научно-исследовательский институт педиатрии и детской хирургии», ФГУ «Новосибирский научно-исследовательский институт травматологии и ортопедии», ГУ «Научно-исследовательский институт кардиологии ТНЦ СО РАМН», Государственное образовательное учреждение высшего профессионального образования «Санкт-Петербургская государственная медицинская академия им. И.И. Мечникова», ФГУ «Российский кардиологический научно-производственный комплекс», Государственное образовательное учреждение высшего профессионального образования «Санкт-Петербургская государственная педиатрическая медицинская академия». Ко второй категории можно отнести 18 федеральных клиник, остальные — к третьей.

Таким образом, для целей планирования объемов телемедицинских консультаций представляется целесообразным наибольшее объе-



мы консультаций планировать для федеральных медицинских учреждений, отнесенных к высшей и первой квалификационным категориям.

Головными по профилям высокотехнологичной медицинской помощи могут являться федеральные медицинские учреждения, выполняющие наибольшие объемы государственного задания на оказание ВМП каждого конкретного профиля. Вариант перечня этих учреждений представлен в *таблице 2*.

Головные по профилям высокотехнологичной медицинской помощи федеральные медицинские учреждения могут осуществлять диспетчерские функции при управлении объемами профильной высокотехнологичной медицинской помощи. Суть диспетчеризации в данном контексте и необходимость ее практического внедрения сводятся к следующему.

За основу способа финансирования государственного задания на оказание ВМП целесообразно взять вариант сочетания предварительного авансового платежа с ретроспективной оплатой (смешанная оплата), но с акцентом на предварительный платеж, объем которого должен соответствовать годовым объемам государственного задания. Объем медицинской помощи, финансируемой в рамках ретроспективной оплаты, также должен быть также запланирован и обеспечен резервированными для его оплаты финансами.

Это означает, что основная часть расчетов плательщика с исполнителями государственного задания должна планироваться заранее, а окончательные взаиморасчеты должны производиться 3–4 раза в год в рамках относительно небольшого объема деятельности. Именно этот объем деятельности подлежит диспетчеризации. Это — оказание помощи при неотложных состояниях, а также в случаях установления медицинских показаний к вмешательствам у больных, проживающих в регионе с исчерпанными плановыми объемами помощи.

Как показал опыт Федерального агентства по высокотехнологичной медицинской помощи (Росмедтехнологии), объем этой деятельности

может составлять от 12% от суммарных объемов ВМП, предоставляемых населению Российской Федерации в ФМУ по государственному заданию. Так, например, в 2007 году Росмедтехнологиями реализованы меры по организации оказания высокотехнологичной медицинской помощи на безвозмездной для больных основе за счет резервных средств федерального бюджета дополнительно 6484 больным, включая более 1,8 тыс. случаев госпитализации больных для оказания высокотехнологичной медицинской помощи по неотложным показаниям. На финансовое обеспечение этих объемов высокотехнологичной медицинской помощи Росмедтехнологиями дополнительно доведены объемы бюджетных ассигнований федеральным медицинским учреждениям на сумму 2,6 млрд. рублей. Цель такого подхода состояла также в обеспечении реальной конкуренции однопрофильных федеральных медицинских учреждений, в финансовом поощрении лучших клиник, пользующихся наибольшим спросом у населения. При этом наименее востребованные медицинские учреждения могли рассчитывать только на минимальный объем финансирования. В будущем, по мере приближения к более радикальному законодательству в здравоохранении, могут быть сняты гарантии и этой оплаты.

Осуществляя и координируя деятельность по оказанию медицинских телекоммуникационных услуг, головные по профилям высокотехнологичной медицинской помощи федеральные медицинские учреждения будут способствовать восстановлению традиций преемственности в оказании медицинской помощи и выборе адекватных условий, технологий ведения и организации маршрутов пациентов, в том числе через сквозное регулирование объемов помощи. Это будет также способствовать переходу от «сепаратных» к интегрированным отношениям между медицинскими учреждениями различной ведомственной подчиненности.

В будущем госпитализация больного в федеральное медицинское учреждение должна стать невозможной без предварительного





Таблица 2

Вариант перечня головных по профилю высокотехнологичной медицинской помощи федеральных медицинских учреждений

<i>Профиль ВМП</i>	<i>Головное по профилю ВМП федеральное медицинское учреждение</i>
Абдоминальная хирургия	ГУ «Научный центр здоровья детей РАМН» (ВМП по профилю для детей 0–17 лет), ФГУ «Институт хирургии им. А.В. Вишневского» (ВМП по профилю для взрослых)
Гастроэнтерология	ФГУ «Государственный научный центр колопроктологии»
Гематология	ГУ «Гематологический научный центр РАМН»
Дерматовенерология	ФГУ «Центральный научно-исследовательский кожно-венерологический институт»
Комбустиология	ФГУ «Институт хирургии им. А.В. Вишневского»
Неврология	Российская детская клиническая больница (ВМП по профилю для детей 0–17 лет), Санкт-Петербургский государственный медицинский университет им. академика И.П. Павлова (ВМП по профилю для взрослых)
Нейрохирургия	ГУ «Научно-исследовательский институт нейрохирургии им. академика Н.Н. Бурденко РАМН»
Онкология	ГУ «Российский онкологический научный центр им. Н.Н. Блохина РАМН»
Оториноларингология	ФГУ «Санкт-Петербургский научно-исследовательский институт уха, горла, носа и речи»
Офтальмология	ФГУ «Межотраслевой научно-технический комплекс «Микрохирургия глаза» им. акад. С.Н. Федорова»
Педиатрия	ГУ «Научный центр здоровья детей РАМН»
Ревматология	Государственное образовательное учреждение высшего профессионального образования «Московская медицинская академия им. И.М. Сеченова»
Сердечно-сосудистая хирургия	ФГУ «Новосибирский научно-исследовательский институт патологии кровообращения им. академика Е.Н. Мешалкина» (ВМП по профилю для взрослых), ГУ «Научный центр сердечно-сосудистой хирургии им. А.Н. Бакулева РАМН» (ВМП по профилю для детей)
Торакальная хирургия	ФГУ «Новосибирский научно-исследовательский институт туберкулеза»
Травматология и ортопедия	ФГУ «Научно-исследовательский детский ортопедический институт им. Г.И. Турнера» (ВМП по профилю для детей), ФГУ «Российский научно-исследовательский институт травматологии и ортопедии им. Р.Р. Вредена» (ВМП по профилю для взрослых)
Трансплантация	ФГУ «Научно-исследовательский институт трансплантологии и искусственных органов»
Урология	ФГУ «Научно-исследовательский институт урологии»
Челюстно-лицевая хирургия	ФГУ «Центральный научно-исследовательский институт стоматологии и челюстно-лицевой хирургии»
Эндокринология	ФГУ «Эндокринологический научный центр»

телеконсультирования. Выполнение этого условия позволит создать единое и современное информационное пространство, объединяющее всех субъектов и объектов управления, прежде всего в сфере обеспечения населения высокотехнологичной медицинской помощью, в

котором все производители высоких и высокозатратных медицинских услуг будут четко прослеживаться по структуре и объемам предоставленной помощи. Это позволит также создать единый банк данных пациентов, проследить маршруты больных и результаты оказания



помощи, мониторировать ход выполнения договоров, контрактов и соглашений, которые должны стать основой обеспечения результативности при организации оказания и финансировании всех видов медицинской помощи, включая высокотехнологичную.

Важно также отметить, что в будущем все варианты предварительной и ретроспективной оплаты ВМП по государственному заданию предполагают использование одноканального финансирования и полных тарифов на высокотехнологичную медицинскую помощь. И в том, и в другом случае единицей расчетов будет являться стоимость законченного случая лечения в разрезе клинико-затратных групп (КЗГ) и других подобных клинико-экономических группировок больных. Разница лишь в том, что при предварительной оплате КЗГ используются для формирования основного годового бюджета медицинского учреждения, а при ретроспективной оплате — для покрытия сверхплановых издержек.

Использование одноканального финансирования и системы полных тарифов приведет к значительному увеличению объемов финансов, которые потребуются для оплаты деятельности федеральных клиник по оказанию помощи в экстренных случаях и при неотложных состояниях, а также в случаях установления медицинских показаний к вмешательствам у больных, проживающих в регионе с исчерпанными плановыми объемами помощи. При этом наличие глобальной телекоммуникационной системы диспетчеризации потоков пациентов может стать обязательным организационным условием.

Информация является ключом к управлению в любой системе здравоохранения, а телекоммуникационные технологии могут стать основой информационного обеспечения в отрасли. С учетом наличия специфических географических факторов, особенностей региональных систем расселения и территориальных систем здравоохранения, показателей состояния здоровья населения, содержа-

ния и направлений политики государства развитие телемедицины становится необходимым условием совершенствования организации оказания медицинской помощи населению Российской Федерации.

Общий и серьезный недостаток действующей в России системы здравоохранения — слабая функциональная и управленческая интеграция. Даже в рамках одного муниципального образования стационары и поликлиники действуют сами по себе без должной координации их работы, а также без адекватного управления структурой предоставляемой медицинской помощи и анализа эффективности использования ресурсов. Функциональная и управленческая дезинтеграция еще более выражена по вертикали и характеризуется отсутствием должного взаимодействия между медицинскими учреждениями государственно-муниципального сектора здравоохранения разных уровней подчиненности, то есть основные потери возникают «на стыках» системы.

Обостряет проблему действующая система финансирования медицинской помощи, основанная на оплате из разных источников одних и тех же видов медицинской помощи, предоставляемой населению в медицинских учреждениях разной подчиненности (муниципальных, региональных, федеральных).

Мероприятия, направленные на ликвидацию потерь, возникающих из-за плохой координации деятельности отдельных уровней и звеньев оказания медицинской помощи, целесообразно реализовывать с использованием телекоммуникационных технологий. Эти технологии являются инновационным, эффективным и перспективным инструментом всех видов взаимодействия в здравоохранении (клинического, информационного, организационного). Они ориентированы на обеспечение этапности оказания медицинской помощи; управленческой интеграции в здравоохранении; своевременности оказания и равнодоступности медицинской помощи; оперативности принятия управленческих решений.



Д.Н. РОМАНОВ,

заместитель директора по внедрению МЕДИАЛОГ, г. Москва, romanov@postmodern.ru

А.А. БОРЕЙКО,

директор по маркетингу «Пост Модерн Текнолоджи», г. Москва, boreyko@postmodern.ru

ВНЕДРЕНИЕ ПРОМЫШЛЕННОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ЗАМЕНОЙ МОРАЛЬНО УСТАРЕВШИХ ПРОГРАММНЫХ РЕШЕНИЙ

УДК 61:658.011.56

Романов Д., Борейко А. Внедрение промышленной медицинской информационной системы с заменой морально устаревших программных решений («Пост Модерн Текнолоджи»)

Аннотация: Статья очерчивает комплексный подход к реализации проекта внедрения медицинской информационной системы с заменой морально устаревших программных решений. Приводятся основные группы или уровни решаемых при этом задач.

Ключевые слова: медицинская информационная система, проект внедрения, проблемы внедрения, замена устаревших программных решений, замена информационной системы

UDC 61:658.011.56

Romanov D., Boreiko A. The deployment of a medical information system accompanied with the replacement of the outdated program solution (Post Modern Technology Ltd)

Abstract: The article outlines an integrated approach to the deployment of a medical information system accompanied with the replacement of the old program solution by a new one. The main groups or levels of project tasks are presented.

Keywords: medical information system, project of automation, problems of deployment, replacement of the old program solution, replacement of a medical information system

В настоящей статье рассмотрены проблемы внедрения в условиях замены старой медицинской информационной системы (МИС) на новую. Поскольку эпоха использования комплексных медицинских информационных систем в российских лечебных учреждениях началась относительно недавно, то замена старого программного решения на новое в настоящее время, как правило, означает переход с внутренней или кустарной разработки на промышленное решение.

Сказанное вовсе не обязательно означает, что в случае замены систем новое решение оказывается во всем лучше старого. Как будет показано ниже, новое программное обеспечение может даже в чем-то уступать прежним разработкам. Почему в таком слу-

чае ЛПУ все же решаются на замену? Каковы наиболее типичные причины и побудительные мотивы к смене медицинской информационной системы?

Основной причиной является развитие самого медицинского учреждения. Увеличение числа оказываемых пациентам услуг, географическое расширение деятельности и образование филиалов, приобретение новейшего диагностического и лабораторного оборудования с цифровым управлением — любой из этих процессов может поставить вопрос о степени соответствия старых программных продуктов новым условиям работы.

Дело в том, что внутренняя разработка равно, как и результаты труда временно привлеченных групп программистов, редко обла-



дает способностью к масштабированию при резком изменении круга задач или объемов обрабатываемой информации. Данный недостаток связан с двумя факторами. Во-первых, с ошибками проектирования: первые версии «домашних» продуктов всегда создаются как небольшие, иногда узкоспециальные решения. Со временем они обрастают новыми функциями, которые включаются в архитектуру первоначального решения не самым оптимальным образом. Во-вторых, из-за отсутствия многих компонентов, которые у промышленных систем имеются по определению: документация, инструменты тестирования, управление версиями и т.п.

Указанные недостатки самописных программ могут быть неактуальны для ЛПУ на протяжении длительного времени — пока организация работает по заведенному распорядку и не привносят сколько-нибудь значительных изменений в процессе оказания медицинских услуг. Но каждое серьезное изменение объемов и сложности работы может дестабилизировать работу информационной системы. Особенно в том случае, когда она не обладает необходимым набором артефактов для своего развития и, строго говоря, системой не является.

Внесенные на скорую руку и недокументированные модификации программного кода (а такой режим разработки для самодельных программ является скорее нормой, чем исключением) рано или поздно не только затрудняют развитие, но и вызывают проблемы поддержки и даже могут парализовать работу всей организации. Конечно, лучше всего, если данные проблемы руководство успеет распознать заблаговременно. Замена информационной системы в пожарном порядке — далеко не самый благоприятный сценарий внедрения нового решения, каким бы хорошим оно ни было.

Спокойная и вдумчивая подготовка к замене медицинской информационной системы, безусловно, является одним из главных условий

успешного перехода к новой технологии. Данная статья адресована тем руководителям и специалистам, которые уже имеют опыт эксплуатации медицинских информационных систем и задумались о смене инструмента автоматизации. Такие проекты внутри одной организации происходят нечасто. Вот почему так важно знать об их основных особенностях, включая как явные сложности, так и подводные камни.

Прежде всего необходимо принимать во внимание то обстоятельство, что при переходе на новую систему проектная работа не ограничивается заменой программного продукта. Информационная система задействована на разных уровнях управления и в различных аспектах деятельности организации. Имеет смысл обозначить как минимум четыре группы задач, успешная реализация каждой из которых является критически важной для успеха проекта в целом. Итак, вот эти группы:

- 1)** техническая модернизация, то есть собственно замена программного или программно-аппаратного комплекса;
- 2)** изменение навыков и знаний персонала;
- 3)** трансформация системной и бизнес-логики;
- 4)** модернизация проектной культуры лечебного учреждения.

Рассмотрим подробнее каждую группу задач и проблемы, связанные с их решением.

1. Техническая модернизация

Техническая модернизация — это то, что в подавляющем большинстве случаев занимает центральное место в планах руководства ЛПУ на ранних этапах проекта замены информационной системы. Со временем на передний план выходят и другие важные темы, но сама идея «поменять программу» ассоциируется именно с программным обеспечением — его качеством и возможностями.

Если идея замены ПО пустила корни и дала плоды, например, в виде тендера на поставку системы, то уже на конкурсном этапе вскрываются некоторые дополнительные аспекты. Так становится понятно, что,





наряду с прикладным программным обеспечением, может последовать замена и базового ПО, то есть операционных систем и систем управления базами данных. На горизонте может возникнуть задача модернизации оборудования, стоимость решения которой порой сопоставима со стоимостью программного обеспечения и услуг внедрения.

Задача технической модернизации включает в себя и более сложные вопросы. Например, проблему переноса данных из старой системы. Данная проблема содержит несколько аспектов, каждый из которых может существенно усложнить и замедлить выполнение проекта. Наибольшие трудности связаны с закрытостью устаревшего программного обеспечения: отсутствием полной и достоверной информации о его устройстве и принципах работы, начиная от программных алгоритмов и заканчивая структурой базы данных. Следует также упомянуть такую неприятность, как «замусоренность» данных — неблагоприятное состояние базы данных, сопровождаемое обилием дубликатов, случайных и ошибочных записей.

Обычно в каждой программе есть свои особенности хранения данных. Зачастую они не покрывают всех реальных ситуаций, которые возникают в процессе эксплуатации системы. При появлении таких исключений разработчики находят решения и принимают определенные соглашения о том, как реализовывать ту или иную ситуацию. Хорошо, если это делается в рамках единой системной логики. К сожалению, весьма часто решения принимаются, что называется, «по месту» и при этом не документируются. При смене информационной системы приходится решать данные вопросы заново.

В дополнение к упомянутым сложностям практически всегда отсутствуют четкие алгоритмы переноса данных, за исключением тех случаев, когда у поставщика нового решения уже есть опыт демонтажа именно такой устаревшей системы. Понятно, что такая ситуация

возможна только при замене пусть устаревших, но промышленных решений. И она непредставима в отношении самописных или кустарных разработок.

Несмотря на серьезность описанных проблем, их, тем не менее, трудно отнести к разряду основных. Их решение в значительной степени зависит от квалификации поставщика новой медицинской информационной системы и от наличия под рукой хотя бы одного специалиста, знакомого со старой. Так или иначе данные проблемы решаются. Только в очень редких случаях они могут полностью парализовать проект. Гораздо большую сложность составляют проблемы иного рода — связанные с людьми и привычными методами работы.

2. Изменение навыков и знаний персонала

Медицина относится к тем видам деятельности, где кадры действительно решают все или почти все. Именно поэтому отношение персонала к новой системе может быть более критичным для внедрения, нежели технические сложности замены ПО и переноса данных. Нежелание сотрудников менять привычный порядок работы может оказаться фатальным для любого проекта автоматизации.

Руководителю необходимо различать два фактора, которые вызывают негативное отношение врачей и медперсонала к новой информационной системе. С одной стороны, может иметь место обычный саботаж. Людям свойственно держаться за свои привычки и сопротивляться переменам. Если активное меньшинство специалистов, открытых к освоению новых технологий, не имеет достаточно влияния в организации в силу ее размеров или по другим причинам, а пассивное меньшинство пользователей преобладает и даже выдвигает своих лидеров, то требуется политическая воля и даже некоторая жесткость для успешного претворения в жизнь планов по внедрению новой системы.



С другой стороны, сопротивление переменам может происходить не только от злого умысла, но по объективным причинам. Полученные некогда навыки работы доводятся до автоматизма, что, вообще говоря, служит условием эффективной работы в заданных ситуациях и, более того, является неотъемлемой частью профессионализма медицинских работников. Поэтому, наряду с дисциплинарными требованиями, очень полезно озабочиться тем, чтобы расширение знаний и обновление профессиональных навыков происходили менее болезненно.

Иными словами, освоение новой системы должно сопровождаться не только негативными эмоциями. Оно должно быть связано с положительными стимулами. А процесс и формы обучения могут быть организованы так, чтобы минимизировать сложности в освоении нового инструмента. Здесь сыграют свою роль и свойства медицинской информационной системы: ее способность к адаптации под конкретную организацию и даже под требования отдельного специалиста, и квалификация поставщика решения и творческий подход руководства ЛПУ.

3. Трансформация системной и бизнес-логики

Задачей, непосредственно связанной с переподготовкой персонала, но обладающей еще более высоким уровнем сложности, является трансформация бизнес-логики организации. Сложность связана не только с множеством деталей, неизбежно всплывающих при автоматизации основных процессов, но также с тем обстоятельством, что в рамках информационной системы бизнес-логика неотделима от логики и архитектуры системного решения.

Как убедительно показывают отцы-основатели современных методов системного проектирования¹, терминология и вся модель, заложенная в систему, представляют собой сплав

из понятий предметной области (то есть в данном случае — технологического процесса ЛПУ), с одной стороны, и понятий системной архитектуры, с другой. Ведь информационная система — это не только программное обеспечение, но еще и совокупность терминов, алгоритмов и схем принятия решений. Старая программа может во многом определять словарь пользователей, в ней могут быть другие подходы к хранению данных и т.д.

Область системных понятий у разных разработчиков может различаться в значительно большей степени, чем бизнес-логика работы разных лечебных учреждений. Иными словами, у старой и новой систем, кроме родового названия «система», может быть мало, что общего.

Таким образом, в результате замены информационной системы изменения затрагивают не одну изолированную область, как это может казаться на первый взгляд (была одна программа, затем ее поменяли на другую), а три. Меняется бизнес-логика, логика построения системы, а также принципы их сочетания и взаимодействия, реализуемые в рамках комплексного решения.

Рассмотрим конкретные проявления данной коллизии. Один из наиболее характерных примеров — проблема воспроизведения в новой системе множества полезных наработок, которые были в старой. В процессе своей эволюции любая информационная система обрывает массой всевозможных дополнений, которые делаются для расширения начального или стандартного (у тиражных решений) функционала. Часто такие дополнения делаются сторонними разработчиками, но в результате воспринимаются как органичная часть системы.

В ходе внедрения нередко ситуация, когда отсутствие такого расширения в новом продукте вызывает негативную реакцию, поскольку отсутствующая функциональность уже воспринимается как стандарт, а непростая исто-

¹ См., например, Booch, Grady. Object Solutions. Managing the Object-Oriented Project. NY, 2000.





рия ее появления в старой программе давно предана забвению. При этом может быть даже поставлен вопрос о необходимости отказа от новой системы.

Решением данной проблемы может служить максимально полное предпроектное обследование со спецификацией всех функциональных требований. В ходе такого обследования можно будет, в частности, оценить, насколько те или иные функции необходимы и, если они действительно нужны, выяснить возможность доработки новой системы с учетом этих требований. Необходимо отметить, что разные промышленные решения обладают разным уровнем адаптивности. И лучше всего выяснить пределы «эластичности» нового решения на этапе выбора продукта, в крайнем случае — на этапе обследования.

Отсутствие какой-то функции в новой системе в привычном виде не всегда является однозначным минусом. Может оказаться, что те же задачи могут быть настроены в новом инструменте более оптимальным образом. Случается, что у заказчика МИС возникает искушение настроить новую программу до запятой, как старую. Особенно если высокий уровень адаптивности новой системы позволяет надеяться на возможность такой настройки. Дабы не ломать сложившихся стереотипов от новой системы, пытаются требовать точного повторения старой, что часто приводит к нетривиальным ситуациям, которые могут завести проект в тупик. К таким требованиям стоит подойти критически.

Не так уж редки ситуации, когда функциональные требования основаны на нечеткой формализации, и стоящие за ними бизнес-процессы не были должным образом описаны и подвергнуты анализу. Предпроектное обследование — именно то время, когда у организации есть редкая возможность пересмотреть свою практику работы и провести корректировку бизнес-процессов при сравнительно низких издержках, а главное — с возможностью воплотить в новой системе наиболее разумные и полезные улучшения.

4. Развитие проектной культуры руководства ЛПУ

Описывая проблемы внедрения с заменой старой системы на новую, мы подошли к тому уровню задач, которые представляют наибольшую сложность для руководителя медицинского учреждения. До сих пор речь шла о тех задачах, при решении которых управляющее воздействие направлено на внешние (для руководителя) объекты: технические средства, персонал, бизнес-модель и архитектура информационной системы. Теперь же разговор пойдет о развитии проектной культуры, то есть о том, что в значительной степени относится к сознанию и управленческой культуре самих руководителей. А себя, как известно, изменить бывает сложнее, чем окружающий мир.

Опишем вкратце те симптомы, которые заставляют обратить особое внимание на данную группу задач. Среди основных проблем следует упомянуть проблему целеполагания. Довольно часто у руководства медицинского учреждения отсутствует понимание того, какой эффект должен получиться в результате внедрения новой информационной системы. Даже имея опыт внедрения и эксплуатации информационных систем, руководители ЛПУ не всегда могут четко сформулировать, какого результата от замены систем они ожидают. Как следствие — отсутствие как четких планов, так и ясных методов оценки результата внедрения.

Кроме того, на этапе внедрения нередко вскрываются пробелы в понимании руководителем отдельных аспектов деятельности собственной организации. Оказывается, что разные подразделения и сотрудники могут по-разному понимать логику бизнес-процессов как на своем, так и на смежном участке работы. Такие нестыковки рано или поздно приводят к конфликтным ситуациям. В условиях лоскутной автоматизации или низкой дисциплины использования информационной системы данные конфликты часто разрешаются неформально. И такой метод решения может устраивать все стороны конфликта.



При смене систем многие такие ситуации приходится разбирать заново и искать более формализованное решение. Проблему составляет даже не столько само наличие организационных конфликтов и сопутствующих им неформальных решений, сколько готовность руководителя к таким изменениям, его способность «вынырнуть» из административной рутины и совместно с ключевыми специалистами и поставщиком решения найти наиболее оптимальное решение.

Крайне редко можно встретить лечебное учреждение, у руководителей которого имелись бы готовые наработки по организации внедрения, например, в форме регламентов или паспорта проекта. В данных условиях не приходится удивляться тому, что внедрению предшествует неправильная оценка трудозатрат, необходимых для выполнения всех необходимых настроек новой системы. Сплошь и рядом можно наблюдать отсутствие понимания многих из вышеперечисленных проблем, связанных с внедрением: технических сложностей, важности человеческого фактора и т.д.

Чем вызваны эти трудности? Было бы несправедливо обвинять в них руководителей ЛПУ. Наряду с человеческими недостатками, здесь, безусловно, присутствует системная проблема. Теория и практика проектного управления¹ различают проектную и процессную деятельность. Причем эти различия можно отнести не только к характеру деятельности, но и к навыкам руководителей, возглавляющих разные типы организаций. Проекты ограничены во времени, они имеют цель и жизненный цикл. Процессы же не имеют таких четких целей, хотя и обладают порой значительным уровнем технологической сложности.

Медицинские организации в массе своей относятся к процессному типу деятельности, что накладывает определенный отпечаток на их управленческую культуру. Врачи и руководители клиник довольно часто характеризуют значительную часть своей работы как рутину. Когда в медицинскую организацию приходит постав-

щик информационной системы, то происходит встреча двух типов управленческих культур — проектной и процессной, встреча, которая не всегда проходит с полным взаимопониманием.

Как любая организация, где преобладает процессная, а не проектная деятельность, ЛПУ может испытывать трудности всякий раз, когда возникает задача выполнить сложный проект, — будь то ремонт здания или внедрение МИС. При взаимодействии с малыми группами разработчиков (сторонних и тем более своих) руководство ЛПУ может позволить себе «не опускаться» до «технических деталей». Кустарные разработки в свою очередь имеют свойство подстраиваться под любые требования заказчика лишь бы сохранить клиента, что ведет к разрушению такого важного компонента проектного управления, как управление требованиями. Соответственно при переходе на промышленное решение данную задачу приходится ставить и решать практически с нуля. Это лишь один из примеров того, почему лечебным учреждениям для успешного внедрения МИС требуется своего рода прививка проектной культуры.

Именно поэтому мы считаем важным обратить внимание профессионального сообщества на необходимость развития проектной культуры внутри лечебных учреждений. Добиться этого можно главным образом за счет развития новых направлений менеджмента и соответствующих им новых специальностей, таких, которые сочетали бы в себе знание процессов управления ЛПУ, общих стандартов проектного управления и практики реализации ИТ-проектов в медицине. Не так важно, как именно будут называться подобные специалисты: СЮ, проджект-менеджеры в здравоохранении или каким-то другим термином. Важно понимать необходимость подобного сплава знаний и навыков и признавать за ним решающее значение, когда речь идет о таком непросто-м виде проектной деятельности, как замена медицинской информационной системы.

¹ PMBOK® Guide 2004



Э.Ш. САЛИХОВА,

к.м.н., доцент, руководитель медицинского управления ООО «Медконсалтинг», г. Москва, ESalihova@med-cons.ru

М.А. КРАСИКОВ,

руководитель управления развития ООО «Медконсалтинг», MKrasikov@med-cons.ru

Т.Б. ШУСТИКОВА,

ведущий бизнес-аналитик отдела проектов ООО «Медконсалтинг», TShustikova@med-cons.ru

С.А. ШЕВЧЕНКО,

ведущий эксперт по медицине отдела проектов ООО «Медконсалтинг», SShevchenko@med-cons.ru

ИНФОРМАТИЗАЦИЯ ЗДРАВООХРАНЕНИЯ РЕГИОНАЛЬНОГО УРОВНЯ НА ОСНОВЕ ТИПОВЫХ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

УДК 61:658.011.56

Салихова Э.Ш., Красиков М.А., Шустикова Т.Б., Шевченко С.А. *Информатизация здравоохранения регионального уровня на основе типовых медицинских информационных систем (ООО «Медконсалтинг», г. Москва)*

Аннотация: В статье рассмотрена концепция реализации региональных проектов информатизации учреждений здравоохранения на основе применения типового программного обеспечения, построенного на базе единой программной платформы. Приведены описания требований и функциональных возможностей основных блоков предложенной концепции, а также дан обзор наиболее важных положительных эффектов от их внедрения.

Ключевые слова: типовая медицинская информационная система, Медконсалтинг, региональные проекты информатизации здравоохранения.

UDC 61:658.011.56

Salikhova E.Sh., Krasikov M.A., Shustikova T.B., Shevchenko S.A. *Computerization of health care at the regional level based on the model of medical information systems (ООО «Medkonsalting», Moscow)*

Abstract: The article discusses the concept of regional projects of informatization of public health institutions through the application of software model, built on a single software platform. The paper presents the requirements and functionality of the basic blocks of the proposed concept, as well as an overview of the most important positive effects of their introduction.

Keywords: model medical information system, Medkonsalting, regional health information projects.

На сегодняшний день в отечественном здравоохранении информационные технологии начинают играть все более важную роль. Этому способствует множество предпосылок, усиливающих в интегральном результате потребность в медицинских информационных системах (МИС): это и задачи формирования статистической отчетности и взаиморасчетов по ОМС/ДМС, это и учет платных услуг, это и задачи интеграции с различными участниками формируемого медицинского информационного пространства, включая региональные МИАЦ, территориальные

ФОМС, федеральные информационные системы и многое другое. При этом, на наш взгляд, в последнее время растет не просто спрос на медицинскую информационную систему, а потребность именно в типовых решениях, способных не только решить поставленные перед МИС задачи, но и стать полнофункциональным и гибким компонентом интеграционного плана, способным обмениваться информацией с другими информационными системами.

Очевидно, что в настоящее время система здравоохранения любого региона России представляет из себя сложную и многоуровневую



среду, эффективное управление которой сложно представить без применения информационных систем на основе собранной в электронном виде первичной медицинской информации. Подтверждением тому служат и обсуждаемые в последние 2 года профессиональным сообществом планы Департамента информатизации Минздравсоцразвития РФ по созданию единой федеральной информационной системы учета оказанной медицинской помощи, которая также строится на принципе сбора первичной медицинской информации о каждой услуге или посещении пациентов ЛПУ на базе региональных центров обработки данных и последующей обработки этой информации с целью адекватного представления о работе ЛПУ региона, повышении эффективности расхода ресурсов и управлении всей системой здравоохранения в целом. При этом на различных уровнях государственной власти высказываются четкие призывы к массовому внедрению электронных историй болезни, автоматизации документооборота в ЛПУ. Также общеизвестно, что в России разработано большое количество различных программных продуктов, включая наиболее популярный класс медицинских информационных систем. По различным оценкам, лишь незначительная часть из них может быть применена для комплексных проектов автоматизации ЛПУ и использована как часть общей информационной системы здравоохранения регионального уровня. Большинство программного обеспечения (ПО) в сфере здравоохранения может быть применено только для специализированных задач внутри ведомства или медицинской организации, что делает их фактически непригодными для последующих неизбежных процессов интеграции и совместного использования накопленных банков медицинских данных.

Такое состояние рынка МИС не удовлетворяет руководителей здравоохранения, глав регионов и муниципальных образований. По нашим данным, в регионе с населением 3,0–3,5 млн. чел. источником данных для формирования достоверного представления об эффективности

работы системы здравоохранения, которое должно быть основано на нескольких десятках показателей (смертность, заболеваемость, временная нетрудоспособность и т.д.), могут выступать не менее 150 учреждений, находящиеся в подчинении 10 ведомств. Трудно представить себе реально работающую единую региональную систему подобного уровня и сложности, основанную на применении разрозненных программных продуктов, не способных обмениваться результатами своей работы в режиме реального времени. *Именно сложность реализации проектов информатизации на региональном уровне является главной причиной разработки компанией ООО «Медконсалтинг» концепции Единой медицинской информационной системы (ЕМИС).*

Основное назначение ЕМИС — оптимизация управления системой здравоохранения региона в динамично меняющихся условиях экономики, повышение качества оказания медицинской помощи пациентам региона и повышение эффективности распределения ресурсов. Осуществление автоматизированного сбора данных и их последующая статистическая обработка возможны только при организации единого информационного пространства на территории: создания единообразной структуры данных в подразделениях субъекта РФ, использование в них единой нормативно-справочной информации, обеспечение надежной автоматизированной передачи данных между информационными базами подразделений.

Основные принципы функционирования ЕМИС (рис. 1):

1. Автоматизированный сбор первичных медицинских данных осуществляется подсистемой сбора информации, которая позволяет оперативно собирать данные учреждений здравоохранения через защищенную сеть в региональное централизованное хранилище.

2. Обеспечение защищенной передачи данных осуществляет подсистема информационного обмена МИС, обеспечивающая гарантированную доставку данных без потерь и искажений.





3. Управление нормативно-справочной информацией (НСИ) выполняется подсистемой единой нормативно-справочной информации, которая обеспечивает централизованное управление и ведение справочников и классификаторов, утвержденных как на федеральном, так и на региональном уровнях.

Описание технической реализации

С технической точки зрения, вся ЕМИС представлена в виде Типовой медицинской информационной системы (ТМИС), созданной для каждого конкретного участника ЕМИС. Ключевая особенность типовых решений в том, что они способны решить задачи различных медицинских организаций (поликлиники, стационара, станции скорой медицинской помощи и т.д.), но при этом обеспечить возможность использования единой НСИ и автоматизированный обмен и консолидацию всей информации на региональном уровне. Типовые МИС как компоненты ЕМИС реализованы в виде линейки самостоятельных программных продук-

тов «Медицинская организация» компании ООО «Медконсалтинг», разработанные на платформе «1С: Предприятие 8». Выбор платформы был продиктован наличием в большинстве ЛПУ программного обеспечения для бухгалтерии на базе 1С. Единая программная платформа бухгалтерского учета и созданная на ее основе типовая МИС сделали возможной простую интеграцию всех модулей единой информационной системы.

Основными преимуществами данного подхода являются:

- широкие возможности и простота настройки системы;
- открытость системы, включая быстрое внедрение, глубоко проработанные возможности настройки вплоть до изменения исходного кода МИС;
- возможность поддержки компаниями-партнерами на всей территории РФ;
- удобство сопряжения с финансово-экономическими прикладными программами;
- невысокая стоимость решения;
- масштабируемость;

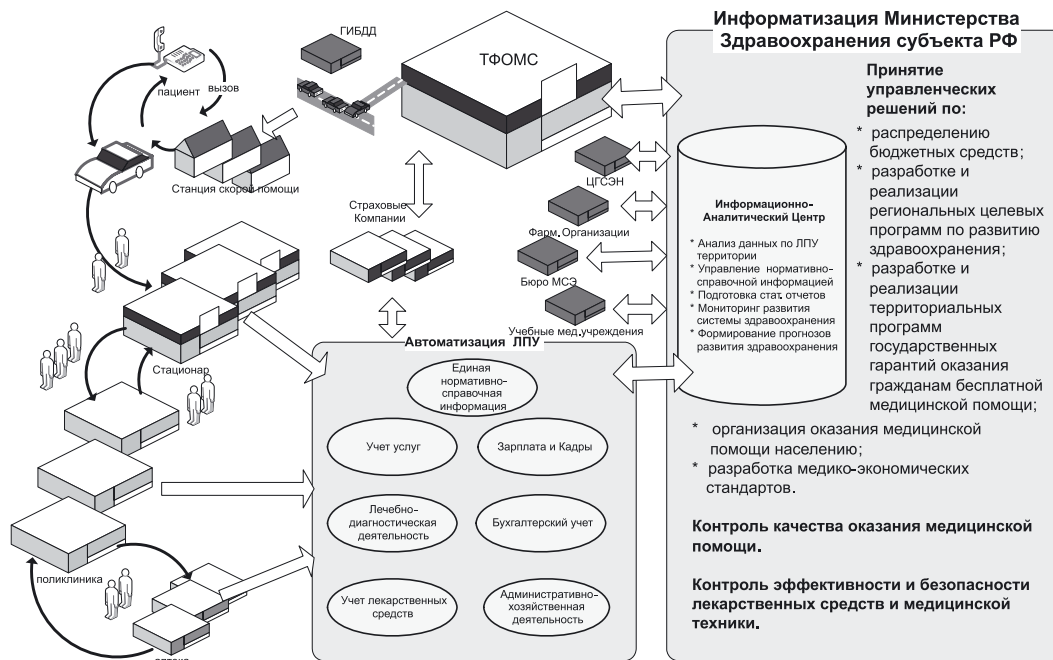


Рис. 1. Схема функционирования Единой медицинской информационной системы



- возможность интеграции с медицинским оборудованием, аптечной системой, бухгалтерской системой, лабораторной информационной системой (ЛИС) и др.

Очень важным преимуществом предложенной концепции и разработанных решений является простота интерфейсов рабочих столов. В условиях невысокого уровня компьютерной подготовки большинства медицинских сотрудников это залог лучшего восприятия и быстрой обучаемости работе с системой, сокращения времени внедрения и, как следствие, снижения его стоимости. Также важной особенностью является то, что линейка продуктов представлена типовыми решениями для стационаров, поликлиник и консультативно-диагностических центров.

Типовая МИС уровня ЛПУ — это важнейший, базовый элемент всей региональной медицинской информационной системы. Разработанная типовая МИС уровня ЛПУ представляет собой решение с широкими возможностями адаптации под действующие в ЛПУ процессы. Так, МИС может использоваться в 2-х режимах:

- Комплексный проект, подразумевающий подключение к МИС всех медицинских сотрудников, участвующих в лечебно-диагностическом процессе, в режиме реального времени. Данный подход имеет максимальную эффективность, но требует и максимальных затрат, особенно на создание инфраструктуры и оснащение ЛПУ большим числом компьютерной техники.

- Ввод данных операторами. При этом варианте использования медицинский персонал полностью исключается из процесса ввода данных в конфигурацию — в таком случае данные в МИС будут вводиться операторами с неким утвержденным на этапе внедрения отставанием от реального времени оказания медицинской услуги пациенту. Данный подход позволяет осуществить ввод только некоторой, наиболее важной части медицинской информации (например, талонов амбулаторных пациентов), но зато он не требует от ЛПУ дорогостоящих затрат на оснащение всех рабочих мест ПК, а значит, может быть введен в эксплуатацию в кратчайшие сроки.

Функционал типовой МИС уровня ЛПУ включает в себя ведение электронных историй болезни пациентов, регистрацию оказываемых им услуг, ведение взаиморасчетов со страховыми компаниями и с пациентами (в случае оказания платной медицинской помощи), регистрацию расходов ЛПУ на лечение пациента, а также на поддержание работоспособности учреждения, учет оборота лекарственных средств и других аптечных товаров ЛПУ. В системе реализована возможность использовать в работе как различные медицинские классификаторы, так и различные стандарты лечения, включая внутренние стандарты ЛПУ. Также реализована возможность планирования вакцинации населения, проведения медицинских осмотров, планирования и проведения диспансерного наблюдения, автоматического формирования эпикризов различных видов на основании введенных в систему данных. Учет лечебно-диагностической деятельности медицинской организации ведется по различным схемам в соответствии с профилем подразделения.

МИС уровня Информационно-аналитического центра — это центральный узел всей системы. В нее из ЛПУ передаются расходы по статьям бюджета, штатное расписание и данные об использовании рабочего времени персонала, данные по коечному фонду стационаров и прочая необходимая для последующего статистического анализа информация. База данных Аналитического центра собирает и хранит в себе всю единую нормативно-справочную информацию, используемую во всех ЛПУ территории. Функционал ЕМИС в Информационно-аналитическом центре включает в себя механизмы управления единой нормативно-справочной информацией, задания и хранение параметров целевых программ, механизмы поэтапного сравнения ключевых показателей целевой программы с их целевыми значениями, унифицированные формы отчетности для предоставления вышестоящим организациям, а также различные гибко настраиваемые отчеты для внутренней аналитики лечебно-диагностической





и административно-хозяйственной деятельности в области здравоохранения субъекта РФ.

Информационные системы бухгалтерского и кадрового учета обеспечивают расширенные возможности для автоматизации различных учреждений системы здравоохранения, включая государственные и частные ЛПУ, территориальные ФОМС, МИАЦ и другие организации. Данные продукты также созданы на базе единой платформы «1С: Предприятие 8». Для ЛПУ, финансируемых за счет бюджетных средств, используется «1С: Бухгалтерия бюджетного учреждения 8», которое позволяет вести бухгалтерский учет согласно инструкции, утвержденной Приказом Министерства финансов от 31 октября 2000 г. № 94н, и представляет собой упорядоченную систему сбора, регистрации и обобщения информации в денежном выражении о состоянии финансовых и нефинансовых активов и обязательств организации.

В целях автоматизации кадрового учета в коммерческих ЛПУ используется специальное решение «1С: Зарплата и Управление персоналом 8». Для ЛПУ, финансируемых за счет бюджетных средств, используется «1С: Зарплата и кадры бюджетного учреждения 8», которое, в отличие от стандартного функционала ИС кадрового учета, позволяет учитывать при расчете заработной платы медицинских работников квалификационные группы и повышающие коэффициенты, вести учет нормочасов, а также предоставляет возможность учитывать рабочее время сотрудника по двум и более ставкам. Все документы в данной ИС формируются с учетом распределения заработной платы по источникам финансирования.

Эффективность предложенной концепции и преимущества внедрения

Создание ЕМИС на уровне субъекта РФ позволит оптимизировать обмен информации с учреждениями других ведомств: ЦГСЭН, аптечными организациями, учебными медицинскими учреждениями, отделами ЗАГС,

бюро медико-социальной судебно-медицинской экспертизы.

Из ИС ЦГСЭН в Информационно-аналитический центр ЕМИС может передаваться информация о санитарном состоянии территории, инфекционных больных и выявленной профпатологии, данные по заболеваемости населения территории субъекта РФ. Полученные в ЕМИС данные могут передаваться в ИС аптечной организации и использоваться при планировании структуры товарного ассортимента аптек, в том числе по обеспечению необходимыми лекарственными средствами. Информационный обмен с Бюро МСЭ позволит учитывать данные об уровне инвалидизации населения и реабилитации инвалидов в статистической обработке данных, поступающих из ЛПУ.

Статистические данные по заболеваемости населения, по укомплектованности штатных расписаний ЛПУ могут учитываться учебными заведениями медицинского профиля при планировании кадровой оснащенности ЛПУ территории.

Руководители ЛПУ, работающие в системах ОМС и ДМС, могут в любой момент времени получать отчетность об оказанных услугах в следующих разрезах:

- по контрагентам;
- по договорам;
- по подразделениям медицинской организации;
- по отделениям каждого подразделения;
- по пациентам;
- по диагнозам;
- по врачам.

В результате использования типовой МИС повышается качество оказываемых медицинских услуг, сокращается число врачебных и управленческих ошибок;

- ликвидируются проблемы неразборчивого почерка;
- исключается возможность потери данных вследствие утери бумажного носителя;
- используется вся имеющаяся информация о пациенте посредством службы одного окна;



- создается база данных за весь период наблюдения;
- в помощь врачу осуществляется компьютерный контроль: исключение «потерь» диагнозов, контроль полноты использования «настораживающей» информации, контроль своевременности проведения лечебно-профилактических мероприятий;
- оптимизируются планы обследования пациентов и загрузка персонала.

Дополнительным преимуществом в работе новой МИС для главных врачей медицинских центров является возможность расчета реальной себестоимости лечения на каждого конкретного пациента. Своевременность и достоверность всей представляемой информации позволяют оптимизировать расходы ЛПУ, вести грамотную кадровую политику и принимать управленческие решения, направ-

ленные на успешное развитие Вашего бизнеса в динамично меняющихся условиях конкуренции на рынке медицинских услуг.

В результате реализация концепции ЕМИС на уровне субъекта РФ позволит:

- повысить качество оказываемых услуг за счет достоверности, полноты, оперативности формирования финансовой и статистической отчетности;
- оптимизировать распределение и использование бюджетных средств;
- эффективно реализовывать как федеральные, так и территориальные программы, направленные на уменьшение заболеваемости в регионе;
- отслеживать в динамике значения показателей деятельности системы здравоохранения субъекта РФ и эффективно управлять ее развитием.

ЛИТЕРАТУРА



1. Интервью СNews с Олегом Симаковым, директором Департамента информатизации Минздравсоцразвития РФ//<http://www.cnews.ru/reviews/free/publichealth/int/simakov/>.
2. Описание программных продуктов компании «Медконсалтинг»//<http://www.med-cons.ru>.
3. Описание программных продуктов Фирмы 1С//<http://www.v8.1c.ru>.
4. Указ Президента Российской Федерации от 28.04.2008 № 607 «Об оценке эффективности деятельности органов местного самоуправления городских округов и муниципальных районов»//Собрание законодательства РФ. — 05.05.2008. — № 18. — Ст. 2003.
5. Письмо Минздравсоцразвития Российской Федерации от 29.06.2009 № 20-0\10\2-5067 «О направлении рекомендаций по способам оплаты медицинской помощи, ориентированным на результаты деятельности медицинских организаций, участвующих в реализации Территориальной программы государственных гарантий оказания гражданам Российской Федерации бесплатной медицинской помощи»//Здравоохранение. — 2009. — № 10.
6. О мерах по созданию государственной информационной системы персонифицированного учета оказания медицинской помощи гражданам Российской Федерации//Врач и информационные технологии. — 2008. — № 6. — С. 4-13.
7. Как информатизированы российские клиники?//<http://www.cnews.ru/reviews/free/publichealth/article/informatisation.shtml>



ООО «МЕДИЦИНСКАЯ КОНСАЛТИНГОВАЯ КОМПАНИЯ»

117218, Москва, ул. Б. Черемушкинская, д. 36, к. 2
Тел.: + 7 (495) 755-80-85; факс: (495) 988-31-61
e-mail: fran@med-cons.ru, www.med-cons.ru



Н.В. КОБЛЯКОВ,

президент компании Senior Group, г. Москва, info@seniorhotelgroup.com

РАЗРАБОТКА И ВНЕДРЕНИЕ ДИСТАНЦИОННОЙ ТЕХНОЛОГИИ СОЦИАЛЬНОГО И МЕДИЦИНСКОГО ОБСЛУЖИВАНИЯ ПОЖИЛЫХ ЛЮДЕЙ КАК ПРИМЕР ЧАСТНО- ГОСУДАРСТВЕННОГО ПАРТНЕРСТВА В СИСТЕМЕ ЗДРАВООХРАНЕНИЯ

УДК 61:658.011.56

Кобляков Н.В. Разработка и внедрение дистанционной технологии социального и медицинского обслуживания пожилых людей как пример частно-государственного партнерства в системе здравоохранения (Компания Senior Group, г. Москва)

Аннотация: Предложена мобильная дистанционная технология социального и медицинского обслуживания пожилых людей с использованием элементов европейской системы Senior Care

Ключевые слова: пожилые люди, медицинское обслуживание, дистанционные технологии

UDC 61:658.011.56

Kobliakov N.V. Development and implementation of remote technology for social and medical services for older people as an example of public-private partnership in the health system (Company Senior Group, Moscow)

Abstract: Was proposed a remote mobile technology for social and medical services for older people using elements of the European system of Senior Care

Keywords: elderly, health care, remote technology

Новые информационные технологии для домашних систем ухода за пожилыми людьми становятся все более востребованными по мере ускорения темпов старения населения. Согласно оценкам ООН (*Development Human Report, 2006. P. 298–300*), проблема старения населения характерна практически для всех стран мира, в том числе и для России. В большей степени увеличивается число россиян старше 80 лет, то есть именно той возрастной категории, которая в наибольшей степени нуждается в посторонней помощи и серьезных социально-медицинских услугах. Уже сегодня тысячи пожилых россиян стоят в очередях на обслуживание патронажных сестер. На основе прогнозного моделирования, выполненного компанией Senior Group, можно ожидать, что через три года в дома престарелых РФ выстроится очередь примерно в 200 тысяч человек.



Именно поэтому российский рынок информационных систем демонстрирует высокую потенциальную восприимчивость к дистанционным технологиям комплексного обслуживания и контроля состояния пожилых людей. Одну из таких технологий несколько месяцев назад предложила компания Senior Group.

В основе технологии лежит европейский принцип Senior Care — уход за пожилыми людьми. Стандарт Senior Care подразумевает отношение к пожилым людям, нуждающимся не столько в лечении, сколько в социализации, в ощущении востребованности. Система «Мобильный помощник» обеспечивает пожилым людям безопасность и в то же самое время дает им чувство независимости, уверенности в том, что они по-прежнему самостоятельны, не нуждаются в чужом вмешательстве в свою жизнь.

Суть «Мобильного помощника» максимально приближена к французской модели Teleassistance. Пожилой человек получает мобильный телефон с упрощенной системой набора и приема звонков. В его квартире устанавливается громкоговоритель, который соединяется с call-центром. Таким образом, пожилой человек может в любой момент связаться с оператором, просто нажав кнопку на браслете. Получив звонок, оператор оценивает ситуацию и в зависимости от этого вызывает к своему подопечному экстренные или социальные службы. В свою очередь оператор имеет возможность в любое время связаться с пожилым человеком, узнать о состоянии его здоровья, напомнить о необходимости принять лекарства и т.п.

Сначала мы пытались импортировать систему из Европы: просто закупить необходимое количество аппаратов. Однако почти сразу выяснилось, что процесс ее сертификации в России займет не один год. Поэтому Senior Group приняла решение разработать российский аналог, взяв за образец французскую модель.

В качестве дополнения для людей, которые теряются в пространстве, наша компания предлагает тревожные кнопки — персональные трекеры. До этого момента подобные технологии использовались в России только в сфере охраны имущества. Нажав на кнопку, человек подает сигнал тревоги, который немедленно высвечивается на дисплее оператора call-центра. Оператор видит координаты подопечного на карте и может прийти к нему на помощь.

Уникальной технологией является программное обеспечение системы дистанционного контроля Soft Pomoshnik — автоматизированная система планирования и отслеживания выполнения услуг на дому с возможностью расширения до управления всем комплексом социальных услуг компании Senior Group: call-центры, Сениор Отели, патронажные службы.

Программа является эксклюзивной разработкой компании Senior Group. Soft Pomoshnik — гибкомасштабируемая система, позволяющая генерировать синтетические отчеты любой сложности по всем регионам Российской Федерации, что обеспечивает прозрачность информации на всех уровнях.

WEB-интерфейс программы дает возможность удаленной работы пользователей. Использование современных технологий, таких как Silver Light, DOTNET-FrameWork 3.5 и SQL BD, позволяет сделать интерфейс программы таким же быстрым и эргономичным, как приложения для локального компьютера.

Надежная защита информации обеспечивается благодаря следующим факторам:

- использованию защищенного соединения с базой данных;
- системе авторизации на основе разветвленной системы прав пользователей;
- возможности авторизации на базе LDAP, позволяющей синхронизацию доступа в систему с доменными правами пользователя.

Программа Soft Pomoshnik службы ухода на дому пополняет, хранит и обрабатывает информацию по следующим разделам:





- Клиент (Ф.И.О., возраст, адрес проживания, телефон, физический и социальный статус).
- Вид и количество оказываемых услуг с привязкой по клиентам, времени и датам.
- Персонал, оказывающий услуги (Ф.И.О., должность, ранг).
- Договор (номер, дата) как обоснование оказания услуг.
- Обратная связь по качеству предоставления услуг.
- Отчеты (статистика, анализ, обработка информации).

Фактически это планировщик, который идеальным образом подстраивается под систему работы территориальных управлений социальной защиты. Основное преимущество этой системы состоит в том, что она web-based. Ее не надо устанавливать. С любого компьютера можно зайти на сайт и за 15 секунд скачать эту программу.

Первой опытной площадкой для реализации программы «Мобильный помощник» стал город Калининград. Выбор на «бывший Кенигсберг» пал неслучайно: именно с этой точки на карте Европа кажется совсем близкой. Возможно, именно поэтому инициатива Senior Group о развертывании в городе системы «Мобильный помощник» была положительно воспринята руководителями социальной отрасли. Обеспечивая качественное медико-социальное обслуживание пожилых людей, программа также предоставляет работу инвалидам-надомникам. Это стало возможным благодаря программному обеспечению Soft Pomoshnik, которое позволяет организовывать установку компьютеров в любом месте, а не только в помещении call-центра.

Общая финансовая стоимость проекта — 4,4 миллиона рублей, из которых 2,2 миллио-

на — собственные средства компании Senior Group и 2,2 миллиона — средства Фонда региональных социальных программ «Наше будущее», предоставленные компании на условиях беспроцентного займа. В результате проекта около 350 пожилых и маломобильных людей будут подключены к программе «Мобильный помощник», будет создано 20 рабочих мест, в том числе и для людей с ограниченными возможностями.

Введение новой системы дистанционного контроля состояния позволит в значительной степени оптимизировать расходы региональных и местных бюджетов на содержание патронажных служб. Senior Group уже завтра готова начать в любом регионе России пилотный проект, бесплатно предоставив центрам социального обслуживания свою систему, чтобы совместно протестировать новый продукт. Это реальный способ модернизации социальной сферы, о необходимости которой не так давно говорил Президент России.

Реализуемый в Калининграде проект наглядно демонстрирует, что частно-государственное партнерство является необходимым для развития всей социальной отрасли в целом. Основой и стержнем новой политики должно стать создание отрасли заботы о старшем поколении. Речь не идет о преуменьшении роли государственного сектора, но о развитии негосударственного, путем привлечения частных инвестиций и передового национального и зарубежного опыта управления. Отрасль заботы о старшем поколении должна отличаться от существующей системы социальных служб более высоким профессионализмом, новаторскими идеями и участием частного капитала и, как следствие, обеспечивать более качественную социальную защиту пожилых граждан нашей страны.



ИТОГИ II ВСЕРОССИЙСКОЙ УЧЕБНО-МЕТОДИЧЕСКОЙ КОНФЕРЕНЦИИ ПО ПРЕПОДАВАНИЮ МЕДИЦИНСКОЙ ИНФОРМАТИКИ В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ ВЫСШЕГО И ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

По приказу Минздравсоцразвития России № 886 от 11 ноября 2009 г. на базе Российского государственного медицинского университета прошла II Всероссийская учебно-методическая конференция, на которой были рассмотрены теоретические вопросы информатизации здравоохранения, подняты организационные и методические проблемы преподавания медицинской информатики в высшем и дополнительном медицинском образовании, а также предложены пути дальнейшего совершенствования учебно-педагогического процесса по данной дисциплине.

Доклады участников конференции будут опубликованы в этой рубрике «ВиИТ» в течение года.

В рамках конференции был проведен круглый стол «Актуальные проблемы преподавания медицинской информатики в медицинском и фармацевтическом образовании», где был обсужден целый ряд вопросов, касающихся путей совершенствования преподавания медицинской информатики в учреждениях высшего и дополнительного профессионального образования. Обсужден вопрос кадрового обеспечения преподавания курса «Медицинская информатика», отмечена необходимость организации повышения квалификации преподавательского состава курса на кафедрах ведущих ВУЗов РФ. Участники круглого стола высказались за возвращение основной специальности «Организация здравоохранения и общественное здоровье» выпускникам медицинских ВУЗов по специальности «Медицинская кибернетика». Приход таких специалистов в учреждения здравоохранения позволит организовать сбор, учет, а также формирование отчетности и анализа медицинской

статистической информации с использованием современных информационных технологий.

Активно обсуждалась проблема программного и технического обеспечения курса «Медицинская информатика» (выбор между стандартными лицензионными программными продуктами и средствами открытого программного обеспечения (Open Source), нехватка специализированных медицинских программных продуктов и программно-аппаратных комплексов, использование современных методов коммуникации для учебного процесса и обмена опытом преподавания). В.П. Омельченко и В.К. Гасников обратили внимание участников конференции на проблемы последипломного образования, в том числе на необходимость использования информационных технологий в составе циклов повышения квалификации и тематического усовершенствования в соответствии с профилем врача.

Существенная часть заседания круглого стола была связана с организационно-методическими вопросами преподавания медицинской информатики: увеличением количества аудиторных часов и переносом преподавания дисциплины на более старшие курсы, обсуждением ФГОС 3-го поколения и разработкой новой примерной программы по медицинской информатике.

Рассматривалась возможность организации информационного портала по преподаванию медицинской информатики как места хранения электронных методических пособий и программных средств для учебного процесса, создания общего тезауруса понятий медицинской информатики.

Во исполнение решения I Всероссийской учебно-методической конференции по препода-





даванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования в 2006 г. был подготовлен проект новой программы по медицинской информатике (ответственный — Зарубина Т.В.), однако до настоящего времени его не предлагали для всеобщего обсуждения, так как не был утвержден новый ФГОС. На данный момент разработка ФГОС 3-го поколения находится в завершающей стадии, что позволяет начать активное обсуждение и доработку созданного проекта новой примерной программы по медицинской информатике.

В ходе заседания круглого стола особое внимание было уделено реализации непрерывного ИТ-образования в ВУЗах, а именно, включению в преподавание клинических дисциплин блоков с применением информационных технологий соответствующего профиля.

В целях совершенствования учебно-методической работы и повышения качества подготовки студентов по медицинской информатике на конференции принято решение:

1. Выразить благодарность Оргкомитету за организацию II Всероссийской учебно-методической конференции по преподаванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования и просить продолжить практику обмена опытом преподавания медицинской информатики и повышения квалификации.

2. Поручить:

2.1. Комиссии в составе: Зарубина Т.В., Гасников В.К., Николаиди Е.Н., Карась С.И., Кобринский Б.А., Кудрина В.Г., Монич В.А., Николаев А.Г., Омельченко В.П., Проценко В.Д., Салманов П.Л., Санников А.Г., Чернов В.И.:

- анализ предложений по созданию информационного портала по преподаванию дисциплины «Медицинская информатика»;

- организацию обмена методическими материалами и программными средствами, используемыми в учебном процессе по медицинской информатике;

- анализ представленных на рынке современных программных продуктов и рекомендацию наиболее подходящих из них в качестве программного обеспечения для учебного процесса.

2.2. Зарубиной Т.В. и Николаиди Е.Н.:

- организовать обсуждение проекта новой примерной программы по дисциплине «Медицинская информатика»;

- анализ и учет поступивших предложений по изменению и дополнению примерной программы по дисциплине «Медицинская информатика».

3. Просить ректора Российского государственного медицинского университета (акад. РАМН, проф. Володин Н.Н.) рассмотреть возможность организации на базе кафедры медицинской кибернетики и информатики циклов повышения квалификации для преподавателей, осуществляющих преподавание медицинской информатики в ВУЗах, в целях отработки методики преподавания дисциплины.

4. Рекомендовать ректорам медицинских и фармацевтических ВУЗов в целях реализации непрерывного ИТ-образования использовать информационные технологии соответствующего профиля при преподавании клинических дисциплин (5% от времени аудиторных занятий).

5. Просить Министерство здравоохранения и социального развития Российской Федерации рассмотреть вопросы:

- о восстановлении в списке основных врачебных специальностей для выпускников медицинских ВУЗов по специальности «Медицинская кибернетика» специальность «Организация здравоохранения и общественное здоровье»;

- предусмотреть в структуре последипломной профессиональной подготовки всех врачебных специальностей подготовку по профилю использованию современных информационных технологий;

- предусмотреть в перспективных планах работы организацию и проведение регулярных учебно-методических конференций по преподаванию медицинской информатики 1 раз в 2–3 года.



Т.В. ЗАРУБИНА,

д.м.н., профессор, заведующая кафедрой медицинской кибернетики и информатики
Российского государственного медицинского университета, г. Москва, t_zarubina@mail.ru

Е.Н. НИКОЛАИДИ,

к.м.н., доцент кафедры медицинской кибернетики и информатики Российского
государственного медицинского университета, г. Москва

АНАЛИЗ ДИНАМИКИ ПРЕПОДАВАНИЯ МЕДИЦИНСКОЙ ИНФОРМАТИКИ В УЧРЕЖ- ДЕНИЯХ ВЫСШЕГО И ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УДК 378.147:004:614(470)

Зарубина Т.В., Николаиди Е.Н. Анализ динамики преподавания медицинской информатики в учреждениях высшего и дополнительного образования Российской Федерации (ГОУ ВПО РГМУ Росздрава)

Аннотация. Статья представляет анализ результатов анкетирования, проведенного при подготовке Второй Всероссийской учебно-методической конференции по преподаванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования. Обсуждаются некоторые методические и организационные проблемы преподавания курса.

Ключевые слова: учебная дисциплина «Медицинская информатика»; учебно-методическая конференция; специализированное программное обеспечение; учебно-методическое обеспечение.

UDC 378.147:004:614(470)

Zarubina T.V., Nikolaidi E.N. The analysis of dynamics of teaching of medical computer science in establishments of the higher and an additional education of the Russian Federation (Russian State Medical University)

Abstract. The article presents the analysis of the results of a questionnaire on teaching discipline medical informatics in high school medical education. Some of the methodological and organizational problems are analyzed.

Keywords: academic discipline «medical informatics»; educational-methodical conference; specialized software; training-methodical support.

Кафедра медицинской кибернетики и информатики Российского государственного медицинского университета (РГМУ) имени Н.И. Пирогова, на базе которой в ноябре 2009 г. проводилась Вторая Всероссийская учебно-методическая конференция по преподаванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования, была создана в 1973 г. С.А. Гаспаряном. В настоящее время это коллектив, включающий 6 профессоров, 8 доцентов, старших преподавателей, ведущих и старших научных сотрудников, инженеров, аспирантов; более половины коллектива кафедры составляют ее выпускники. Кафедра является выпускающей по вузовской специальности 060114 «Медицинская кибернетика».

Выпуск врачей-кибернетиков осуществляется в настоящее время на медико-биологических факультетах двух высших учебных заведений страны: РГМУ и Сибирского государственного медицинского университета. В сентябре 2009 г. был осуществлен первый набор студентов на отделение медицинской кибернетики Медицинского института Пензенского государственного университета. Будущим врачам-кибернетикам преподается пять профильных предметов, несколько специальных курсов по выбору студентов; заканчивается образование выполнением и защитой дипломной работы. Только РГМУ выпущено уже более 1000 специалистов данного профиля.

Кафедра медицинской кибернетики и информатики РГМУ имени Н.И. Пирогова является общеуниверситетской, и преподава-



ние на ней осуществляется для всех отделений и факультетов ВУЗа. Особое место среди преподаваемых дисциплин занимает курс «Медицинской информатики».

Практическая медицина 21 века как в нашей стране, так и за рубежом немыслима без использования информационных технологий. Поэтому около десяти лет назад в учебные программы всех врачебных специальностей была включена дисциплина «Медицинская информатика», преподавание которой осуществляется в соответствии с типовой учебной программой, разработанной РГМУ и утвержденной МЗ РФ в 2000 г. [1].

Основная цель курса «Медицинская информатика», сформулированная в типовой программе: дать студентам сведения о современных компьютерных технологиях в приложении к медицине и здравоохранению, дать знания о методах информатизации врачебной деятельности, автоматизации клинических исследований, компьютеризации управления в системе здравоохранения, научить пользоваться компьютерными приложениями для решения задач медицины и здравоохранения, средствами информационной поддержки врачебных решений, автоматизированными медико-технологическими системами.

В ноябре 2005 года на базе Российского государственного медицинского университета по распоряжению Министерства здравоохранения и социального развития РФ [2] и при курировании Всероссийским учебно-научно-методическим центром (ВУНМЦ) по непрерывному медицинскому и фармацевтическому образованию была проведена Первая Всероссийская учебно-методическая конференция по вопросам преподавания медицинской информатики в медицинских ВУЗах России. Основное внимание на ней было уделено организационным и методическим проблемам преподавания медицинской информатики и его совершенствования с использованием современных достижений развивающейся информатики, психологии и педагогики, методик преподавания и опыта кафедральных коллективов. В

решении Первой Всероссийской учебно-методической конференции по вопросам преподавания медицинской информатики в медицинских ВУЗах России была отмечена практическая значимость данной дисциплины в подготовке современного врача и сформулированы основные задачи, решение которых необходимо для дальнейшего развития и совершенствования преподавания медицинской информатики.

Для координации работ по совершенствованию учебно-методического обеспечения курса «Медицинская информатика», а также для эффективной реализации принятых на Первой Всероссийской учебно-методической конференции решений весной 2007 года была создана Проблемная учебно-методическая комиссия по вопросам преподавания медицинской информатики. В перечень задач, решаемых данной комиссией, входят экспертная оценка издаваемой учебно-методической литературы и предлагаемых вариантов типовых тестовых заданий для текущего контроля знаний студентов по дисциплине «Медицинская информатика»; обсуждение предметного содержания типового набора специализированного программного обеспечения учебного процесса и проекта новой программы по дисциплине «Медицинская информатика».

В целях совершенствования преподавания медицинской информатики в учреждениях высшего и дополнительного профессионального образования, а также подготовки медицинских специалистов в области информатизации здравоохранения в мае 2008 года в рамках Всероссийской конференции «Информатизация здравоохранения 2008» состоялось расширенное заседание Проблемной учебно-методической комиссии по вопросам преподавания медицинской информатики [3]. Основное внимание участников этого заседания было уделено проблемам и перспективам преподавания медицинской информатики на вузовском и последипломном этапах подготовки врачей.

При подготовке Первой Всероссийской учебно-методической конференции необходимо



было оценить ситуацию с преподаванием дисциплины «Медицинская информатика» в различных ВУЗах Российской Федерации. В 2005 году для решения этой задачи при активном участии ВУНМЦ Минздравсоцразвития разрабатывалась и рассылалась по ВУзам анкета, включающая в себя вопросы по организации в ВУЗе преподавания дисциплин «Информатика» и «Медицинская информатика». Такая же анкета (без изменений) была предложена ВУзам Оргкомитетом Второй Всероссийской учебно-методической конференции по преподаванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования. Повторное анкетирование позволило оценить не только сложившуюся в настоящее время ситуацию с преподаванием указанных дисциплин, но и динамику учебно-педагогического процесса.

Общая характеристика заполненных анкет

Нами получено 26 заполненных анкет: 11 из медицинских государственных университетов, 8 из медицинских государственных академий, 4 из государственных классических университетов, 3 из учреждений последипломного образования (табл. 1).

Оценить динамику учебно-педагогического процесса по информатике и медицинской информатике возможно по данным 16 ВУЗов, приславших заполненные анкеты в 2005 и 2009 годах (табл. 2).

Преподавание дисциплины «Медицинская информатика»

По результатам анализа 23 анкет из высших медицинских учебных заведений и государственных университетов, преподающих дисциплину «Медицинская информатика» студентам медицинских факультетов, можно сделать следующие обобщения:

- Кубанский ГМУ — дисциплина «Медицинская информатика» не преподается (такая ситуация осталась без изменений с 2005 года);

- дисциплина «Медицинская информатика» чаще преподается на кафедрах, в названиях которых есть словосочетание «медицинская информатика» или указано «с курсом медицинской информатика» (11 ВУЗов, в Воронежской ГМА им. Н.И. Бурденко «Медицинская информатика» преподается на кафедре информационных систем, в Белгородском ГУ — на кафедре пропедевтики внутренних болезней и клинических информационных технологий), в 3 ВУЗах дисциплина преподается на кафедрах общественного здоровья и здравоохранения, в 3 ВУЗах — на кафедрах медицинской физики с курсом информатики (табл. 3);

- разделы курса «Медицинская информатика» преподаются на одной кафедре (за исключением Ростовского ГМУ, в котором преподавание дисциплины осуществляется на кафедрах Общественного здоровья и здравоохранения и Медицинской и биологической физики);

- в 20 анкетах указано наличие типовой учебной программы по медицинской информатике (в большинстве случаев — утвержденной МЗ РФ в 2000 г.); особо необходимо указать на отсутствие типовой учебной программы по данным анкет Смоленской ГМА (ситуация не изменилась с 2005 года) и Красноярского ГМУ;

- преподаватели, ведущие курс по данной дисциплине, чаще всего имеют специальность: «Лечебное дело» (11), инженер (7), «Математика-информатика» (9), «Физика и организация здравоохранения» (по 4) (рис. 1);

- фактическое количество аудиторных часов в большинстве случаев находится в диапазоне от 34 до 38; преподавание дисциплины осуществляется в основном на 5–7 семестрах (рис. 2 и рис. 3);

- среди предложений по оптимальному количеству аудиторных часов на преподавание дисциплины встречаются: увеличить до 45–50 часов — в 9 анкетах, до 60 часов — в 1 анкете, до 70–75 часов — в 5 анкетах; 4 ВУЗа считают количество имеющихся аудиторных часов на преподавание медицинской информатики достаточным; КемГМУ предла-





Таблица 1

Список ВУЗов, предоставивших заполненные анкеты

<i>Медицинские государственные университеты (11)</i>	<i>Государственные классические университеты (4)</i>
Алтайский ГМУ	Белгородский государственный университет
Башкирский ГМУ	Российский университет Дружбы народов
Владивостокский ГМУ	Тулеский государственный университет
Казанский ГМУ	Ульяновский государственный университет
Красноярский ГМУ	
Кубанский ГМУ	
Российский ГМУ	
Ростовский ГМУ	
Рязанский ГМУ	
Самарский ГМУ	
Сибирский ГМУ	
<i>Медицинские государственные академии (8)</i>	<i>Учреждения последипломного образования (3)</i>
Воронежская ГМА им. Н.И. Бурденко	Российская МАПО
Ижевская ГМА	Санкт-Петербургская МАПО
Кемеровская ГМА	Новокузнецкий ГИУВ
Нижегородская ГМА	
Оренбургская ГМА	
Смоленская ГМА	
Тюменская ГМА	
Ярославская ГМА	

Таблица 2

Список ВУЗов, предоставивших повторно заполненные анкеты

Алтайский ГМУ	Кубанская ГМА
Белгородский ГУ	Нижегородская ГМА
Владивостокский ГМУ	Оренбургская ГМА
Воронежская ГМА им. Н.И. Бурденко	Российский ГМУ
Ижевская ГМА	Ростовский ГМУ
Казанский ГМУ	Самарский ГМУ
Кемеровская ГМА	Смоленская ГМА
Красноярская ГМА	Ярославская ГМА

гает увеличить объем дисциплины «Медицинская информатика» до 140–160 аудиторных часов, а РУДН — до 216 часов;

- при анализе выполнения учебной программы по отдельным разделам дисциплины выявлено, что в 17 ВУЗах программа выполняется в полном объеме; не преподаются

разделы по моделированию физиологических процессов (ТюмГМА), по экспертным системам (РостГМУ) и по использованию ИС в управлении здравоохранением (ОргМА); значительные отличия в используемой рабочей программе от типовой отмечены в анкете из Тульского ГУ: практическая работа ориенти-

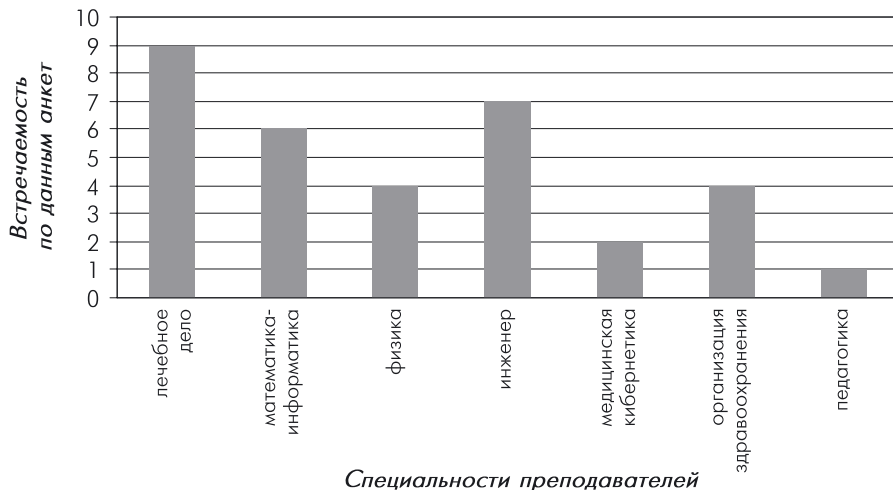


Рис. 1.
Специальности преподавателей

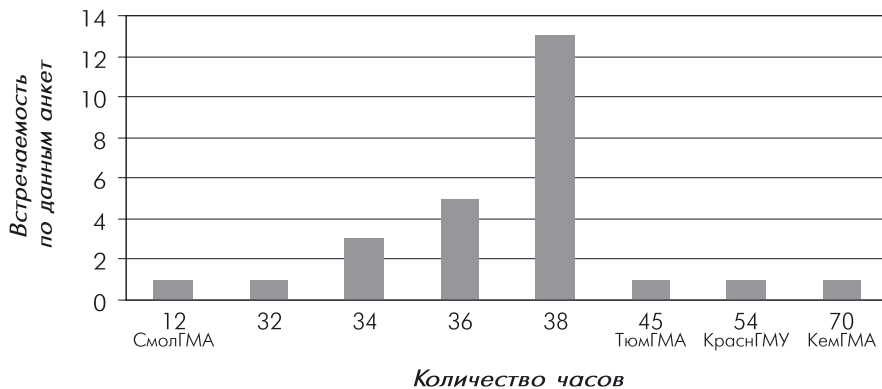


Рис. 2.
Фактическое количество аудиторных часов

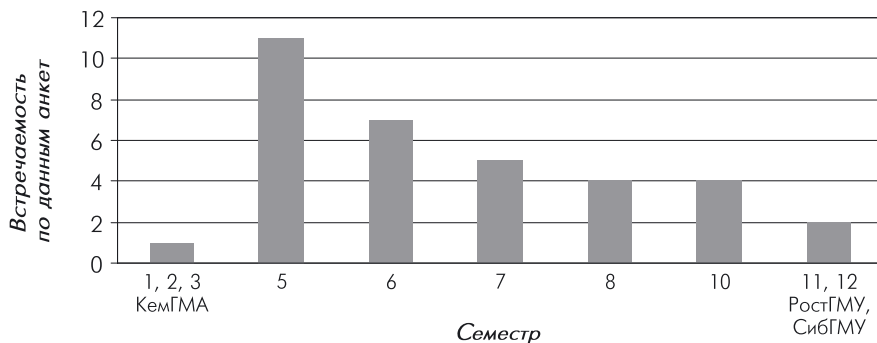


Рис. 3.
Фактическое место курса «Медицинская информатика» в учебных планах

рована на используемые в здравоохранении программные продукты, включая регистры по проблемным направлениям здравоохранения; данных о выполнении учебной программы в СмоЛГМА не предоставлено;

- курс оснащен вычислительной техникой: в большинстве случаев работа осу-

ществляется в режиме 1 компьютер на 1–2 студента (20 ВУЗов); в 20 анкетах из 22 анализируемых отмечено, что рабочее место преподавателя оснащено компьютером, и преподавание осуществляется не только в виде демонстраций (исключением стал БашГМУ).





Таблица 3

Перечень кафедр, на которых преподают «Медицинскую информатику»

Медицинской информатики	1	11
Медицинской кибернетики и информатики	1	
Медицинской информатики и высшей математики	1	
Медицинской информатики и инновационных технологий	1	
Медицинской и биологической физики с курсом медицинской информатики	1	
Лучевой диагностики и терапии с курсом медицинской информатики	1	2
Общественного здоровья и здравоохранения с курсом медицинской информатики	5	
Информационных систем	1	
Кафедра пропедевтики внутренних болезней и клинических информационных технологий	1	
Общественного здоровья и здравоохранения	3	
Медицинской физики с курсом информатики	3	
Математики и информатики	1	
Медицинской и биологической физики	1	
Санитарно-гигиенических и профилактических дисциплин	1	
Лучевой диагностики и онкологии	1	

Из учебно-методической литературы по «Медицинской информатике» наиболее часто используются:

- Медицинская информатика. Практикум. Гельман В.Я., Санкт-Петербург, 2001 — 12 упоминаний;
- Практикум по медицинской информатике. Омельченко В.П., Демидова А.А., Ростов-на-Дону, 2003 — 7 упоминаний;
- Медицинская информатика. Учебное пособие. Чернов В.И. и соавт., Воронеж, 2004 — 6 упоминаний;
- Медицинская информатика. Учебное пособие. Кудрина В.Г., Москва, 1999 — 3 упоминания.

Медицинская информатика. Учеб. для студ. высш. учеб. заведений/Б.А. Кобринский, Т.В. Зарубина. — М.: Издательский центр «Академия», 2009; Медицинская информатика. Учебное пособие/С.Д. Гусев.— Красноярск: Издательство, ООО «Версо», 2009.

Наличие собственных разработок для курса «Медицинская информатика» отмечено в 16 анкетах, в том числе указаны следующие пособия:

- Медицинская информатика. Практикум. — СибГМУ, Томск, 2002;
- Медицинская информатика. Методическое пособие для преподавателей. — М., РГМУ, 2005;
- Косарева Д.И., Хайбуллина И.Р. Методические указания и контрольные задания по медицинской информатике. — Уфа, 2006;
- Основы медицинской информатики: учебно-метод. пособие/А.В. Аладышев, Е.А. Субботин. — Барнаул: АГМУ, 2008;
- Руководство к практическим занятиям по общественному здоровью и здравоохранению, медицинской информатике. — Ижевск, 2008;
- Информатизация здравоохранения. Хромушин В.А., Черешнев А.В. — Тула, 2007.

Необходимыми методическими разработками в большинстве откликнувшихся на анкетирование ВУЗов практическая часть курса оснащена на 100% (19 высших учебных заведений). Об обеспечении практических занятий методическими разработками на 80% сообщил Ульяновский ГУ, на 75% — РязГМУ. СмолГМА сообщила, что методические материалы находятся в стадии разработки.



По-прежнему, одной из самых сложных проблем, связанных с преподаванием дисциплины «Медицинская информатика», остается оснащение курса специальным программным обеспечением. Использование специализированного программного обеспечения в курсе «Медицинская информатика» отмечено в большинстве случаев (16 анкет из 22 анализируемых). Однако список указанных программных продуктов весьма разнороден и в основном включает в себя собственные разработки.

Среди перечисленных в ответах программных средств присутствуют: МИС «Кондопога», АС «Стационар», АС «Поликлиника», МИС «Интерин Promis», «Управление коечным фондом региона», МИС «Медстатфин», «Кадры ЛПУ», Медико-экономическая информационная система, АС «Квалификация», АС «Управление здравоохранением округа Москвы», МИС «Department», МИС «Интерис», АРМ «Травматологический статус», АРМ санитарного врача «Санитас», АРМ врача общей практики и др. Таким образом можно отметить, что среди используемых программных средств преобладают системы учрежденческого уровня, МИС отделений, автоматизированные рабочие места врачей.

Оценка динамики учебно-педагогического процесса по дисциплинам «Информатика» и «Медицинская информатика»

Среди 16 ВУЗов, повторно приславших заполненные анкеты, одна анкета — из Белгородского ГУ и 15 анкет — из высших медицинских учебных заведений (в том числе анкета из Кубанского ГМУ, где преподавание медицинской информатики не ведется, и анкета из Самарского ГМУ, в которой не содержится сведений о преподавании медицинской информатики). Таким образом, оценка динамики учебно-педагогического процесса по дисциплинам «Информатика» и «Медицинская информатика» проводилась по 14 анкетам из высших учебных заведений.

Проведенный анализ позволяет сделать следующие выводы:

- абсолютное большинство анкет свидетельствует о повышении уровня владения материалом по основам информатики у обучаемых студентов (на *рис. 4* указан процент студентов с удовлетворительным уровнем знаний);
- в трех ВУЗах (Владивостокском ГМУ, Ярославской и Ижевской ГМА) в название кафедры, преподающей медицинскую информатику, добавлено уточнение «с курсом медицинской информатики»;
- принципиальных изменений в организации преподавания дисциплины «Медицинская информатика» (количество аудиторных часов, фактическое место курса в учебном плане, наличие типовой программы и специальности преподавателей) не выявлено (*рис. 5*).

Преподавание дисциплины «Медицинская информатика» в последипломном медицинском образовании было представлено в 3 анкетах: Российской МАПО, Санкт-Петербургской МАПО и Новокузнецкого ГИУВ. Анализ полученных ответов выявил существенные различия в объеме и содержании используемых рабочих учебных программ по данной дисциплине, отсутствие единого подхода в методике и организации учебного процесса.

В заключение необходимо отметить основные пожелания и предложения, сформулированные в абсолютном большинстве анкет, полученных Оргкомитетом II Всероссийской учебно-методической конференции по преподаванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования. Прежде всего это необходимость организации циклов повышения квалификации для преподавателей, ведущих курс «Медицинская информатика», а также конструктивное рассмотрение вопроса о создании типового набора специального программного обеспечения и базы тестовых вопросов для учебного процесса по данной дисциплине.



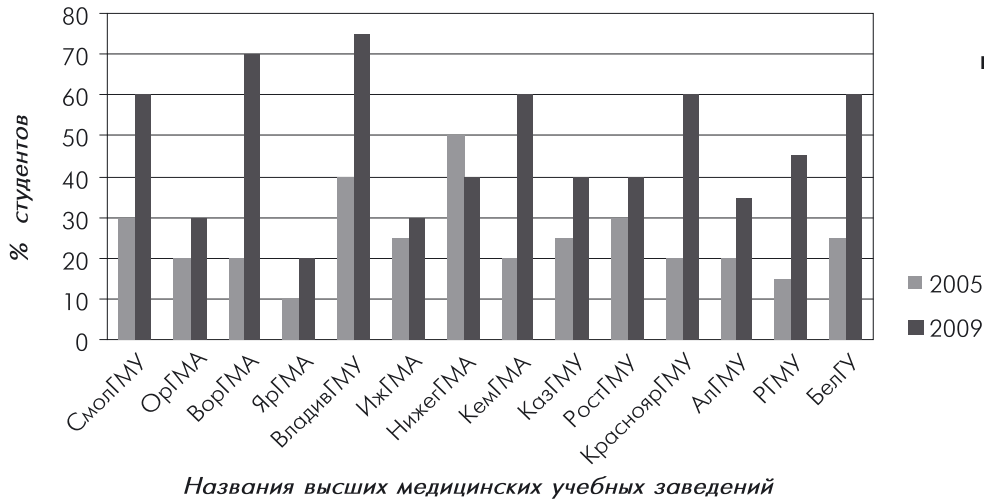


Рис. 4. Изменения в оценке знаний студентов по основам информатики

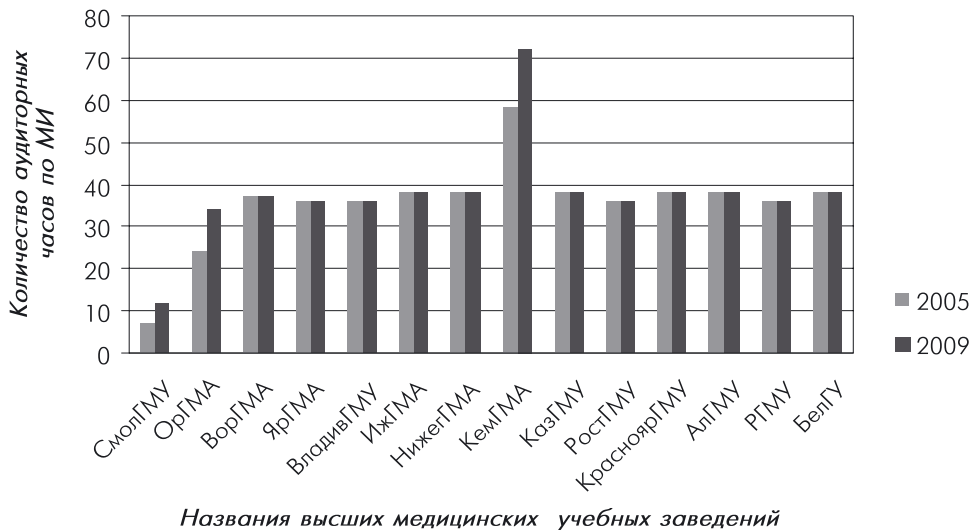


Рис. 5. Сравнение количества аудиторных часов по дисциплине «Медицинская информатика»

Решение указанных проблем позволит существенно поднять качество учебно-педагогического процесса и обеспечить непрерывность преподавания дисциплины «Медицинская информатика», необходимой современному врачу в его повседневной практической работе.

Главными особенностями преподавания дисциплины «Медицинская информатика» на кафедре медицинской кибернетики и информатики РГМУ им. Н.И. Пирогова являются осуществление преподавания врачами-кибернетиками, имеющими опыт научных разработок и проектирования систем; использование совре-

менных программных средств; широкое использование как формы обучения решения ситуационных задач в рамках специальных программных средств при индивидуальной работе с компьютером. Тематический план практических занятий включает МИС в управлении здравоохранением, Компьютерное моделирование фармакокинетических процессов, Автоматизированные медико-технологические системы контроля и управления функциями организма, Использование автоматизированного рабочего места врача в клинической практике, Использование МИС в управлении лечебно-профилактическими учреждениями.



Несмотря на множество проблем, связанных с преподаванием медицинской информатики, первые результаты уже есть: больше выпускников успешно используют в своей профессиональной деятельности МИС, некоторые пропагандируют применение МИС и даже сами приходят работать в область информатизации здравоохранения.

Со временем информационные технологии должны «прорасти» все медицинское образование, включая клинические дисциплины. Это неизбежно приведет к изменению самого образования.

В учреждениях последипломного образования, на факультетах усовершенствования врачей высших учебных заведений проводятся курсы повышения квалификации и тематического усовершенствования по применению информационных технологий в здравоохранении в объеме 72, 144 и более часов. Однако по-прежнему отсутствует возможность профессиональной переподготовки врачей по медицинской информатике, так как в номенклатуре врачебных специальностей и должностей отсутствуют как соответствующая специальность, так и должность.

О целесообразности введения специальности «Медицинская информатика» в номен-

клатуру специальностей последипломной подготовки врачей (как специальности, требующей дополнительной подготовки, при основной специальности «Организация здравоохранения и общественное здоровье») и врачебных должностей речь на наших конференциях и круглых столах шла неоднократно. Большинство — за введение такой специальности, однако, все понимают, что такую проблему нужно решать системно, после организационно-правовой проработки. А начинать необходимо с возвращения в перечень основных врачебных специальностей для вузовской специальности «Медицинская кибернетика» специальности «Организация здравоохранения и общественное здоровье».

Медицинская информатика все больше внедряется в разные направления клинической медицины и здравоохранения. Улучшение и унификация преподавания медицинской информатики и информационных технологий в медицинских образовательных учреждениях высшего и дополнительного профессионального образования; инициативы по нормативному обеспечению подготовки кадров по медицинской кибернетике и медицинской информатике — наша миссия.

ЛИТЕРАТУРА



1. Программа по медицинской информатике для студентов высших медицинских учебных заведений. — М.: МЗ РФ. ГОУ ВУНМЦ. — 2000. — 9 с.
2. Приказ МЗ и СР РФ № 3359-ВС от 18.07.2005 «О проведении Всероссийской учебно-методической конференции по преподаванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования».
3. Приказ МЗ и СР РФ № 3040-РХ от 28.04.2008 «О проведении расширенного заседания Проблемной учебно-методической комиссии по медицинской информатике в рамках 4-го Международного специализированного форума «Медицина-2008» и Всероссийской конференции «Информатизация здравоохранения-2008».
4. Приказ МЗ и СР РФ № 886 от 11.11.2009 «О проведении II Всероссийской учебно-методической конференции по преподаванию медицинской информатики в образовательных учреждениях высшего и дополнительного профессионального образования».



ИНФОРМАТИЗАЦИЯ ДОЛЖНА СТАТЬ НЕОТЪЕМЛЕМОЙ ЧАСТЬЮ ИНФРАСТРУКТУРЫ МЕДИЦИНСКОГО УЧРЕЖДЕНИЯ

Сегодня гостем рубрики является Зоя Борисовна Рахманова, руководитель Медицинского информационно-аналитического центра в составе Московского областного научно-исследовательского клинического института (МОНКИ) им. М.Ф. Владимирского. Кандидатскую диссертацию «Применение логико-лингвистических методов при построении диагностических медицинских систем» защитила на стыке специальностей «АСУ» и «Управление в биологических и медицинских системах». Разработала оригинальную экспертную систему, основанную на методологии искусственного интеллекта. Инициатор развития в Московской области системы «Телемедицина Подмосковья». Вопросы Зое Борисовне задают Наталия Куракова и Александр Гусев.



Н.К.: По заданию Департамента информатизации Минздравсоцразвития Вы проводили анкетирование регионов с целью выяснения наиболее подготовленных к реализации Системного проекта персонифицированного учета медицинской помощи. Какие параметры «автоматизации ЛПУ» были выбраны в качестве реперных и в каком диапазоне варьировались выявленные показатели для отдельных ЛПУ и регионов?



Зоя Рахманова: На конференциях по информатизации озвучивалось, что решения Департамента принимались на основании сведений о числе компьютеров и их типах на душу медицинского персонала, развитости сети Интернет в результате анкетирования. «Реперные» показатели, которые проще всего было просчитать, можно увидеть в 8 сводных таблицах, рассчитанных из анкет и выложенных на сайте ЦНИИОЗ (www.mednet.ru). А вот с другими таблицами дело обстоит сложнее.

Золотым правилом постановщика задач является следующее. Все вводимые в систему данные для дальнейшего свода и анализа должны быть четко определены как в количественном формате (в инструкции необходимо отразить единицы измерения, источник информации и т.п.), так и в качественном формате (создать классификаторы, справочники и пр.). К сожалению, это правило к анкете для оценки уровня развития информационной и технологической инфраструктуры государственных и муниципальных медицинских учреждений не было применено. Нечеткость определений начи-



нается уже с первого пункта анкеты «Полное наименование учреждения здравоохранения». И как только не заполнялся этот пункт! В результате непонятно, как в этой каше можно было выловить значения кодификатора. Неоднозначно понимались исполнителями пункты «Численность работников в учреждении здравоохранения (согласно штатному расписанию)» и «Численность работников в удаленных структурных подразделениях учреждения здравоохранения (согласно штатному расписанию)». Показатель «Оснащение работников компьютерами» для РФ по результатам анкетирования, представленным на сайте ЦНИИОЗ, равен 0,09, для Московской области — 0,1. Этот же показатель по Московской области, рассчитанный по данным из формы № 30, равен 0,19. Такая разница при совпадении числа компьютеров в анкете и форме № 30 объясняется значительным расхождением в численности медперсонала. Так, в форме № 30 число медработников — 68 407, в анкете — 132 228, что почти в два раза больше. А этот показатель был одним из «реперных».

При отсутствии внятно написанной инструкции возникли проблемы и множество вопросов при заполнении таблиц «Общая характеристика компьютерных сетей учреждения здравоохранения», «Организация телефонной связи в учреждении здравоохранения», «Характеристики доступа к сети Интернет», «Прикладное программное обеспечение, используемое на компьютерах в учреждении здравоохранения», «Характеристика автоматизации основных задач в учреждении здравоохранения». Очень сложной для понимания оказалась таблица «Характеристика каналов связи для электронного обмена данными учреждения здравоохранения с участниками системы здравоохранения и обязательного медицинского страхования».

Кроме того, одна и та же информация дважды заносилась в некоторых таблицах, что непозволительно в автоматизированных системах. Непонятно, как анализировались «Учетные карточки программного средства, эксплуатируемого в учреждении здравоохранения».

В результате эти анкеты исполнители сдавали с третьего—четвертого заходов. Особенно мучительно было заполнять анкеты там, где не было своего ИТ-специалиста. Если подробно рассматривать процесс и итоги анкетирования, это может быть темой отдельной статьи. Будем надеяться, что этот опыт будет полезен, учитывая тот факт, что это анкетирование было в принципе необходимо. К сожалению, для муниципалитетов и ЛПУ Московской области аналитика не проводилась, так как программа обработки анкет рассчитывает показатели только на уровне Федерации и субъектов РФ.

В Московской области такого типа анкетирование было проведено в 2001 г. Рассмотрение вопроса разработки системы мониторинга здоровья населения, системы многофакторной и многоцелевой, для решения задач которой необходимо повсеместное внедрение унифицированных программных средств, телекоммуникационных технологий и слияние различных баз данных, требует определенной готовности на местах.

Для выявления готовности как служб статистики — основных поставщиков информации о деятельности учреждений и состояния здоровья, так и служб информатизации, а также с целью проведения мониторинга состояния информатизации муниципальных ЛПУ было проведено анкетирование. Анкета под наименованием «Анкета руководителя информационно-статистической службы» была разработана в отделе информационных систем и прогнозирования Минздрава Российской Федерации (автор — Какорина Е.П.).





И если сравнить результаты анкетирования 2001 и 2009 годов, мы увидим в основном прогресс только в увеличении числа и улучшении качества компьютеров, большее разнообразие в «зоопарке» прикладного программного обеспечения и развития Интернета и телемедицинских технологий.

Н.К.: Глава Департамента информатизации О.В.Симаков несколько раз говорил о нецелесообразности иметь в штате ЛПУ ИТ-специалиста. Разделяете ли Вы его мнение?



З.Р.: Для медицинских учреждений, уже имеющих собственную развитую ИТ-инфраструктуру, обязательно нужны собственные ИТ-специалисты. Нет смысла и экономически не оправдано ломать уже имеющуюся структуру и переходить на услуги сторонних специалистов.

Другое дело учреждение с неразвитой ИТ-инфраструктурой (например, пара компьютеров в бухгалтерии и один в статистике). Такие учреждения фактически пользуются услугами «приходящего» ИТ-администратора. В такой ситуации ИТ-аутсорсинг действительно выгоден. При этом необходимо заключать договор обслуживания со специализированной компанией, причем уровень квалификации ИТ-специалистов должен быть достаточно высок и стоимость услуг приемлема.

Выбор должен оставаться за медицинским учреждением. В любом случае у медицинских организаций должна быть статья расходов, предусматривающая оплату ИТ-услуг.

Н.К.: По мнению Олега Владимировича, все непрофильные функции в ЛПУ и прежде всего информатизация, должны быть отданы на аутсорсинг. По Вашему мнению, возможно ли привлечение сторонних специалистов для поддержания МИС и какова «цена вопроса» такой услуги?



З.Р.: Поддержание ИТ-инфраструктуры вполне оправдано отдавать на аутсорсинг, а вот для текущего администрирования МИС (апробация и внедрение прикладного программного обеспечения, ведение внутренних справочников, списков персонала, перечней оказываемых услуг, настройка печатных и экранных форм, «конструирование» отчетов и т.п.) необходим специалист в медучреждении, например, врач-информатик (аналитик). Где только их взять? Кроме этого, аутсорсинг для решения задач централизованного ведения электронных историй болезней сторонними организациями, не входящими в сферу здравоохранения, чреват сложностями с исполнением 152 закона об информационной безопасности и ответственности за сохранение персональных данных (человеческий фактор).

Текущее обслуживание компьютеров, серверов, администрирование локальных вычислительных сетей, поддержка и настройка системного программного обеспечения и т.п. — эти и подобные работы могут эффективно выполняться специализированными компаниями на условиях ИТ-аутсорсинга.

Обслуживание МИС, как правило, осуществляется разработчиком или поставщиком, то есть тоже «внешними» специалистами.

Но текущие вопросы по наиболее эффективному использованию «инструментов», предоставляемых МИС, должен решать специалист, работающий в данном учрежде-



нии, хорошо знающий специфику работы своей организации и владеющий возможностями МИС.

Информатизация не может быть «непрофильной функцией». Сегодня это — единственный «инструмент», позволяющий среднему медперсоналу, врачу, заведующему отделением, главному врачу, статистике, специалисту по организации здравоохранения и т.д. эффективно обрабатывать постоянно растущий поток информации в медучреждении. Информатизация — это не панацея, но абсолютно необходимое условие реального повышения эффективности лечебно-диагностического процесса, а также универсальный «инструмент» для оптимизации, а значит в конечном итоге, значительной экономии затрат.

Но это возможно только при комплексной информатизации, то есть при реальном внедрении автоматизированных рабочих мест врачей и электронной истории болезни (медицинской карты). Все остальное (учет медицинских услуг, медицинская статистика и т.п.) вытекает из автоматизированной обработки истории болезни. Только история болезни (медицинская карта) является единственным достоверным источником любой информации о состоянии здоровья пациента, которая может быть востребована как страховыми организациями, так и на любом уровне управления.

Если история болезни (медицинская карта) будет вестись в электронном виде и будет структурирована соответствующим образом, любая статистика и любой учет на любом уровне (ЛПУ, органы управления здравоохранением района, субъекта Федерации, Федерации) становятся абсолютно прозрачными и понятными, о чем и говорилось в докладе О.В. Симакова. Но для этого необходима полная компьютеризация всех ЛПУ.

Однако путь к полной компьютеризации всех рабочих мест в здравоохранении очень непрост и вряд ли будет пройден полностью до 2013 года, как предполагается в презентации О.В. Симакова.

Во-первых, необходимо довести показатель «Оснащение работников компьютерами» до 1. Рассчитать требуемое количество компьютеров несложно, и эта цифра будет намного больше 4 компьютеров на одно юридическое лицо ($7457 \times 4 = 29\,828$) — столько компьютеров, по словам О.В.Симакова, будет закуплено по федеральной программе и передано в ЛПУ для ведения электронных историй болезни. Для примера: одно юридическое лицо — МУЗ «Ногинская ЦРБ» включает 17 входящих учреждений (9 больничных учреждений, 8 АПУ, 1 женская консультация, 1 роддом, 4 отделения скорой медпомощи, 1 станция переливания крови); ГУЗ «Московский областной диспансер» требуется 153 компьютера и организация локальной сети между 17 службами. Откуда взять финансирование для приобретения компьютеров и развития ИТ-инфраструктуры, необходимой для оснащения всех сотрудников, и на каком основании?

Во-вторых, во сколько обойдутся внедрение и адаптация прикладного программного обеспечения (МИС + система сбора и обработки медстатинформации на уровне учреждения, района, субъекта Федерации, Федерации)?

В-третьих, как будет организовано обучение медперсонала навыкам работы на компьютере и с МИС? А обучаемых должно быть немало, учитывая показатель «Оснащение работников компьютерами», равный 0,09.





В-четвертых, на чьи плечи лягут организация и оплата трафика тотальной сети передачи данных?

Это лишь те проблемы, которые лежат на поверхности, и пути решения хотя бы этих проблем должны быть предложены Департаментом информатизации Минздравсоцразвития. Необходимо для выполнения важной и перспективной задачи персонализированного учета услуг и основанной на этом аналитики состояния дел в здравоохранении понять существующие реалии и тщательно проработать все связанные с этим вопросы.

И тут мы опять приходим к выбору — что можно отдать на аутсорсинг, а что нет. Построение развитой ИТ-инфраструктуры, включающей в том числе и автоматизированные рабочие места каждого врача, — практически непосильная задача для медицинского учреждения, но может быть легко реализовано с помощью аренды серверов, «дата-центров», каналов связи и даже отдельных рабочих мест у специализированных компаний и обслуживаться на условиях аутсорсинга.

Собственно на рабочих местах вполне достаточно обычных «офисных» компьютеров или даже «тонких клиентов», то есть терминальных устройств, обеспечивающих подключение к серверу. С точки зрения программного обеспечения, на рабочем месте может быть только Интернет-браузер.

Предварительные расчеты показывают, что для 15–20 рабочих мест в учреждении расходы на «стороннюю» ИТ-инфраструктуру сравнимы с месячной зарплатой «приходящего» системного администратора. Но при этом нет значительных первоначальных затрат на приобретение техники и системного и специального программного обеспечения. То есть можно начинать работу «сейчас», не дожидаясь «светлого будущего», когда будут найдены средства на приобретение собственного аппаратного и программного обеспечения.

Н.К.: Как известно, стоимость автоматизации лечебно-диагностического процесса не входит в тариф, у ЛПУ нет специальных бюджетов на разработку и внедрение МИС. Видите ли Вы какой-либо реальный алгоритм решения этой проблемы?



З.Р.: Информатизация должна стать такой же неотъемлемой частью инфраструктуры поддержки деятельности медицинского учреждения, как, например, водопровод, канализация, вентиляция, энергообеспечение и т.п. В бюджете медучреждения должны быть предусмотрены соответствующие статьи расходов.

Ситуация не изменится до тех пор, пока информатизация будет рассматриваться как что-то «дополнительное», «непрофильное» и т.п.

В текущей ситуации один из вариантов решения — это создание дата-центров, в которых будут функционировать базы данных и соответствующие приложения МИС. Эти дата-центры на сегодняшний день обслуживаются специализированными компаниями на условиях аутсорсинга, а учреждения оплачивают доступ к этим дата-центрам, то есть «услуги связи», которые должны быть в «тарифе». Непосредственно на рабочих местах, где устанавливается свободно распространяемое ПО, достаточно Интернет-браузера. Этими дата-центрами для решения поставленных задач могут и должны выступать МИАЦ при условии соответствующего их оснащения, оплаты труда специалистов МИАЦ не на уровне, существующем для них в настоящее время, а соответствующем мировым стандартам. Для этого Минздрав-



соцразвития в срочном порядке необходимо разработать нормативно-правовую платформу деятельности МИАЦ.

Кроме того, в презентации О.В. Симакова от 7 октября 2009 г. прозвучала позиция, противоположная представленной в презентации от 2 декабря 2008 г. В 2008 г. региональные медицинские информационные ресурсы должны были аккумулироваться в МИАЦ, в 2009 г. — в ТФОМС. Непонятно, почему произошла такая переориентация. В презентации 2009 года упоминаний о МИАЦ нет вообще. При распределении ролей ТФОМС и МИАЦ необходимо учитывать тот факт, что по существующему законодательству сбор, обработка и представление учетно-отчетной информации по государственной медицинской статистике осуществляются только организациями органов управления здравоохранением. Электронные истории болезней и амбулаторные карты, по версии 2009 года, также должны по сетям общего пользования передаваться в ТФОМС и поддерживаться там же, что не является функциями ТФОМС, ограничивающимися финансированием медицинских услуг населению и вынесением штрафов. Передача всех этих функций ТФОМС потребует полного пересмотра существующего законодательства, а органы управления здравоохранением практически превратятся в придаток ФОМС.

Надо рассмотреть и «капитальные затраты»: на приобретение компьютеров или терминальных устройств рабочих мест, подключение к каналам связи и их сертификацию по защите информации. Эти затраты так же, как и затраты на обслуживание баз данных в дата-центрах, могут быть отнесены на централизованные федеральные, региональные или муниципальные программы, то есть не за счет медучреждений, а за счет органов управления здравоохранением.

Непосредственно медучреждения будут оплачивать «услуги связи» и арендную (абонентскую) плату за подключение.

В том виде, как это происходит сегодня, информатизация — это действительно «непрофильная» функция.

В большинстве медучреждений уже внедрен и продолжает увеличиваться «зоопарк» из нескольких, а то и более десятка разноплановых программно-аппаратных средств, практически никак не взаимодействующих друг с другом и решающих задачи в основном для вышестоящих или сторонних организаций (учет услуг, медицинская статистика, специальные регистры, например, «раковый», «сахарный диабет», «туберкулез» и т.п.).

Каждое из таких средств имеет, как правило, автономную базу данных, требует ввода персонифицированных данных, соответственно отдельного обслуживания, сертифицирования и т.п., а это многократно увеличивает расходы и усложняет работу персонала медучреждения, так как требует дополнительной работы по вводу данных, но почти ничего не давая взамен самому медицинскому учреждению.

Если есть электронная история болезни (медицинская карта), значит, любые отчеты, реестры, регистры, учетные формы и т.п. могут быть получены автоматически. Персонал медучреждений освобождается от «непрофильных» функций, а занимается непосредственно лечебно-диагностическим процессом, ведет «историю болезни» (медицинскую карту) и использует возможности информатизации в своих интересах, не отвлекаясь на нужды сторонних и вышестоящих организаций.

Вышестоящие организации получают возможность, подключившись к той же инфраструктуре, получать любые отчеты в реальном времени, причем исключая манипулирование данными на уровне медучреждения.





Таким образом, идеологически правильные положения в докладе О.В. Симакова требуют более детальной проработки и осознания существующих возможностей здравоохранения для их реального воплощения.

А.Г.: В Вашем выступлении на конференции «Информационные технологии в медицине-2009» Вы представили интересный и очень сложный проект, который реализуете совместно со специализированной компанией-разработчиком медицинских информационных систем. Судя по настрою, Вы оцениваете этот проект как успешный опыт частно-государственного партнерства. Какие наиболее важные требования, на Ваш взгляд, должна соблюдать компания-разработчик МИС, чтобы такого опыта было больше? Что, на Ваш взгляд, самое сложное в такого рода партнерстве?



З.Р.: Самое сложное — это с, одной стороны, соблюсти баланс интересов медучреждений (как пользователей), разработчиков и организаторов здравоохранения, с другой стороны, обеспечить эффективное взаимодействие между участниками процесса.

Соответственно компания-разработчик должна предлагать решения, удовлетворяющие требования стандартов и текущего законодательства, а также «привлекательные» для всех участников. То есть решение должно предоставлять возможности, востребованные и полезные непосредственным пользователям (среднему медперсоналу, врачам, статистикам, руководителям медучреждений), а также сторонним и руководящим организациям, а не только одной из сторон.

Типовой пример: программа формирования статистической отчетности: статистик в медучреждении открывает «пустую» статистическую форму, «вручную» перебирает медкарты и вводит в открытую форму подсчитанные цифры, далее начинается «автоматизация»: контроль введенных значений, объединение отчетных форм и т.п. Все это важно для вышестоящей организации, ответственной за формирование отчетности, но практически не используется в данном медицинском учреждении.

А.Г.: Вы приняли участие к небольшой дискуссии по вопросу оправданности применения специализированных телемедицинских комплексов. Действительно, в последнее время появилась тенденция отказа от такого рода решений в пользу массовых средств видео- и аудиокоммуникаций наподобие Skype и т.д. Хотелось бы поподробнее узнать Ваше мнение по этой перспективе.



З.Р.: Если сравнивать ВКС и Skype, увидим следующее.

На данное время максимальное разрешение Skype с web-камерами 640x480, для кодеков ВКС — от 4CIF до 1080p.

Для более высокого разрешения для Skype необходимы дорогостоящая камера и дополнительное устройство оцифровки видео и звука.

В Skype более сложное управление и настройка, чем у кодеков ВКС. В Skype нет ряда возможностей, которые предоставляют кодеки ВКС, например, управление камерой по звуку, удаленное управление камерой. Бесплатный Skype не поддерживает «многоточку».



Единственным центральным элементом для Skype является сервер идентификации, который находится в Америке, на котором хранятся учетные записи пользователей и резервные копии их списков контактов. При установке соединения между ПК данные шифруются и ключи для расшифровки данных рассылаются с центрального сервера Skype. Говорить о безопасности при такой схеме нельзя.

Для соединения по Skype обязательно наличие выхода в Internet. Кодяки ВКС могут работать только в локальной сети.

В Skype при использовании высокого разрешения частота кадров падает до 2–5 кадров/сек. У кодеков ВКС частота кадров сохраняется не ниже 25 кадров/сек.

Аппаратный кодек ВКС по быстродействию превосходит Skype. Так как Skype программный продукт, для полноценной работы необходим недешевый компьютер с частотой от 1 ГГц.

Если сравнивать ВКС с Вебинар, можно воспользоваться отзывами об этой технологии в Интернете. Специалисты по обучению и развитию воспринимают этот формат по-разному. Александр Степанов, начальник обучения и развития персонала Ростелеком: «Если говорить об обучении, то видеоконференц-связь подходит для семинарских занятий больше. Для тренинга необходима обратная связь от участников и групповая динамика, которая в данном формате отсутствует. К тому же, если в группе больше 15 человек, то на отслеживание результата обучения с использованием Вебинар уйдет очень много времени. В Ростелекоме видеоконференц-связь используется для проведения информационных мероприятий, семинаров и совещаний. Главное — составить удобное расписание, ведь наша страна расположена в 5 часовых поясах».

Г-н Р. Стоц часто выступает спикером веб-конференций, записи которых в последствии размещаются на портале www.Workforce.com. Согласно Роджеру Стоцу, если участников больше 20 человек, то лучше использовать односторонний формат взаимодействия. Если же Вас слушают меньше 20 человек, то взаимодействие с аудиторией может проходить в форме дискуссии. На Западе Вебинары и веб-конференции используются компаниями-провайдерами в качестве маркетингового инструмента, а вот внутренние специалисты компаний часто прибегают к онлайн-мероприятиям как к инструментам обучения и коммуникации.

На рынке веб-конференций в мире работают несколько известных провайдеров данной услуги. Один из лидеров отрасли — компания WebEx, в начале марта 2007 года приобретенная Cisco за 3,2 млрд. \$. Более бюджетным вариантом могут быть услуги компании Interwise. Также в секторе веб-конференций работает компания Adobe со своим продуктом Acrobat Connect. Алексей Корольков, генеральный директор компании Websoft, в своем блоге рассказывает о бесплатном сервисе по проведению мероприятий vRoom от Illuminate. Правда, бесплатная версия vRoom имеет ограничения: вместе с «тьютором» число участников сессии не должно превышать трех человек.

По мнению Михаила Пеньковского, Вебинар — это скорее маркетинговый инструмент компании, нежели инструмент обучения.

Так что выбор остается за пользователем в зависимости от поставленных им задач. Во всяком случае, я вижу преимущества специализированных телемедицинских комплексов для телемедицинских задач, но проблемой их использования является консерватизм врачей, с большим трудом переходящих на новые инновационные технологии, а также неразвитость правового поля, регламентирующего деятельность этих комплексов.





А.Г.: Что, на Ваш взгляд, нужно предпринять в первую очередь на федеральном уровне для развития ИКТ в медицине?



З.Р.: Что касается перечня эффектов от комплексной информатизации здравоохранения, приведенных в докладе директора Департамента информатизации О.В. Симакова, то он критике не подлежит. Изложены идеи, которые много лет приводятся в различных докладах, статьях и выступлениях специалистов по этой тематике, в ранее принятых концепциях информатизации здравоохранения, создания государственной системы мониторинга здоровья населения России.

Но, если внимательно ознакомиться с докладами директора Департамента информатизации О.В. Симакова «О мерах по созданию информационной системы здравоохранения в части персонифицированного учета оказания медицинской помощи гражданам Российской Федерации» от 2 декабря 2008 г. и «Основные задачи развития ИКТ в здравоохранении Российской Федерации» от 7 октября 2009 г., то обнаружится ряд неточностей и противоречий, которые свидетельствуют об отсутствии в Минздравсоцразвития единой, долговременной, продуманной концепции развития комплексной информатизации здравоохранения.

Опыт прошедших лет показал, что попытки решить такую большую задачу с привлечением коммерческих организаций существенных результатов не дали. Коммерческие организации банкротятся, реорганизуются и в общем счете ни за что не отвечают. Из доклада директора Департамента информатизации О.В. Симакова следует, что в течение трех лет будет создана и внедрена единая для России электронная карта пациента. Известно, что в связи с этим происходит большое финансирование коммерческих организаций, начиная с мероприятий ФЦП «Электронная Россия». До сих пор остается открытым вопрос о разработке и утверждении очередной концепции информатизации здравоохранения, версия которой была разработана в рамках той же ФЦП «Электронная Россия». И хотя концепция не утверждена, начато и продолжается финансирование указанных работ, что противоречит последовательности действий, приведенных в докладе.

Данная проблема решается традиционно «в лоб», то есть предпринимаются попытки «с нуля» разрабатывать за государственный счет некие типовые решения, единые системы и т.п. Таким способом задача не может быть решена. Уже потрачено и будет потрачено еще большее количество государственных средств, но удовлетворительного, устраивающего всех решения не будет. Будет создано некое ядро системы, которое при условии бесплатной передачи в ЛПУ потребует значительного вложения средств тем же ЛПУ для внедрения, адаптации и доработки «типового» программного обеспечения, или медицинской информационной системы (МИС) под реалии этого ЛПУ.

Единственный способ получить действительно работающую систему персонифицированного учета — это заняться на федеральном уровне разработкой стандартов обмена информацией, перечней требований к медицинским информационным системам, при соблюдении которых любая удовлетворяющая эти требования МИС может быть использована в качестве «типовой», внедрить единый идентификатор пациента, развивать ИТ-инфраструктуру, обеспечить, в том числе законодательно, условия финансирования на уровне медучреждений и т.п. Другими словами, сформулировать «правила игры», а не заниматься разработкой, стимулировать развитие рынка, а не выходить на этот рынок в качестве «большого игрока»...



Таким образом, разрозненные, сегодня почти не взаимодействующие друг с другом МИС, уже имеющиеся на рынке и востребованные конечным пользователем, автоматически объединятся в единую систему.

Более того, значительное количество разных МИС, подключаемых к системе, обеспечат конкурентную среду, постоянно стимулирующую разработчиков к дальнейшему совершенствованию своей продукции, а у конечного пользователя всегда будет возможность выбора, а не использования «навязанного сверху» продукта, который далеко не всегда учитывает специфику работы конкретного учреждения.

А.Г.: В последнее время во всех секторах ИТ-экономики, в медицинских информационных системах в том числе, усиливаются призывы к более масштабному применению открытого программного обеспечения. При этом данное направление уже начало раздваиваться — речь ведь идет уже не только о применении системы Linux или СУБД с открытым исходным кодом, но и о том, что утилитарные разработки в виде медицинских информационных систем также должны быть бесплатными для ЛПУ, а получение прибыли разработчиками и системными интеграторами предлагается осуществлять в сфере услуг по внедрению и техническому сопровождению, а не в виде оплаты лицензий за программное обеспечение. Как Вы относитесь к этим мыслям?



З.Р.: Открытое, свободно распространяемое программное обеспечение — это возможность минимизировать первоначальные затраты на внедрение. В условиях ограниченного финансирования это очень существенное преимущество. Услуги по внедрению и техническому сопровождению — это тоже дополнительная работа, особенно на начальном этапе внедрения, которая требует существенных затрат от разработчика (поставщика), а не только возможность «получения прибыли».

Соответственно, если программное обеспечение передается бесплатно, то это можно рассматривать как своеобразный лизинг. Кроме того, есть еще значительные затраты на создание самого продукта, которые тоже надо учитывать. Поэтому оплата за лицензии или за текущее обслуживание — это скорее «форма», чем «содержание». Затраты на разработку могут покрываться за счет продажи лицензий, а могут быть включены в стоимость услуг по внедрению и сопровождению. В зависимости от ситуации вполне могут быть использованы оба варианта.

Наиболее перспективным видится вариант оплаты за обслуживание, так как снижает необходимость отслеживания количества подключаемых рабочих мест (лицензий). Но следует иметь в виду, что оплата лицензий — это возможность разработчика (поставщика) получить значительные средства сразу, а текущее обслуживание — со значительной рассрочкой, соответственно стоимость текущего обслуживания будет включать еще и некий «кредитный» или «инфляционный» процент.





КАК ОРГАНИЗОВАТЬ АВТОМАТИЗИРОВАННУЮ ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКИХ УЧРЕЖДЕНИЯХ

Издательский дом «Менеджер здравоохранения»
подготовил к печати новую книгу серии
«МЕНЕДЖМЕНТ В ЗДРАВООХРАНЕНИИ»



Автоматизированная обработка персональных данных в медицинских учреждениях. Столбов А.П., Кузнецов П.П. — ИД «Менеджер здравоохранения», 2010. — 210 с.

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. Приведены примеры соответствующих организационно-распорядительных и иных документов.



Книга представляет практический интерес для руководителей ЛПУ, а также других учреждений здравоохранения и системы ОМС, и призвана оказать методическую помощь при организации автоматизированной обработки медицинской информации в соответствии с требованиями закона «О персональных данных».

С содержанием книги и условиями приобретения можно ознакомиться
на сайте издательства: www.idmz.ru



ЗАКОН «О ПЕРСОНАЛЬНЫХ ДАННЫХ»: ТИПОВЫЕ УГРОЗЫ ДЛЯ ЛПУ 2010 ГОДА

39-е заседание, 3 декабря 2009 г., Президиум РАМН, Москва
Заседание было посвящено рассмотрению вопросов, связанных с порядком приведения в соответствие с положениями закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ действующих и вновь разрабатываемых медицинских систем, и мерах, предпринимаемых в связи с этим Минздравсоцразвития России.



Первые ответы на эти вопросы были даны в докладе **Рылова Сергея Павловича**, заместителя начальника отдела развития информационно-коммуникационной технологической инфраструктуры системы здравоохранения, социального развития и трудовых отношений Минздравсоцразвития России. Он сформулировал основные требования к корпоративным медицинским информационным системам по обеспечению защиты и конфиден-

циальности персональных данных в учреждениях и организациях здравоохранения.

Докладчик напомнил, что, согласно Постановлению Правительства Российской Федерации от 17 ноября 2007 г. № 781, информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее — оператор), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным инте-

ресам личности, общества и государства.

Согласно Порядку проведения классификации информационных систем персональных данных, утвержденному приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных, должны быть отнесены *к специальным информационным системам*.

По результатам анализа исходных данных, *класс специальной информационной системы* определяется на основе модели угроз безопасности персональных дан-

Информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных, должны быть отнесены к специальным информационным системам.





Класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных.

ных в соответствии с методическими документами, разрабатываемыми в соответствии с пунктом 2 Постановления 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».

При создании типовой модели угроз учитывается, что «МИС является специальной информационной системой, так как в ней обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;

- в МИС одновременно обрабатываются данные от 1000 до 10 0000 субъектов персональных данных;

- в МИС не предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных (юридически значимым документом является «бумажная» история болезни, по которой принимаются решения).

В модели угроз должны рассматриваться 2 типа нарушителей:

- внешние нарушители — физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование МИС;

- внутренние нарушители — физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование МИС.

Для МИС ЛПУ основную угрозу представляют внутренние нарушители.

При разработке требований к корпоративным медицинским информационным системам по обеспечению защиты и конфиденциальности персональных данных в учреждениях и организациях здравоохранения исходили из того, что для МИС ЛПУ основную угрозу представляют внутренние нарушители. В разработанной модели угроз рассматриваются 8 типов нарушителей:

- администраторы МИС (категория I);

- администраторы конкретных подсистем или баз данных МИС (категория II);

- пользователи МИС (категория III);

- пользователи, являющиеся внешними по отношению к конкретной АС (категория IV);

- лица, обладающие возможностью доступа к системе передачи данных (категория V);

- сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы МИС, но не имеющие права доступа к ресурсам (категория VI);

- обслуживающий персонал ЛПУ (охрана, работники инженерно-технических служб и т.д.) (категория VII);

- уполномоченный персонал разработчиков МИС, который на договорной основе имеет право на техничес-

кое обслуживание и модификацию компонентов МИС (категория VIII).

Считается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей. Наибольшую опасность представляют лица категорий III–VIII при допущении, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролируемых мер.

Учитывая особенности функционирования, небольшое количество актуальных угроз и незначительность опасности их реализации, МИС определяется как специальная информационная система персональ-



МИС определяется как специальная информационная система персональных данных с требованиями по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в основном соответствующими 3-му классу.

ных данных с требованиями по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, в основном соответствующими 3-му классу.

Такой взгляд на построение угроз для типовых МИС типовых ЛПУ утвержден надзорными органами и согласован с ФСТЭК.



По оценкам директора Департамента информатизации Минздравсоцразвития России **О.А. Симакова**, на перевод медицинских систем в соответствие с требованиями 152-ФЗ потребуется не менее 15 млрд. рублей.

По словам О.Симакова, достигнута договоренность с ФОМС о делегировании ТФОМС прав на сбор, обработку и передачу персональных данных на региональном и федеральном уровнях. ФОМС и ТФОМС прошли соответствующие процедуры

На перевод медицинских систем в соответствие с требованиями 152-ФЗ требуется не менее 15 млрд. рублей.

лицензирования и обладают необходимым сертифицированным программным обеспечением. Нормативное закрепление указанной процедуры предусмотрено при принятии закона «Об обязательном медицинском страховании».

До указанного момента в соответствии с требованиями закона 152-ФЗ необходимо получать у пациентов согласие на обработку персонифицированных данных согласно со статьей 9.4.

Также ЛПУ необходимо привести в соответствие с положениями закона используемые ими бухгалтерские, кадровые информационные системы и системы электронного документооборота, ко-

торые не являются специальными. Крупнейшие разработчики указанных систем уже сертифицировали дополнительные модули и планируют установить их в процессе плановых обновлений.

Отвечая на вопрос, планируется ли создание инфраструктуры (центров компетенций), которая будет помогать в решении вопросов, возникающих в ЛПУ, или каждое ЛПУ будет решать эти проблемы в одиночку, не имея квалифицированных специалистов, которые могли бы справиться с этими вопросами,

директор Департамента информатизации О.Симаков ответил: «Мы всячески стараемся облегчить финансовую нагрузку, которая возникнет у ЛПУ в связи с 152-ФЗ, но сегодня нет ни одной МИС, полностью удовлетворяющей требованиям этого закона. Все финансовые затраты на это мероприятие ложатся на организацию. Ни средств, ни полномочий для создания новых специализи-

Сегодня нет ни одной МИС, полностью удовлетворяющей требованиям этого закона.





Все финансовые затраты на это мероприятие ложатся на организацию.

рующихся на обеспечении соответствия 152-ФЗ организаций нет.

«Сегодня мы имеем методуказания, согласованные с ФСТЭК, которые будут проведены приказом МЗ СР РФ». Все территориальные фонды ОМС прошли сертификацию. Мы не хотим оставлять ЛПУ наедине с такими органами, как Россвязнадзор и др. Вся работа будет выполняться на базе фондов».

В течение полугода будет работать горячая линия, оказывающая консультационную поддержку ЛПУ при подготовке комплекта документов.

По мнению О. Симакова, сложность надвигающейся на ЛПУ проблемы сильно преувеличена. В этом смысле корректна аналогия с проблемой 2000 года, которая была абсолютно надуманной и существовала только для

систем стратегического ракетного нападения, ориентированных на физическое время.

«Мы полагаем, что методуказания и участие ТФОМС закроют в течение года все проблемы ЛПУ, связанные с

«Мы полагаем, что методуказания и участие ТФОМС закроют в течение года все проблемы ЛПУ, связанные с защитой персональных данных».

защитой персональных данных. Никакого рецепта для МИС, кроме сертификации, нет. Перед ЛПУ стоит дилемма: либо дорабатывать свои МИС до типовых требований, либо тратить деньги на новую систему», — полагает О. Симаков.

Директор Департамента также высказал точку зрения о целесообразности в большинстве случаев использования аутсорсинга для установ-

ки и обслуживания информационных систем медицинского учреждения. В качестве ключевых узлов аутсорсинга в регионах и муниципальных образованиях он предлагает использовать структуру медицинских информационно-аналитических центров (МИАЦ). В самом же ЛПУ целесообразно создать должность заме-

стителя директора по медицинскому оборудованию и информационным технологиям с минимальным штатом. Такая конфигурация позволит концентрироваться на основных функциях по оказанию медицинской помощи в условиях бесперебойной работы оборудования и систем его обслуживания.

Н. Куракова

Работа над ошибками

В статье А.В. Гусева «Обзор рынка комплексных медицинских информационных систем», опубликованной в журнале «ВиИТ» (2009, № 6, стр. 4–17), приведены неверные сведения о компании «АКСИМЕД», являющейся разработчиком и поставщиком медицинской информационной системы «АМУЛЕТ». Неправильно указано название компании (в таблице 1 на стр. 5 и рисунке 2 на стр. 13); приведен неверный адрес сайта компании (<http://www.amulet-med.ru> вместо <http://www.aksimed.ru> в таблице 1 на стр. 5); в тексте на стр. 11 МИС ошибочно названа «Аксимед».

Редакция приносит извинения компании в лице ее руководства и сотрудников.



ИНФОРМАЦИОННЫЕ СИСТЕМЫ В ЗДРАВООХРАНЕНИИ: НОВЫЕ ВИДЕНИЕ, ФУНКЦИИ И ТРЕБОВАНИЯ

40-е заседание, 17 декабря 2009 г., Президиум РАМН, Москва
Заседание было посвящено рассмотрению требований к типовым МИС с точки зрения создаваемой концепции информатизации здравоохранения.



Директор Департамента информатизации Минсоцразвития РФ **Симаков Олег Владимирович** в своем докладе «Цели и направление создания информационной системы в здравоохранении» выделил главную цель информатизации — повышение доступности и качества оказываемой медицинской помощи и эффективное использование ресурсов отрасли.

Он подчеркнул, что для эффективного использования ресурсов нужны фактические, а не планируемые расходы на пациента. «Российское здравоохранение движется к

внедрению диагностически-ориентированных групп (ДОГ). Уже сегодня создано около 120 стандартов (по сравнению с 600 стандартами в системах здравоохранения других стран), которые либо связаны с нозологиями, либо работают в интересах создания будущих ДОГ».

На уровне субъектов РФ, по мнению О. Симакова, должен быть сделан акцент на информированности населения о возможности получения той или иной медицинской помощи и квалификации лечащего врача. «На сайте госуслуг мы предлагаем информацию по оказанию высокотехнологической медицинской помощи. Есть открытый доступ для всех и закрытый доступ к порталу для тех, кто уже получил квоты. Со второго квартала 2010 г., граждане будут получать информацию о лечащих врачах из регистра медперсонала: какой медВУЗ окончил, когда и какое повышение квалификации прошел. Таким образом у гражданина появится возможность

составить впечатление о квалификации врача. Система отработана на Ивановской области. За первый квартал этот регистр будет заполнен с помощью региональных МИАЦ. При этом предполагается не ручной, а автоматизированный ввод информации. Эта работа федерального уровня. Все остальные виды информации должны предоставляться на уровне региона».

Комментируя архитектурный подход к созданию системы, О. Симаков отметил, что «на федеральный уровень будут подниматься только аналитические данные. При этом персональные данные отделяются от медицинских. Сливаться эти два массива будут только на месте оказания медпомощи. В следующем году мы будем делать модель врачебной тайны, чтобы в момент оказания медицинской помощи мы получали информированное согласие пациента и соблюдали его право на защиту персональных данных».

Каждый главный врач может проконсультироваться



со своими разработчиками и выбрать наиболее подходящую типовую МИС для стыковки. Сегодняшняя статистика говорит о том, что лишь у 18% ЛПУ уже есть МИС, а у 80% их либо нет, либо персональные компьютеры не связаны в сети и не используются в медицинских целях, поэтому остается широкое поле деятельности и для типовых решений, и для вендоров для продажи МИС лечебным учреждениям. По словам О. Симакова, предложение ввести МИС в депозитарий МЗ СР РФ в качестве типовой системы сделано уже четырем разработчикам, их МИС уже состыковываются. Трудоемкость стыковки составляет 1 человекомесяц. «Разработано интерфейсное решение для стыковки по двум важнейшим показателям: законченный случай стационара и посещения поликлиники. Стык этих четырех систем означает, что макет, позволяющий с относительно низкой трудоемкостью осуществлять интегрирование МИС, уже разработан».

Комиссия по инновациям при Президенте РФ одобрила инициативы МЗ СР РФ по созданию электронной медицинской библиотеки и разработке экспертных систем мониторинга индивидуального состояния граждан, попадающих в рискованные зоны. «Сейчас пишется карта про-

екта, уточняется объем выделенных средств, анализируется опыт Израиля и Германии в части индивидуального мониторинга групп риска по сердечно-сосудистым заболеваниям, диабету и т.д.».

«Когда речь идет о линейных ЛПУ, мне хочется перейти на промышленную индустриальную платформу как магистральную линию развития потому, что промышленный поход — подход универсальный.»

«В 2010 году наши усилия будут сосредоточены на создании системы, а не на решении частных задач. Будем переходить к поэтапному внедрению электронной медицинской карты в формате сочетания электронного и бумажного документооборота. Логика заключается в том, чтобы не отдельное учреждение переводить на электронный документооборот, а весь субъект».

На вопрос президента АРМИТ Михаила Эльянова, как один МИАЦ, например, Москвы или Московской области, может обслужить

несколько сотен ЛПУ, О.В. Симаков ответил: «Такой, например, как в Челябинской области, где один МИАЦ решает сервисные проблемы 370 медицинских учреждений региона».

В заключение директор Департамента информатизации заметил: «Когда речь идет о линейных ЛПУ, мне хочется перейти на промышленную индустриальную платформу как магистральную линию развития потому, что промышленный поход — подход универсальный. Либо на конкурсной аутсорсинговой основе, либо по госзаданию нужно обеспечить сервисную поддержку ЛПУ. А 1,5 ИТ-специалиста в ЛПУ эту проблему не решат. По стоимости владения (не прямые затраты) аутсорсинг дешевле, чем штатный специалист».

Либо на конкурсной аутсорсинговой основе, либо по госзаданию нужно обеспечить сервисную поддержку ЛПУ. А 1,5 ИТ-специалиста в ЛПУ эту проблему не решат.



Александр Константинович Тарасов, начальник отдела развития информационно-коммуникационной технологической инфраструктуры системы здравоохранения, социального развития и трудовых отношений Департамента информатизации здравоохранения МЗ СР РФ, уточнил требования к МИС, разделив их на три группы: функциональные требования, требования по обмену данными, требования по использованию справочно-нормативных документов.

При работе с данными персонифицированного учета медицинской помощи МИС должна реализовывать следующий **набор функций**:

- аутентификацию и авторизацию прав доступа сотрудников МО при входе в МИС;
- регистрацию факта оказания медицинской помощи пациенту, включая операции, лечебные и диагностические манипуляции;

- хранение и возможность передачи сведений в сводный реестр персонифицированного учета сведений об оказанной медицинской помощи;

- формирование и передачу в СМО счета на оплату лечения и получение из СМО сведения об оплате или отказе оплаты. Для проведения медицинской экспертизы формирование и передачу в ответ на запрос персонально идентифицируемых сведений о медицинской помощи, оказанной пациенту;

- формирование официальных форм учетно-отчетной медицинской документации и передачу этих форм органам управления здравоохранением;

- формирование любых бланков медицинской документации.

Требования по подсистеме **обмена данными** МИС:

- Импорт/Экспорт персонифицированных данных, медицинских карт пациентов, реестров услуг, счетов, НСИ.

- При реализации требуется обеспечить единый клиентский интерфейс для автоматизации всех процессов, связанных с обслуживанием пациентов и планированием деятельности медицинского учреждения.

- Программное обеспечение должно использовать утвержденный перечень классификаторов или полное взаимодействие с ним.

- Прикладное программное обеспечение функциональных подсистем должно быть построено по модульному принципу, то есть включать в себя модули и компоненты, которые могут быть модернизированы без необходимости перепроектирования всей системы в целом.

- МИС должна строиться в расчете на единое информационное пространство здравоохранения муниципального образования, субъекта РФ, РФ с возможностью репликации и агрегирования информации на несколько уровней.

- Для обеспечения безопасной системной среды система должна включать систему безопасности, включающую надежную аутентификацию, ролевое управление доступом, безопасный обмен данными с использованием криптопреобразования (шифрования) канала связи.

- Должна быть обеспечена возможность интеграции с информационными системами управления ресурсами.

- Должна быть обеспечена интеграция с информационной системой ведения паспортов ЛПУ, регистра медицинского персонала, регистра медицинской техники.

- МИС должна иметь средства для создания интерфейсов взаимодействия с внешними информационными системами.

Подготовила Н.Куракова



От редакции:

Предлагаем ознакомиться с проектом новой редакции паспорта научной специальности 03.01.09 Математическая биология, биоинформатика (физико-математические, биологические, медицинские науки).

ПРОЕКТ

Краткий паспорт научной специальности 03.01.09 МАТЕМАТИЧЕСКАЯ БИОЛОГИЯ, БИОИНФОРМАТИКА

(физико-математические, биологические, медицинские науки)

I. Формула специальности

«Математическая биология, биоинформатика» — научная специальность, которая изучает организацию, функционирование, развитие, патологические состояния живых систем различного уровня методами и средствами математики и информатики.

Решение научных проблем данной специальности имеет как фундаментальное, так и прикладное значение.

II. Области исследования

1. Математическое и компьютерное моделирование живых систем: субклеточных структур, клеток, тканей, органов, систем органов, организмов, популяций, биоценозов.

2. Математическое и компьютерное моделирование эволюционных процессов в живой природе.

3. Компьютерная геномика, протеомика, иммуномика.

4. Математическое и компьютерное моделирование экологических систем.

5. Математическое и компьютерное моделирование биологического действия ксенобиотиков. Компьютерная фармакология. Компьютерная токсикология.

6. Компьютерное распознавание и синтез изображений в биологических и медицинских исследованиях.

7. Разработка новых вычислительных технологий на основе результатов исследова-

ний живых систем; развитие бионических подходов.

8. Математические модели, численные методы и программные средства применительно к процессам получения, накопления, обработки и систематизации биологических и медицинских данных и знаний.

9. Организация, ведение и использование автоматизированных банков данных по биологии и медицине, в том числе банков междисциплинарных данных.

10. Интеллектуальные системы анализа и прогнозирования свойств биологических объектов на основе специализированных баз и банков данных и знаний (в том числе полнотекстовых).

11. Математическое и компьютерное моделирование распространенности и структуры заболеваний.

12. Решение задач медицинской диагностики, прогнозирования исходов заболеваний, оценки эффективности медицинских вмешательств и технологий с помощью математического аппарата и вычислительных алгоритмов.

13. Системы информационного обеспечения и поддержки биологических и медицинских исследований, включая анализ точек роста и тенденций развития научных направлений.

Примечания

— Специальность не включает системы управления здравоохранением, в том числе их моделирование (см. 14.02.03 — Общественное здоровье и здравоохранение)



См. также специальности:

- 01.02.08 — Биомеханика (пункт 7)
- 03.01.00 — Биофизика (пункты 1)
- 03.01.02 — Молекулярная биология (пункты 1, 3, 5)
- 03.01.04 — Биохимия (пункты 1, 5)
- 03.01.07 — Молекулярная генетика (п. 3)
- 03.00.08 — Экология (пункты 1, 4)
- 03.00.14 — Биологические ресурсы (пункты 1, 4)
- 03.03.01 — Физиология (пункты 1)
- 03.03.03 — Иммунология (пункты 1, 3)
- 03.03.04 — Клеточная биология, цитология, гистология (пункты 1, 6)
- 03.03.05 — Биология развития, эмбриология (пункты 1, 3, 6)
- 03.03.06 — Нейробиология (пункты 1, 6)
- 05.13.18 — Математическое моделирование, численные методы и комплексы программ (пункты 1–5, 8, 11)
- 05.25.05 — Информационные системы и процессы (пункты 9, 11, 13)
- 05.26.06 — Химическая, биологическая и бактериологическая безопасность (пункт 5)
- 14.03.03 — Патологическая физиология (пункты 1, 6)
- 14.03.04 — Токсикология (пункт 5)
- 14.03.06 — Фармакология, клиническая фармакология (пункт 5)
- 14.03.10 — Клиническая лабораторная диагностика (пункт 6)
- 14.04.02 — Фармацевтическая химия, фармакогнозия (пункт 5)

III. Отрасли наук, по которым присуждаются ученые степени

- Физико-математические — за исследования по всем пунктам;
- Биологические — за исследования по пунктам 1–10, 13;
- Медицинские — за исследования по всем пунктам.



14-16 апреля 2010 г.

Выставка и конференция
«Медицинские
информационные технологии»

6-й Международный форум MedSoft-2010

Москва, Центральный дом предпринимателя

ОРГАНИЗАТОРЫ:

- Ассоциация Развития Медицинских Информационных Технологий (АРМИТ)
- Центральный Дом Предпринимателя

ТЕМАТИКА ВЫСТАВКИ И КОНФЕРЕНЦИИ:

- Компьютерные системы для исследований и диагностики (функциональная и лучевая диагностика, лабораторные исследования и др.)
- Системы компьютеризации массовых обследований и профилактики
- Компьютерные системы в фармации
- Компьютерные системы в стоматологии
- Системы управления деятельностью медицинских учреждений и органов управления здравоохранением. Региональные системы
- Компьютерные системы медицинского страхования
- Телемедицинские системы
- Медицинский Интернет
- Обучающие системы. Электронные атласы. Мультимедийные средства
- Интеллектуальные медицинские системы
- Электронные истории болезни и амбулаторные карты
- Системы для научных исследований
- Системы обработки изображений и многое другое

Генеральный спонсор Титульный спонсор




Спонсоры




**ВХОД НА ВЫСТАВКУ СВОБОДНЫЙ.
УЧАСТИЕ В МЕРОПРИЯТИЯХ ДЕЛОВОЙ
ПРОГРАММЫ БЕСПЛАТНО**

Адрес:
Центральный дом предпринимателя, ул. Покровка, 47/24
Проезд: ст. м. «Красные ворота», «Курская»
Информация по тел.: (499) 200-10-62
Программа конференции и список участников выставки
опубликованы на сайте: www.arnit.ru



АКТУАЛЬНЫЕ НОРМАТИВНЫЕ ДОКУМЕНТЫ И СТАНДАРТЫ

КАК РОСПОТРЕБНАДЗОР ПЛАНИРУЕТ УЛУЧШИТЬ ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ СВОЕЙ ДЕЯТЕЛЬНОСТИ?

Приказ Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека от 6 октября 2009 г. № 638 «О совершенствовании информационного обеспечения деятельности Роспотребнадзора»

Утвержден план мероприятий по совершенствованию информационного обеспечения деятельности Роспотребнадзора.

Так, в течение 2009–2011 гг. планируется внедрить единую систему внутриведомственного электронного документооборота, а в IV квартале 2010 г. — создать удостоверяющий центр и систему электронной цифровой подписи Роспотребнадзора.

В 2010 г. предстоит запуск системы электронной почты Роспотребнадзора. Она будет обеспечивать массовую рассылку документов в электронном виде и контроль их получения. Одновременно будут созданы прикладные информационные и справочные системы для автоматизации процессов сбора, обработки, хранения и передачи (обмена) информации между структурными подразделениями Роспотребнадзора.

На 2010–2013 гг. запланировано создание ведомственного электронного архива.

В 1 и 2 квартале 2010 г. будет усовершенствована системы ведения реестров Роспотребнадзора.

Определены структурные подразделения Роспотребнадзора, ответственные за выполнение плановых мероприятий.

В КАКИЕ СРОКИ ФЕДЕРАЛЬНЫЕ ОРГАНЫ ВЛАСТИ ДОЛЖНЫ ПЕРЕЙТИ НА ПРЕДОСТАВЛЕНИЕ ГОСУСЛУГ И ИСПОЛНЕНИЕ ГОСФУНКЦИЙ В ЭЛЕКТРОННОМ ВИДЕ?

Распоряжение Правительства РФ от 17 октября 2009 г. № 1555-р

Утвержден план перехода федеральных органов исполнительной власти на предоставление госуслуг и исполнение госфункций в электронном виде.

В план, в частности, вошли услуги в сфере постановки на налоговый учет, уплаты налогов и сборов, регистрации юрлиц и ИП, получения выписок из ЕГРЮЛ и ЕГРИП, лицензирования отдельных видов деятельности, выдачи документов, связанных с таможенным оформлением товаров. Также изменения затронут процедуры оформления и выдачи удостоверяющих личность документов, регистрации по месту жительства и месту пребывания, постановки на учет транспортных средств и др.

По каждой услуге или функции определены ответственные исполнители и сроки реализации необходимых мероприятий. Реализация плана в целом должна быть завершена до конца 2015 г.

Методическое и организационное руководство процессом перехода осуществляет Минкомсвязь России. Ответственные органы власти должны ежеквартально представлять информацию о результатах выполнения плана в Министерство по установленной им форме. Минкомсвязи России, в свою очередь, должно ежеквартально представлять в Правительство РФ доклад о ходе реализации плана.



Функции по обеспечению соответствия мероприятий, проводимых в рамках административной реформы, плану возложены на Минэкономразвития России.

Распоряжение Правительства РФ, утвердившее перечень госуслуг и (или) функций, осуществляемых с использованием информационных и телекоммуникационных технологий, утратило силу.

КАКИЕ ИЗМЕНЕНИЯ ТФОМС И РЕГИОНАЛЬНЫЕ ОТДЕЛЕНИЯ ФСС МОГУТ ВНОСИТЬ В РЕКОМЕНДУЕМУЮ ФОРМУ СОГЛАШЕНИЯ ОБ ИНФОРМАЦИОННОМ ОБМЕНЕ ДРУГ С ДРУГОМ?

Письмо Федерального фонда обязательного медицинского страхования от 29 декабря 2009 г. № 6780/91-и «О внесении дополнений в Соглашение об информационном обмене и взаимодействии между территориальным фондом ОМС и региональным отделением Фонда социального страхования»

Вопросы информационного обмена и взаимодействия между ТФОМС и региональными отделениями ФСС РФ регулируются заключаемыми между ними соглашениями и приложениями к ним в виде регламентов информационного обмена между указанными органами.

Разъяснено, что при организации взаимодействия допускается учитывать региональные особенности и вносить соответствующие дополнения в рекомендуемые формы соглашения и регламента. Однако дополнения не должны противоречить основным структурам, определяющим информационный обмен, и положениям типовой формы соглашения.

Для получения от медицинских организаций сведений о том, что случай оказания медпомощи связан с травмой на производстве, необходимо предусмотреть соответствующий показатель в формах реестров счетов по оплате медпомощи медицинских и страховых медицинских организаций, использующихся в регионах.

С 1 ЯНВАРЯ 2010 ГОДА ОРГАНЫ ЗАГС ОБЯЗАНЫ УВЕДОМЛЯТЬ ТЕРРИТОРИАЛЬНЫЕ ФОНДЫ ОМС О СМЕРТИ ГРАЖДАН

Федеральный закон от 17 декабря 2009 г. № 317-ФЗ «О внесении изменения в статью 12 Федерального закона «Об актах гражданского состояния»

В пункт 2 статьи 12 Федерального закона от 15 ноября 1997 года № 143-ФЗ «Об актах гражданского состояния» (Собрание законодательства Российской Федерации, 1997, № 47, ст. 5340; 2001, № 44, ст. 4149; 2003, № 17, ст. 1553; № 50, ст. 4855) внесено изменение: слова «и орган Фонда социального страхования Российской Федерации» заменены словами «, орган Фонда социального страхования Российской Федерации и территориальный фонд обязательного медицинского страхования».

ООО «НПП «ГАРАНТ-СЕРВИС»
Тел.: 8 800 200 8888 (бесплатный
междугородный звонок),
8 495 647 6238 (для Москвы)
Интернет: www.garant.ru



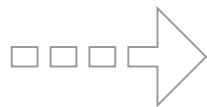
ИНФОРМАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ

*Полные тексты документов доступны на сайтах компании «Гарант»
и Издательского дома «Менеджер здравоохранения»: www.idmz.ru*

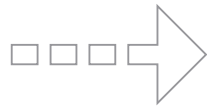




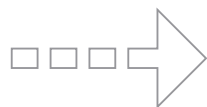
С 1 ЯНВАРЯ 2010 ВВЕДЕНЬ:



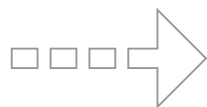
• **ГОСТ Р ИСО/МЭК 18045-2008** Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий//Information technology. Security techniques. Methodology for IT security evaluation//Код ОКС 35.040//Количество страниц — 234.



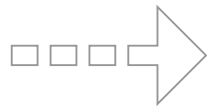
• **ГОСТ Р 53115-2008** Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства//Information protection. Conformance testing of technical information processing facilities to unauthorized access protection requirements. Methods and techniques//Код ОКС 35.040//Количество страниц — 31.



• **ГОСТ Р 53114-2008** Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения//Protection of information. Information security provision in organizations. Basic terms and definitions//Код ОКС 35.020//Количество страниц — 12.



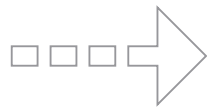
• **ГОСТ Р 53113.1-2008** Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения//Information technology. Protection of information technology and automated systems against security threats posed by use of covert channels. Part 1. General principles//Код ОКС 35.040//Количество страниц — 12.



• **ГОСТ Р 53112-2008** Защита информации. Комплексы для измерений параметров побочных электромагнитных излучений и наводок. Технические требования и методы испытаний//Information protection. Facilities for measuring side electromagnetic radiation and pickup parameters. Technical requirements and test methods//Код ОКС 35.040//Количество страниц — 24.



• **ГОСТ Р 53079.4-2008** Технологии лабораторные клинические. Обеспечение качества клинических лабораторных исследований. Часть 4. Правила ведения преаналитического этапа//Medical laboratory technologies. Quality assurance of clinical laboratory tests. Part 4. Rules for conducting of preanalytical stage//Код ОКС 11.020 //Количество страниц — 69.



• **ГОСТ Р 53092-2008** Системы менеджмента качества. Рекомендации по улучшению процессов в учреждениях здравоохранения//Quality management systems. Guidelines for process improvements in health service organizations//Код ОКС 03.120.10; 11.020//Количество страниц — 82.



WWW.BLOG.MINZDRAVSOC.RU ОТКРЫТ ОФИЦИАЛЬНЫЙ БЛОГ МИНЗДРАВСОЦРАЗВИТИЯ

«Открытие официального блога — неотложное требование времени, вызванное инновациями в информационно-коммуникационной сфере в целом и Интернет-технологиях в частности. Наша задача соответствовать этим изменениям», — сказала Татьяна Голикова.

Блог будут вести руководители Министерства и главы департаментов. Каждый автор в серии сообщений (постов) будет раскрывать тот или иной аспект направления, готовящихся изменений или политики, за который непосредственно отвечает. Предполагаются так же «гостевые посты» от представителей профессионального сообщества, которые вовлечены в работу по реализации проектов в сфере здравоохранения и социального развития.

«Наше Министерство ведет большой объем работ в области развития здравоохранения и социально-трудовой сферы. Поэтому формат коллективного блога — идеально подходит, чтобы из первых уст предоставлять информацию в формате, который стал привычным для пользователей», — рассказала Министр.

Минздравсоцразвития России занимает активную позицию в работе с Интернет-сообществом: для обсуждения Концепции развития здравоохранения до 2020 года был создан сайт zdavo2020.ru, на котором представители экспертного и профессионального сообществ могли внести свои предложения, каждое из которых было рассмотрено и учтено в Концепции. В открытый доступ для обсуждения были выложены и новый перечень жизненно необходимых и важнейших лекарственных средств (ЖНВЛС) и готовящийся закон «Об обращении лекарственных средств». Все комментарии к перечню по включению и исключению препаратов были рассмотрены и на официальном сайте Министерства размещены ответы на эти предложения.

«Корпорации уже давно используют диалог со стейкхолдерами (заинтересованными сторонами) в качестве механизма эффективного управления корпоративным развитием. Для Министерства, отвечающего за социальное развитие страны, крайне необходим диалог со всеми стейкхолдерами социального развития», — сообщила в своем первом посте в коллективном блоге Министерства Татьяна Голикова.

ОТКРЫТА ЭЛЕКТРОННАЯ ВЕРСИЯ ОБЩЕСТВЕННОЙ ПРИЕМНОЙ МИНЗДРАВСОЦРАЗВИТИЯ

В январе 2010 года открыта электронная версия общественной приемной для обращения граждан в онлайн-режиме — <http://www.minzdravsoc.ru/reception>.

«Параллельный запуск официального блога Министерства и общественной приемной на сайте — логичный шаг в продолжение той открытой информационной политики, которую мы проводим», — отметила Министр. «Наша цель — создать все необходимые ресурсы, как для информирования о политике Министерства, так и для прямого общения с гражданами, экспертным и профессиональным сообществом».

Посетители коллективного блога Министерства смогут оставлять комментарии после регистрации.

Справочно:

Зачем нам нужен наш блог?

• Через традиционные СМИ (газеты, журналы, телеканалы), мы часто не имеем возможности рассказать Вам то, что хотелось бы. Просто потому, что у СМИ свой формат, и не все в него попадает.





• Также не все важное может быть заключено в официальный формат Ministerского сайта (<http://www.minzdravsoc.ru>).

• Плюс — СМИ и сайт не позволяют нам находиться с Вами в диалоге и без большой дистанции.

Собственно, блог нами запланирован как «неформат» для информации, которая не укладывается в рамки традиционных СМИ. А также для диалога между Министерством и теми, для кого Министерство работает. В конечном итоге мы надеемся на создание сообщества, совместно обсуждающего вопросы социального развития России. И даже совместно работающего на социальное развитие.

Зачем Вам нужен наш блог?

• Для получения оперативной и эксклюзивной информации по направлениям работы Министерства: социальному развитию, трудовым отношениям, пенсионному обеспечению, здравоохранению.

• Для прояснения решений или действий Министерства.

• Для понимания того, как работает наш коллектив.

• Для обсуждения реальных проблем социального развития, здравоохранения, трудовых отношений, социального обеспечения.

• Для участия в принятии важных социальных решений (это у нас неплохо получилось при открытом общественном обсуждении Концепции развития здравоохранения (www.zdravo2020.ru)).

медицинская информационная система **ДОКА+**

обеспечивает в больницах:

- автоматический персонифицированный учёт затрат на лечение;
- использование врачами стандартов лечения и обследования;
 - поддержку принятия решений врачей в ходе лечения;
- информатизацию работы руководителей, врачей, фармакологов, фармацевтов, медсестёр и ведение медицинской документации;
 - рационализацию расходов больниц.

Предназначена для больниц различного профиля, статуса, масштаба.

Ежедневно используется медперсоналом в 23 ЛПУ в 6 регионах РФ.

Легко освоить. Удобно использовать.

Эффективность применения в больницах доказана.

19 лет положительного опыта внедрения и сопровождения систем в больницах.

ООО «МедИнТех». 630117, Новосибирск, ул. Арбузова, 6. Тел. 83833360716.

info@docaplus.com

www.docaplus.ru



МЕДИАЛОГ®

Медицинская информационная система

Современный взгляд на работу клиники

Система МЕДИАЛОГ разработана компанией Пост Модерн Текнолоджи благодаря тесному сотрудничеству с практикующими врачами и руководителями медицинских учреждений - от поликлиник до крупных стационаров. Учитывая их пожелания и рекомендации, система совершенствовалась и развивалась в течение 15 лет.

Опыт использования позволяет утверждать на сегодняшний день, система МЕДИАЛОГ, обладая совокупностью преимуществ, является уникальным продуктом в классе медицинских информационных систем.



POST MODERN TECHNOLOGY

<http://www.postmodern.ru>
+7 (495) 780-60-51



Врач

и информационные
ТЕХНОЛОГИИ

