УДК 004.056

В.Д. Зыков, Р.В. Мещеряков, К.О. Беляков

Защита персональных медицинских данных в автоматизированных медицинских информационных системах лечебно-профилактических учреждений

Рассмотрены структура автоматизированных медицинских информационных систем лечебно-профилактических учреждений, схема информационного взаимодействия в сфере здравоохранения Томской области, а также предложена типовая структура защиты персональных медицинских данных в лечебно-профилактических учреждениях.
Ключевые слова: информационная безопасность, персональные медицинские данные, электронная цифровая подпись.

Современные информационные технологии играют важнейшую роль в медицинской отрасли, но одной из наиболее серьезных проблем, препятствующих их повсеместному внедрению, является обеспечение защиты информации, в том числе защиты персональных данных граждан [1] и сведений, составляющих медицинскую тайну, – персональных медицинских данных. Актуальность проблемы защиты персональных медицинских данных сегодня не вызывает сомнений. Кибертерроризм, доступ физических лиц к базам персональных данных усиливают риск вторжения в сферу частной жизни и нарушения права на ее неприкосновенность. Защита персональных медицинских данных является одной из наиболее острых проблем в информатизации организаций медицинской области.

При построении автоматизированных медицинских информационных систем (АМИС) лечебно-профилактических учреждений (ЛПУ) типовое решение выглядит, как показано на рис. 1.

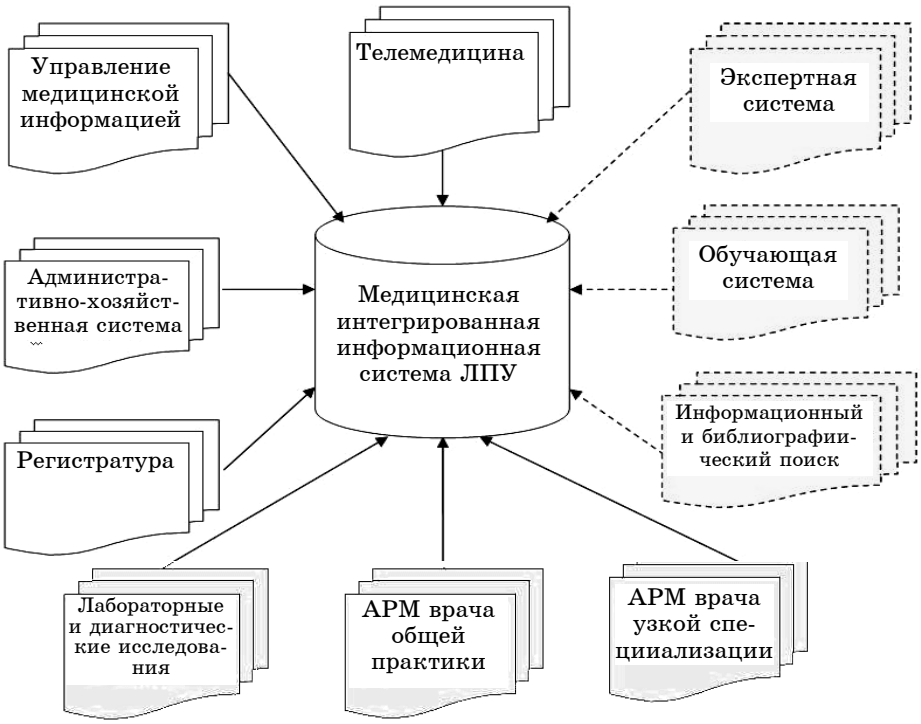

Рис. 1. Типовая структура АМИС ЛПУ

Как видно из рис. 1, АМИС ЛПУ построена по модульному принципу на основе клиент-серверной технологии. Основу серверной части АМИС составляет система управления базами данных (СУБД), в базе данных (БД) которой хранятся персональные медицинские сведения пациентов.

Клиентская часть представляет собой автоматизированное рабочее место (АРМ) сотрудника ЛПУ и клиента СУБД.

На практике АМИС ЛПУ взаимодействуют с информационными системами других учреждений и ЛПУ. Обмен данными происходит на основе согласованных форматов обмена данными. Общая схема информационного взаимодействия в сфере здравоохранения Томской области представлена на рис. 2.

Рис. 2. Общая схема информационного взаимодействия в сфере здравоохранения Томской области

С точки зрения обеспечения информационной безопасности и противостояния угрозам кибертерроризма наиболее актуальными задачами представляются:

1. Задача контроля и разграничения доступа к АРМ ЛПУ, поскольку сотрудники ЛПУ в зависимости от должности должны иметь доступ только к определенным клиентским модулям АМИС и соответствующим им типам персональных медицинских сведений.

2. Задача защиты информации при обмене данными между АРМ ЛПУ и серверной частью, поскольку каналы передачи информации могут проходить через неконтролируемую территорию (ЛПУ территориально может располагаться в нескольких зданиях).

3. Задача защиты информации при обмене данными с информационными системами других учреждений и ЛПУ.

4. Задача обеспечения юридической значимости электронных медицинских документов, обрабатываемых в АМИС, с целью полного перехода от бумажного документооборота к безбумажному.

Поскольку решение данных задач невозможно без использования технологии электронной цифровой подписи (ЭЦП) и технологии оказания доверенных услуг (удостоверяющего центра) [2], наиболее целесообразной для обеспечения защиты персональных медицинских данных представляется типовая структура защиты персональных медицинских данных в ЛПУ, представленная на рис. 3.

Согласно данной типовой структуре, система разграничения доступа для определения полномочий пользователя использует данные, указанные в сертификате открытого ключа ЭЦП.

Данные в АМИС и между информационными системами передаются по защищенному каналу связи с двусторонней аутентификацией сторон (например, по протоколу TLS).

В электронном журнале на серверной части обеспечивается регистрация запросов пользователей АМИС к БД с ЭЦП запросившего.

Для обеспечения юридической значимости электронных медицинских документов, обрабатываемых в АМИС, предполагается использование сервисов «доверенной третьей

стороны» (ДТС) – технологии оказания доверенных электронных услуг различного назначения.

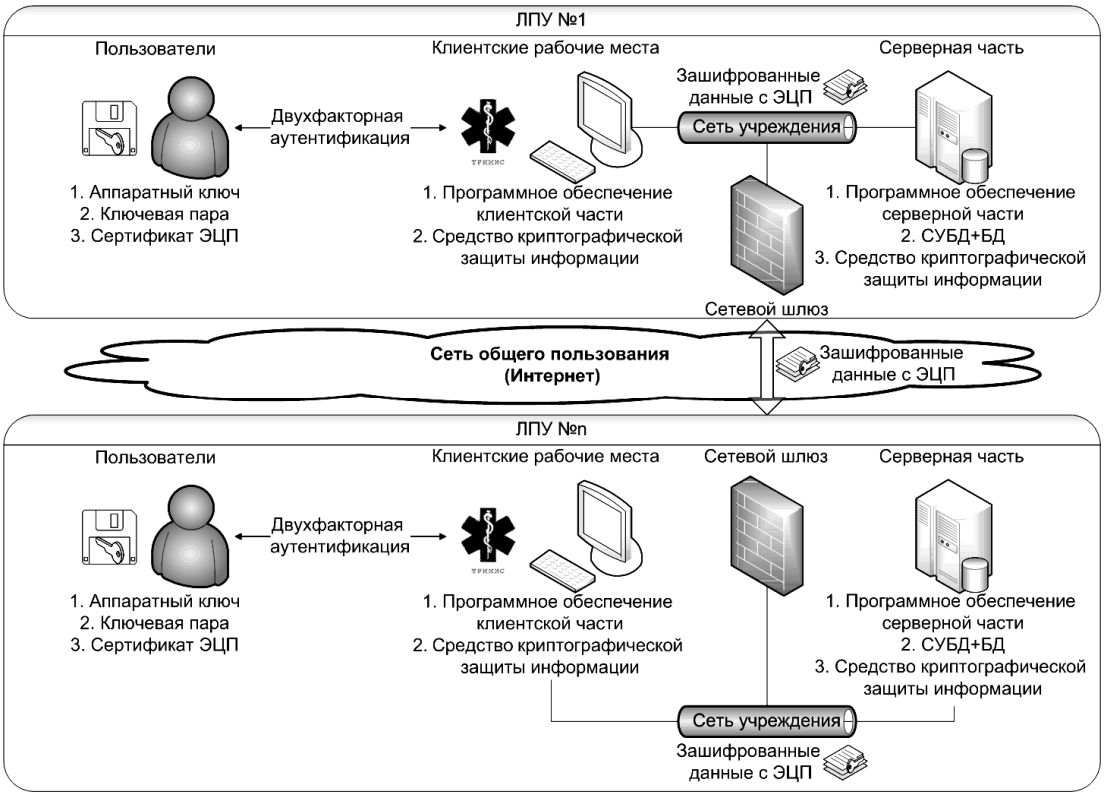

Рис. 3. Типовая структура защиты персональных медицинских данных в ЛПУ

Предлагается использование следующих сервисов ДТС:

1. Центр сертификации – для выдачи сертификатов открытых ключей ЭЦП.
2. Служба «Электронного нотариата» – для проверки валидности сертификата открытого ключа.
3. Сервер точного времени – для предотвращения коллизий, связанных с несовпадением времени.

Рассмотренная типовая структура была реализована в качестве стенда доработанной АМИС «ТРИМИС» разработки ООО «Элекард-Мед», который был представлен и апробирован на 12-й Межрегиональной специализированной выставке-ярмарке «МЕДИЦИНА. ЗДРАВООХРАНЕНИЕ. ФАРМАЦЕВТИКА» 22–24 апреля 2009 г.

Представленный стенд использовал сервисы «доверенной третьей стороны», развернутые на базе Удостоверяющего центра Сибири ТУСУР.

В настоящий момент идет развертывание доработанной АМИС в рамках пилотного проекта на территории Томской области и ведутся исследования о возможности использования дополнительных сервисов ДТС: службы атрибутирования для разграничения доступа на основе атрибутных сертификатов и использования службы штампов времени для подтверждения факта обладания информацией в определенный период времени.

Литература

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
2. Федеральный закон Российской Федерации от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».

Зыков Владимир Дмитриевич
аспирант каф. КИБЭВС ТУСУР, т. (3822) 412-500
Эл. адрес: zvd@udcs.ru

Мещеряков Роман Валерьевич
к.т.н., доцент кафедры КИБЭВС ТУСУР, т. (3822)413-426,
Эл. адрес: mrv@keva.tusur.ru

Беляков Константин Олегович
директор по развитию ООО «Элекард-Мед», т. (3822) 49-23-68,
Эл. адрес: Konstantin.Belyakov@elecard.ru

V.D. Zykov,R.V. Mescheriakov,K.O. Belyakov

Protection of the personal medical data in the automated medical intelligence systems of treatment-and-prophylactic establishments

In article the structure of the automated medical intelligence systems of treatment-and-prophylactic establishments, the circuit of informational interaction in sphere of public health services of the Tomsk region is considered, and also the standard structure of protection of the personal medical data in treatment-and-prophylactic establishments is offered.

Keywords: information security, personal medical data, the electronic digital signature.