ISBN 978-5-901795-18-7 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ. Переславль-Залесский, 2009

УДК 004.056

Я. И. Гулиев, И. А. Фохт, О. А. Фохт, А. Ю. Белякин

Медицинские информационные системы и информационная безопасность. Проблемы и решения

Аннотация. Статья посвящена результатам теоретических исследований и практических разработок Исследовательского центра медицинской информатики Института программных систем Российской академии наук (ИПС РАН) в области обеспечения информационной безопасности в медицинских информационных системах.

Ключевые слова: информационная безопасность, сохранность данных, несанкционированный доступ, медицинская информационная система, персональные данные, защита информации.

1. Введение

Три вектора информационной безопасности

Давным–давно, где-то в районе Древней Греции (а может и не Греции) раздался стук в бочку.

— Послушай, Диоген! Слава о твоей мудрости разлетелась по всем сторонам света. Помоги мне, я в затруднении, — молвил Цербер. Страж Аида переминался с ноги на ногу и озабоченно переглядывался тремя своими огромными головами.

— Как надежно сберечь поднадзорные мне человеческие судьбы, — начала одна голова, — от сглаза и лихих людей?

— Но так, — вмешалась другая, — чтобы не мешали замки да запоры богам, когда им нужно распорядиться охраняемым, ведь негоже напрягать Великих возней с ключами???

— И чтобы Бахус, — настойчиво уточняла третья,— повелевал в судьбах только весельем, Венера — только любовью, а Марс войной!!! И все три головы согласно закивали.

Вечерело. Клонящееся к закату солнце рисовало сверкающую дорожку на водах Адриатики. . .

И вылез из бочки Диоген. И веско сказал:

— Послушай меня, Цербер! Не паръся.

Особенностью медицинской информации является ее конфиденциальность. Права граждан на конфиденциальность информации о факте обращения за медицинской помощью и иных передаваемых

ими при обращении за медицинской помощью сведений, на информированное добровольное согласие как предварительное условие для медицинского вмешательства и отказ от него установлены Основами законодательства РФ об охране здоровья граждан от 22.07.93 №5488-1 (Постановление Правительства Российской Федерации. Основы законодательства Российской Федерации об охране здоровья граждан, 22.07.1993 №5488-1). Сведения, с которыми оперирует МИС, являются персональными данными и могут составлять врачебную тайну.

Информация, обрабатываемая при функционировании информационной системы медицинского учреждения, содержит также персональные данные. Защита персональных данных регламентируется нормативными документами, принятыми на федеральном уровне:

- Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
- Постановление 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»;
- Приказ ФСТЭК/ФСБ/Мининформсвязи России от 13 февраля 2008 года №55/86/20 «Об утверждении порядка проведения классификации ИН персональных данных».

Руководствуясь данной нормативной базой, Федеральная служба по техническому и экспортному контролю — ФСТЭК России — разработала ряд руководящих документов, направленных на выполнение мер по обеспечению безопасности персональных данных при их обработке, в информационных системах:

- «Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 14 февраля 2008 г. заместителем директора ФСТЭК России);
- «Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждена 15 февраля 2008 г. заместителем директора ФСТЭК России);

- «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» (утверждены 15 февраля 2008 г. заместителем директора ФСТЭК России);
- «Рекомендации по обеспечению безопасности персональных данных при их обработке, в информационных системах персональных данных» (утверждены 15 февраля 2008 г. заместителем директора ФСТЭК России).

Ожидается дальнейшая проработка методических рекомендаций ФСТЭК для практического применения при разработке ИС.

Исходя из важности обеспечения защиты информации, многие медицинские учреждения регулируют порядок обработки конфиденциальной информации собственными руководящими документами, разработанными с учетом требований Федерального законодательства, а также специфики ведомства.

Кроме того, база данных медицинской информационной системы содержит критически важную информацию, от которой, зачастую, может зависеть жизнь человека, следовательно, ключевым фактором при создании МИС должно стать обеспечение целостности и сохранности данных, возможности слежения за состоянием системы и ее защищенностью. Особое внимание должно уделяться разделению доступа пользователей МИС к различным фрагментам данных и защите информации от несанкционированного доступа, а также от утраты и искажения данных [1].

Обеспечение заданного уровня информационной безопасности определяется тремя векторами — конфиденциальностью, целостностью и доступностью данных. В зависимости от возрастания уровня каждого из них, соответственно уменьшаются остальные. Так, добиваясь легкости доступа пользователя МИС к данным, приходится в какой-то степени жертвовать конфиденциальностью и целостностью. И наоборот, условие соблюдения конфиденциальности и целостности влечет за собой усложнение обращения пользователя с информацией. В то же время, повышение уровня безопасности вызывает необходимость возрастания всех этих составляющих, что в свою очередь может негативно сказаться на скорости и надежности работы программного обеспечения. Таким образом, простое следование правилам работы со сведениями ограниченного распространения

может парализовать работу ЛПУ в условиях ведения электронной истории болезни.

Современные технологии предлагают множество различных решений проблемы безопасности конфиденциальной информации, основанные на тех или иных механизмах и так или иначе смещенные в сторону того или иного составляющего вектора. Для определения оптимума уровня информационной безопасности необходимо четко представлять степень взаимодействия всех ее составляющих и влияния их на работу конечного пользователя МИС. Вместе с тем следует учитывать применимость того или иного решения в конкретной ситуации функционирования информационной системы.

Необходимо также принимать во внимание, что медицинская информация имеет ряд особенностей по сравнению с другими видами конфиденциальной информации.

Таким образом, построение адекватной схемы защиты данных в каждом конкретном случае является поиском компромисса с учетом специфики работы МИС ЛПУ как системы массового обслуживания. Обеспечением защиты данных в медицинской информационной системе занимается подсистема информационной безопасности (ПИБ).

2. Медицинская информация, как сведения ограниченного распространения

О целом и частном

Цербер с Диогеном сидели на песке. Вокруг в одним им ведомом порядке были разложены доски, досочки, пара металлических ободов, железные гвозди и какие-то скобы.

Невдалеке отчетливо выделялся след от чего-то большого, округлого, еще совсем недавно полувдавленного в том месте в песок.

Смеркалось. Ярким желтым цветом наливалась на стремительно синеющем небе луна.

— Теперь я понял, как она устроена! — радостно воскликнул Цербер и поправился: — Была... устроена. Спокойной ночи, Диоген, — и страж двинулся к своей пещере, загребая песок косолапыми ногами.

Чело Диогена также озарила светлая радость понимания. Вот только озабоченность проглядывала сквозь нее все сильнее с каждым его взглядом на кучу того, что раньше было бочкой.

2.1. Сущности, составляющие основу МИС ЛПУ

Комплексная информационная система, автоматизирующая все стороны жизнедеятельности медицинского учреждения, представляет собой интегрированную информационную и функциональную среду, объединяющую элементы различных классов медицинских информационных систем. Система обеспечивает информационную поддержку всех служб медицинского учреждения от документооборота и финансового учета до ведения клинических записей о пациенте, интеграции с медицинским оборудованием и поддержки принятия решений.

Сущности, составляющие основу архитектуры такой МИС, и взаимосвязи между ними представлены на следующей схеме (Рис. 1):

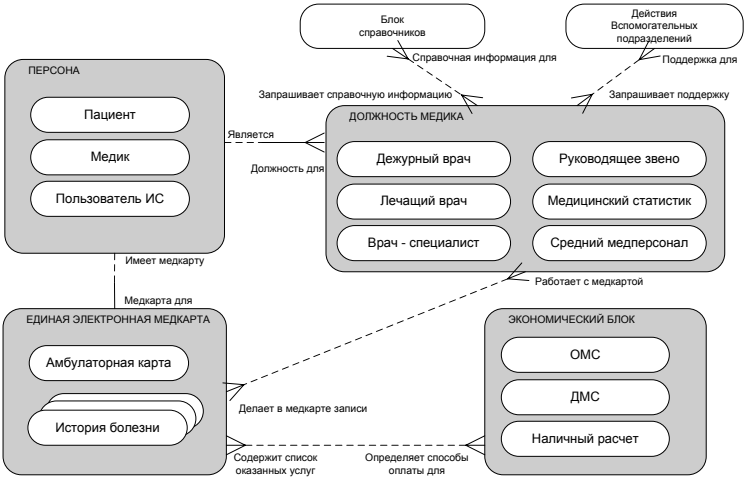

Рис. 1. Структура МИС

Основными объектами предметной области в информационной системе являются:

- *Персона* — это может быть любой человек (пациент из состава прикрепленного контингента, сторонний пациент, медперсонал медицинского учреждения, сторонний медперсонал, пользователь ИС). Данная сущность делится на основные типы — Пациент, Медицинский персонал и Пользователь ИС.
- *Единая электронная медкарта*, которая содержит в своем составе Амбулаторную карту и Истории болезни пациента.
- *Должность медика* — должность, определяющая качество, в котором выступает та или иная персона, работая в данный момент времени с медицинской картой (один и тот же человек может выступать в качестве, например, лечащего врача, члена хирургической бригады, заведующего отделением, консультанта и т.д.). Данная сущность делится на основные типы — Руководящее звено, Дежурный врач, Лечащий врач, Врач–специалист (консультант, член хирургической бригады, врач диагностического отделения и т.д.), Медицинский статистик и Средний медперсонал.
- *Экономический блок.* Определяет себестоимость оказанных пациенту услуг и способы оплаты.
- *Блок справочников.* Специалисты–медики в своей работе нуждаются в справочной информации по самым различным вопросам (справочники медикаментов, диагнозов, стандартов оказания медпомощи и т.д.). На диаграмме справочники объединены в сущность Блок справочников без уточнения (на данном этапе) их конкретного вида, содержания и способов работы с ними.
- *Действия вспомогательных подразделений.* Основными сущностями при рассмотрении деятельности медицинского учреждения являются те, что относятся непосредственно к лечебно–диагностическому процессу. Но, чтобы учреждение могло функционировать, необходима работа многих вспомогательных учреждений (отдела кадров, пищеблока, библиотеки и т.д.). На данной диаграмме действия всех этих подразделений обозначены одной сущностью, что позволяет, не конкретизируя и не останавливаясь на них подробно, отметить все-таки их присутствие и важность для деятельности учреждения.

Персона может иметь Амбулаторную карту — если человек входит в состав прикрепленного контингента. Персона может иметь (необязательно) Историю болезни (или даже несколько) — если человек не прикреплен к медучреждению, но попадает в него лечиться. Персона может занимать (необязательно) какую-либо должность (или даже несколько) по отношению к работе с медкартами в данном учреждении.

Должность медика при работе с медкартами ассоциируется (обязательно) с какой-либо одной определенной персоной. Выступая в данной должности, медик может (необязательно) работать с одной или несколькими Амбулаторными картами, а также с одной или несколькими Историями болезней.

Амбулаторная карта ассоциируется (обязательно) с какой-либо одной определенной персоной. В Амбулаторной карте могут делать записи (необязательно) медработники разных должностей. Амбулаторная карта может содержать (необязательно) в своем составе несколько Историй болезни.

История болезни как правило (но необязательно) входит в состав одной определенной Амбулаторной карты. В этом случае она (обязательно) ассоциируется с одной определенной персоной. Однако, если человек не прикреплен к данному учреждению, то он может и не иметь АК, в этом случае ИБ все равно ассоциируется (обязательно) непосредственно с одной определенной персоной. В Истории болезни могут делать записи (необязательно) медработники разных должностей.

Единая электронная медкарта. Содержит в своем составе Амбулаторную карту и Истории болезни. Поддерживает их связи с другими сущностями МИС. Медкарта как правило (но необязательно) содержит список услуг (их может быть несколько), оказанных пациенту.

Экономический блок как правило (но необязательно) подсчитывает стоимость и определяет способы оплаты (может быть комбинация из нескольких) оказанных услуг из списка, содержащегося в Медкарте.

Блок справочников используется (необязательно), но, возможно, неоднократно, медработниками. Использовать справочники (необязательно) могут медработники разных должностей.

Действия вспомогательных подразделений (возможно, различные) могут быть (хотя и необязательно) затребованы в ходе лечебно–диагностического процесса. Пользоваться этими действиями (необязательно) могут медработники разных должностей.

2.1.1. *Обмен информацией между врачом и пациентом*

Объем и степень обмена информацией между врачом и пациентом характеризуют модели их взаимоотношений:

(1) Патерналистическая модель (врач–опекун) — ограничивает права пациента в получении абсолютно полной информации и тем самым ограничивает возможность его участия в принятии решений по тому либо иному виду вмешательства.
(2) Информационная модель (научная, потребительская) — не имеет ограничений в предоставлении информации пациенту.
(3) Интерпретационная модель (врач в роли советчика, консультанта) — имеет определенные врачом ограничения в предоставлении информации пациенту.
(4) Совещательная модель — не ограничивает прав пациента в предоставлении информации, выбор условий принимаемого решения остается за пациентом.

Информационная модель является преимущественной во взаимоотношениях врача и пациента в США. В России по данным исследования этой модели взаимоотношений отдают предпочтение 4,3% врачей, а преимущественной считают интерпретационную модель, в которой существует определенная степень ограничений по предоставлению информации пациенту.

2.2. Спецификация и классификация типов информации в МИС с точки зрения системы безопасности

Попытаемся определить виды информации, которые будут циркулировать в МИС ЛПУ, и возможные операции над этой информацией, а также систематизируем эти данные в соответствие с уровнями секретности, актуальными для ЛПУ.

2.2.1. *Информация пациента*

Прежде всего, выделим фрагменты информации о пациенте. Это:

- О факте обращения.
- Персональные данные пациента.
- Принадлежность к группе.
- Диагноз.
- Анамнез.
- Назначения и рекомендации.
- Состояние, о ходе лечения.
- Себестоимость.
- Способы оплаты.

О факте обращения

Информация о факте обращения в лечебное учреждение отнесена законодательством к личной тайне пациента. И обязана соблюдаться сотрудниками ЛПУ как тайна профессиональная. Говорить о факте обращения, вообще, имеет смысл только в сочетании с персональными данными пациента — то есть, о факте обращения в ЛПУ такого-то человека.

Персональные данные сотрудника ЛПУ

Персональные данные пациента отнесены законодательством к личной тайне пациента. Более того, они выделены в особую категорию, охраняемую специальным образом. Конфиденциальность этих данных должна соблюдаться сотрудниками ЛПУ как тайна профессиональная.

Данный вид информации характеризуется тем, что для собственно процесса лечения пациента он не предоставляет ничего необходимого. Используются такие данные только с целью внутренней идентификации больного для установления однозначной ассоциации между собой всего потока медицинской информации относительно него. Но для данной цели может служить любой, не составляющий персональных данных идентификатор — номер медкарты, штрих-код, магнитная карта и пр.

Принадлежность к группе

К таким данным относятся пол и возраст пациента, регион его проживания, принадлежность его к некоторым профессиям, категориям льготности и пр. Эти данные являются агрегирующими и, при

достаточном уровне абстрагированности, не представляют собой конфиденциальной информации, т.к. по ним нельзя однозначно идентифицировать персону. Такие данные обычно используются в статистике для получения общей картины в той или иной области по тому или иному признаку относительно некоторой группы.

Более того, именно эти данные, как правило, достаточны для лечения пациента. Лечение, назначаемое врачом, прежде всего, основывается именно на принадлежности к некой группе (может стать причиной особенности течения заболевания и выбора способа лечения) и на состоянии человека, которые врач определяет для конкретного пациента, основываясь на объективных данных, на его личных показаниях и на личной медицинской истории пациента, а вовсе не на его ФИО, адресе и номере паспорта.

В то же время следует учесть, что, если уровень детализации низок, то даже такие данные могут однозначно определить человека, то есть, сыграть роль персональных.

Так, например, в Москве информация о некой „ученице 9-ого класса, оказавшейся беременной и из-за этого в прошлую пятницу утром пытавшейся покончить жизнь самоубийством“, ничего не говорит о личности подростка, является абстрактной и может распространяться даже средствами массовой информации как описание некоего явления, а не личности человека. В то же время эта же информация в небольшом населенном пункте, где есть только один 9-ый класс, в нем 5 девочек, 4 из которых были в это время на занятиях, совершенно определенно расскажет одноклассникам девочки о ее проблеме.

Диагноз

Информация о диагнозе относится к личной тайне пациента. И обязана соблюдаться сотрудниками ЛПУ как тайна профессиональная. Этот вид информации характеризуется тем, что составляет врачебную тайну только в сочетании с персональными данными пациента.

Анамнез

Во время сбора анамнеза врачу, зачастую, приходится иметь дело с личной тайной. Причем, не только с личной тайной самого пациента, распорядителем которой он является и которую сообщает врачу по собственной воле, но и с личной тайной близких пациенту людей,

которые согласия на распространение такой информации о них не давали.

Например, это могут быть сведения о наследственных заболеваниях (чем болеют родственники пациента), об обстоятельствах родов (касается и личной тайны ребенка/матери пациента), о заболевании, привычках, характере работы мужа/жены пациента. Все эти сведения, с одной стороны, необходимы, т.к. могут помочь в постановке верного диагноза и способствовать выбору верного способа лечения. С другой стороны, получение этих данных и их обработка явно противоречит законодательству, т.к. это тайна НЕ пациента, о сохранении здоровья которого идет речь.

Данные, входящие в анамнез, также характеризуются тем, что составляют врачебную тайну только в сочетании с персональными данными пациента.

Назначения и рекомендации

В сочетании с персональной информацией о пациенте эти данные составляют врачебную тайну, так как могут поведать о диагнозе пациента и о состоянии его здоровья.

В сочетании с диагнозом, но без персональных данных, такие сведения не конфиденциальны, представляют, скорее, научный или учебный интерес и могут публиковаться в печати.

Самое главное отличие этого вида информации в том, что в сочетании с идентифицирующими пациента данными (даже если для идентификации используются не персональные данные!) эти сведения критически важны для лечения пациента.

Если ранее мы говорили в основном о сохранении конфиденциальности, то сохранность от утраты, от случайной несанкционированной, а тем более от вредоносной модификации назначений и рекомендаций, и особенно при обработке в МИС, имеет жизненно важное значение. И тем большую значимость это обстоятельство приобретает в стационаре, где непосредственно исполняются назначения и где состояние здоровья пациентов, как правило, более тяжелое, чем при амбулаторном лечении.

Несанкционированное изменение таких данных может привести к ситуации, когда пациенту будут проведены лечебные манипуляции (выданы медикаменты) не только не показанные при его заболевании/состоянии, но и прямо вредящие его здоровью, а в отдельных случаях и могущие привести к смертельному исходу.

Состояние, о ходе лечения

В сочетании с персональной информацией о пациенте эти данные составляют врачебную тайну, так как могут поведать о диагнозе пациента и о состоянии его здоровья.

В сочетании с диагнозом, но без персональных данных, такие сведения не конфиденциальны, представляют, скорее, научный или учебный интерес и могут публиковаться в печати.

С точки зрения лечения пациента сохранность таких данных представляет интерес для определения динамики его состояния. Но такой критической роли, как описанные выше назначения и рекомендации, данная информация не играет.

Себестоимость

Себестоимость оказанных пациенту в ЛПУ услуг прежде всего важна для самого ЛПУ. Основываясь на этих данных, ЛПУ может формировать свою экономическую политику, строить свои отношения со страховщиками, поставщиками медикаментов и т.д.

Стоимость лечения и способы оплаты

Стоимость оказанного лечения и способы его оплаты, как правило, представляют из себя личную тайну пациента, а зачастую, и служебную информацию организации–плательщика.

Структура информации пациента, ее составные части и способы группировки для составления тех или иных видов конфиденциальной информации показаны на схеме (Рис. 2).

2.2.2. *Информация сотрудника ЛПУ*

Далее рассмотрим структуру информации о сотруднике ЛПУ. Это:

- персональные данные,
- специализация,
- кадровая информация,
- график работы.

Персональные данные пациента

Персональные данные отнесены законодательством к личной тайне человека. Более того, они выделены в особую категорию, охраняемую специальным образом.

Но персональные данные сотрудника ЛПУ, как специалиста, который лечит людей, носят противоречивый характер. Для того, чтобы пациенты могли идентифицировать специалиста, к которому они

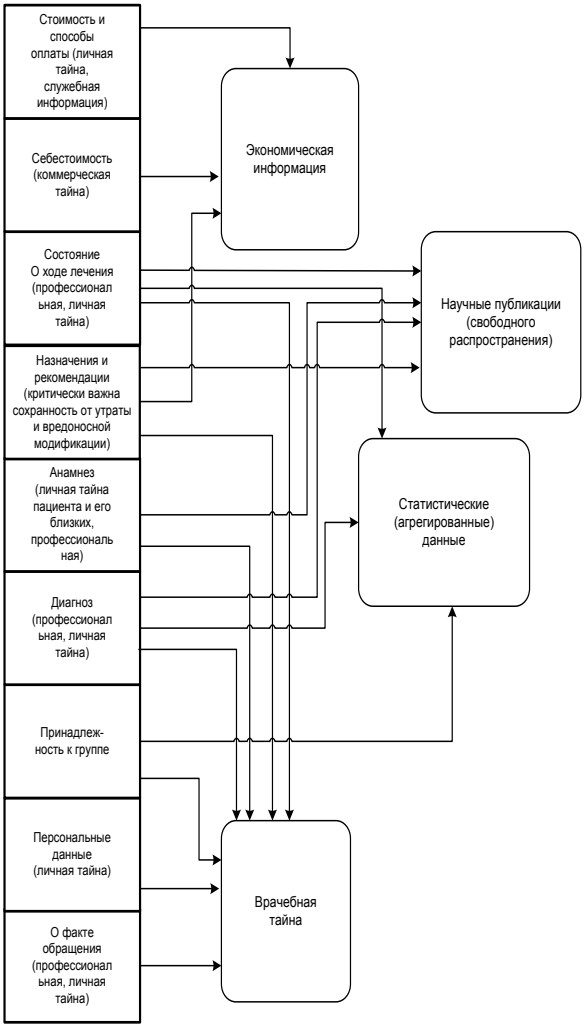

Рис. 2. Информация пациента. Структурная схема

обращаются (а зачастую именно это играет решающую роль в обращении пациента ко врачу), фрагменты персональных данных врачей, в принципе, достаточные для однозначной идентификации, должны быть предоставлены широкому кругу пользователей. Например, они фигурируют в расписании приема, доступном неограниченному кругу людей.

В то же время, такие данные могут быть использованы и злоумышленниками (тогда как действующее законодательство именно по этой причине и призывает сохранять их конфиденциальность) — например, чтобы определить, когда тот или иной человек появится в определенном месте (закончит работу и выйдет из здания) или, напротив, не появится (будет отсутствовать дома).

Специализация

Специализация медицинского работника определяет его роль в лечебно-диагностическом процессе. Эти сведения относятся к базовым в описании ЛПУ как лечебно-профилактического учреждения.

При той трактовке персональных данных, которая дана в предыдущем пункте, специализацию медицинского работника можно, зачастую, отнести к составляющей его персональных данных.

График работы

График работы специалиста, а также данные о не занятых на данный момент временных слотах его приема относятся к базовым в описании ЛПУ как лечебно–профилактического учреждения.

График работы необходим и пациентам, как потенциальным потребителям рабочего времени врача. Далее на схеме показана структура информации сотрудника ЛПУ, ее составные части и способы группировки для составления тех или иных видов конфиденциальной информации (Рис. 3).

Кадровая информация

Данные об образовании, о назначении на должность, о совмещении, о поощрениях/взысканиях и пр. Составляют как личную тайну сотрудника, так и служебную информацию ЛПУ. Сотрудники отдела кадров обязаны сохранять конфиденциальность этих сведений.

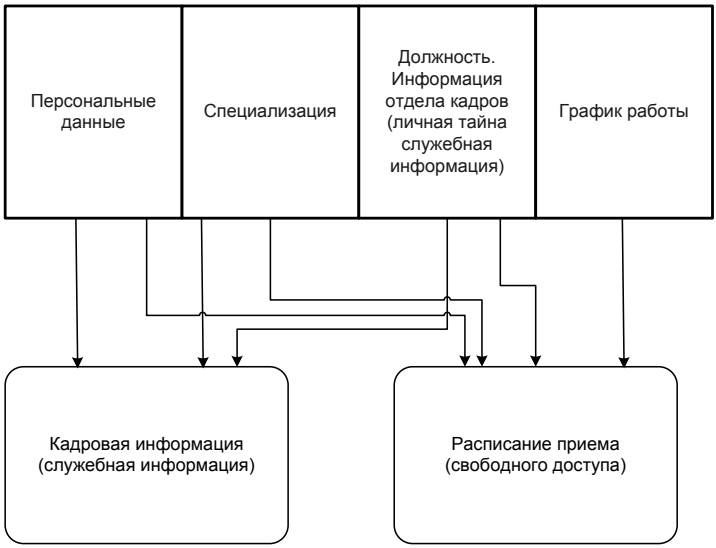

Рис. 3. Информация сотрудника ЛПУ. Структурная схема

2.3. Уровни защиты данных

Как видно из предыдущих разделов, основными типами совокупностей медицинской информации являются:

- информация пациента;
- информация сотрудника ЛПУ;
- справочная информация, описывающая ЛПУ;
- справочная информация, описывающая предметную область.

Данные каждой совокупности могут быть разной степени конфиденциальности, то есть, относятся к различным уровням защиты данных.

2.3.1. *Информация пациента*

Информация пациента сосредотачивается в понятии Медицинская карта (Рис. 4). Выделяются разные уровни конфиденциальности составляющих ее данных (по степени убывания конфиденциальности):

- Персональные данные (без которых практически теряется конфиденциальность остальных составляющих).
- Врачебная тайна (относительно данного пациента и его близких).
- Коммерческая тайна ЛПУ (информация ЛПУ о лечении данного пациента).
- Обезличенные агрегированные данные, входящие в статистическую информацию (могут быть полностью открыты, а могут составлять служебную информацию).

2.3.2. *Информация сотрудника ЛПУ*

Информация сотрудника сосредотачивается в личном деле сотрудника ЛПУ (Рис. 4). Выделяются разные уровни конфиденциальности составляющих ее данных (по степени убывания конфиденциальности):

- персональные данные (фрагменты из которых, несмотря на принадлежность к персональным данным, публикуются открыто);
- кадровая информация (составляющая личную тайну сотрудника и служебную информацию ЛПУ);
- расписание работы персонала (открытая информация, которая защищается лишь относительно сохранности данных).

2.3.3. *Справочники, описывающие ЛПУ*

ЛПУ как учреждение, призванное выполнять лечебно–диагностические функции, описывается комплексом справочной информации (Рис. 5). В медицинской информационной системе справочная информация о ЛПУ хранится в общесистемных справочниках:

- справочник физической структуры ЛПУ (помещений),
- справочник функциональной структуры ЛПУ,
- справочник территориальных участков,
- справочник штатного заполнения,
- справочник абстрактных ресурсов,
- справочник ресурсов,
- справочник услуг,
- справочник пользователей МИС.

Как правило, все это — информация для служебного использования, которая объединяется уровнем защиты «Служебная информация».

2.3.4. *Справочники, описывающие предметную область*

Предметная область деятельности ЛПУ — лечебно–диагностический процесс — также описывается комплексом справочной информации (Рис. 6). В медицинской информационной системе справочная информация о предметной области хранится в общесистемных справочниках:

- К группе, описывающей медицинские манипуляции, относятся справочники:
  - МКБ-10,
  - коды медико-экономических стандартов,
  - список льготных препаратов,
  - схемы наблюдения диспансерного учета,
  - справочник услуг,
  - редактор разбиений МКБ-10, и т.д.
- В качестве справочных пособий в МИС могут дополнительно присутствовать:
  - список профессиональных заболеваний;
  - нормативы обследований при профосмотрах, связанные с рисками профессиональных заболеваний;
  - нормативы по диспансеризации;
  - группы и категории пациентов, подлежащих диспансеризации;
  - нормативы по анализам и исследованиям;
  - Московские городские стандарты оказания медицинской помощи;
  - реестр лекарственных средств;
  - телефонный справочник;
  - наглядные пособия, медицинская литература и т.д.

Как правило, все эти данные полностью открыты. Уровень защиты, объединяющий их, обеспечивает сохранность данных, а не их конфиденциальность.

Задача ПИБ — установить соответствие между специфицированными группами пользователей МИС и классами информации внутри информационной системы.

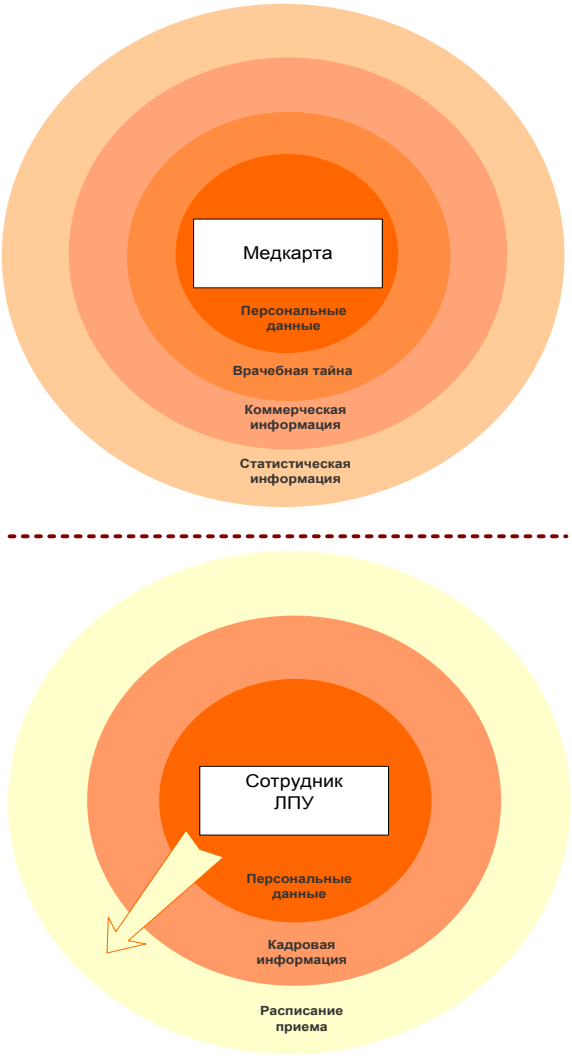

Рис. 4. Информация пациента и сотрудника ЛПУ. Структурная схема

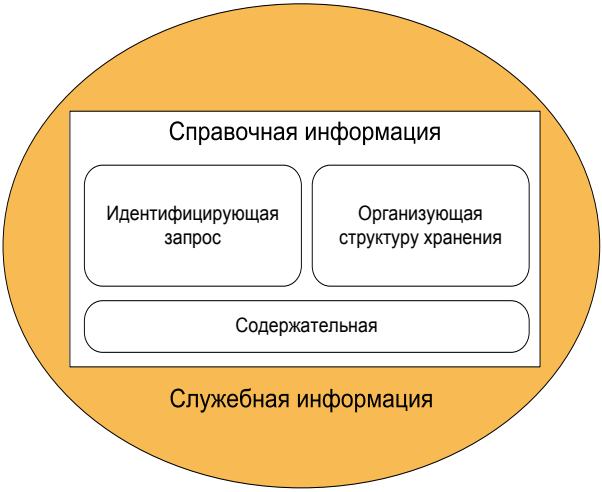

Рис. 5. Справочники, описывающие ЛПУ

Рис. 6. Справочники, описывающие предметную область

3. Модель нарушителя МИС ЛПУ

Гармонию Алгеброй поверяя...

Однажды Диоген с Цербером рассуждали о несовершенстве мира.

Штормило. Раскачиваемые ветром пальмы мели космами песок. За стенкой бочки кто-то чавкал и хрустел костями. В чаще трещало буреломом. В грязной пене прибоя мотылялось невесть откуда принесенное волнами полено.

— А ведь бывает, что солнышко, — жаловался Цербер. — И что полезные растения, и что ровненько так растут. И что у воды неспешно прогуливается белая чайка...

— А это потому, — объяснял Диоген, — что каждый должен заниматься своим делом, и что все должно быть по правилам. Заинтересованный Цербер внимал.

Прошло время.

Грустно глядя из бочки на бескрайние ровные грядки генетически модифицированной сои, простирающиеся, куда ни кинь взгляд, до самого горизонта, и на взвод марширующих вдоль идеально ровной кромки воды чаек, Диоген грустно шептал:

— Цербер... Ты меня не понял.

3.1. Основные проблемы и направления обеспечения ИБ

Информационная безопасность (ИБ) при функционировании медицинской информационной системы обеспечивается за счет взаимоувязанного комплексного использования организационных мер, программных и технических средств защиты [2]. Перечислим основные направления возможных нарушений ИБ:

- утечка данных (нарушение конфиденциальности);
- утрата данных;
- несанкционированная модификация данных.

При включении в МИС средств обеспечения информационной безопасности необходимо помнить, что наращивание требований по ИБ неизбежно накладывает ограничения на доступность данных для пользователей МИС. Есть три вектора информационной безопасности:

- конфиденциальность;
- целостность;
- доступность данных.

И обеспечение ИБ должно строиться на компромиссе между ними, обеспечивая приемлемый уровень безопасности наряду с приемлемыми для работы пользователей ограничениями в части санкционирования использования ресурсов и сервисов МИС.

3.1.1. *Объекты защиты МИС*

Критичными активами информационной системы медицинского учреждения являются:

- информация в БД СУБД;
- ресурсы файлового сервера ЛПУ;
- резервные копии БД СУБД и архивные копии ресурсов файлового сервера;
- управляющая информация операционной системы, СУБД, АРМов администратора МИС и администратора ИБ;
- технологический процесс сбора, обработки, хранения и передачи информации в МИС;
- аппаратно-программный комплекс, обеспечивающий работу МИС.

3.1.2. *Вероятные угрозы ИБ МИС*

Критичными для МИС будут являться следующие виды угроз:

- На физическом уровне — выведение из строя аппаратных средств хранения, обработки и передачи информации (рабочие станции ЛПУ, серверы), отказ, уничтожение носителей информации. Основной источник угроз — техногенные аварии, нарушение правил эксплуатации. Указанные угрозы приводят к потере доступности информации.
- На сетевом уровне и уровне сетевых приложений и сервисов — блокирование работы серверов МИС, несанкционированный доступ к информационному ресурсу в результате ошибочных настроек сетевых сервисов. Угрозы ведут к потере доступности и конфиденциальности информации.
- На уровне операционных систем — уничтожение прикладного ПО, нарушение правильной работы информационных серверов, клиентских рабочих мест в результате заражения компьютерным вирусом при проведении модификации ПО, искажение/уничтожение информации в результате заражения системы компьютерным вирусом при переносе информации с внешних носителей. Основное воздействие данных

угроз — на доступность и целостность, возможное воздействие — на конфиденциальность информации. Субъектом угроз является персонал, нарушающий правила эксплуатации и сопровождения МИС в ЛПУ.

- На уровне управления БД наиболее опасной угрозой является НСД к БД в результате получения административных паролей СУБД, паролей администраторов МИС, либо несанкционированные действия администраторов БД, администраторов МИС. Результатом воздействия таких угроз может быть потеря доступности данных вследствие нарушения работоспособности СУБД и удаления (изменения) объектов или настроек, нарушение целостности, нарушение конфиденциальности данных.
- На уровне технологического процесса — ввод фиктивной информации, неправомерный вывод и разглашение конфиденциальной информации. Основное воздействие данных угроз — на целостность и конфиденциальность информации.

3.2. Модель нарушителя

Внутренние нарушители ИБ МИС ЛПУ — это сотрудники ЛПУ, осуществляющие в соответствии с предоставленными им правами и полномочиями деятельность по реализации поддерживаемых МИС функций и задач, а также лица, обслуживающие аппаратно–программные комплексы МИС или допущенные к ним, в здания и помещения, где функционирует МИС ЛПУ. Внешние нарушители ИБ МИС ЛПУ — это сотрудники ЛПУ, которым не предоставлены права по доступу к ресурсам, в здания и помещения, где функционирует МИС ЛПУ, а также субъекты, не являющиеся сотрудниками ЛПУ, но осуществляющие попытки несанкционированного доступа к указанным ресурсам.

3.2.1. *Внутренние нарушители ИБ МИС ЛПУ*

В рамках построения ПИБ МИС ЛПУ возможны действия внутреннего нарушителя, принадлежащего к любой из следующих четырех категорий лиц:

(1) пользователи МИС ЛПУ — медицинский персонал, осуществляющий доступ к информационным и вычислительным ресурсам МИС ЛПУ в рамках выполнения своих должностных обязанностей;

(2) технический персонал МИС ЛПУ (системные администраторы, администраторы ЛВС, администраторы СУБД, администраторы прикладных программных комплексов, администраторы ИБ, операторы, программисты и инженеры сопровождения) — сотрудники ЛПУ, задачей которых является организация эксплуатации, обслуживание ПО и технических средств МИС ЛПУ;
(3) посетители ЛПУ — лица, персональные данные которых обрабатываются МИС ЛПУ, и которым предоставлен доступ на объекты и в помещения, где функционирует МИС ЛПУ, в установленном порядке;
(4) обслуживающий персонал и охрана объектов и помещений, в которых размещаются технические средства МИС ЛПУ.

Потенциальные внутренние нарушители первой категории осуществляют санкционированный доступ к информационным ресурсам МИС ЛПУ в соответствии с предоставленными полномочиями и правами доступа. В соответствии с действующим законодательством несут административную и уголовную ответственность за нарушение конфиденциальности при работе с информацией, содержащей сведения, составляющие врачебную тайну и персональные данные.

Потенциальные внутренние нарушители первой категории осуществляют доступ к информационным ресурсам МИС ЛПУ посредством прикладного ПО МИС, установленного на технических средствах МИС.

В модели нарушителя по отношению к внутренним нарушителям первой категории принимаются следующие ограничения:

- нарушитель не может реализовывать угрозы, зная, что подобные попытки будут обнаружены сотрудниками, сопровождающими и эксплуатирующими МИС ЛПУ, а также лицами, уполномоченными осуществлять контроль доступа к техническим средствам и ресурсам МИС;
- возможность установки и использования нарушителем технических средств съема и передачи информации, в том числе замаскированных под штатные технические средства (путем подмены), исключается общережимными мерами по противодействию техническому проникновению на территорию объектов и в помещения, где расположены технические средства МИС ЛПУ;

- нарушитель не будет использовать возможно имеющиеся особенности ПО (включая прикладное ПО), которые потенциально позволяют нарушить защищенность системы, но не описаны в документации на ПО и не известны сотрудникам, обеспечивающим эксплуатацию и сопровождение МИС ЛПУ.

Потенциальные внутренние нарушители второй категории осуществляют санкционированный доступ к информационным и вычислительным ресурсам МИС ЛПУ в соответствии с предоставленными полномочиями и правами доступа. Не предоставляются права доступа к информации, содержащей сведения, составляющие врачебную тайну и персональные данные.

Потенциальные внутренние нарушители второй категории осуществляют доступ к информационным и вычислительным ресурсам МИС посредством системного, базового и прикладного ПО, установленного на технических средствах МИС ЛПУ.

В модели нарушителя по отношению к внутренним нарушителям второй категории принимаются следующие ограничения:

- работа по подбору кадров ЛПУ и специальные мероприятия исключают возможность создания коалиций нарушителей из числа сотрудников указанной категории, т.е. объединения и целенаправленных действий по преодолению системы защиты с участием двух и более сотрудников;
- нарушитель не может реализовывать угрозы, зная, что подобные попытки будут обнаружены другими сотрудниками, сопровождающими и эксплуатирующими МИС ЛПУ, а также лицами, уполномоченными осуществлять контроль доступа к ресурсам и техническим средствам МИС ЛПУ;
- возможность установки и использования нарушителем технических средств съема и передачи информации, в том числе замаскированных под штатные технические средства (путем подмены), исключается общережимными мерами по противодействию техническому проникновению на территорию, где функционирует МИС ЛПУ;
- нарушитель не будет использовать возможно имеющиеся особенности ПО (включая прикладное ПО), которые потенциально позволяют нарушить защищенность системы, но не

описаны в документации на ПО и не известны сотрудникам, обеспечивающим эксплуатацию и сопровождение МИС ЛПУ.

Потенциальным внутренним нарушителям третьей и четвертой категорий предоставляется доступ в здания и помещения, в которых расположены технические средства МИС ЛПУ в соответствии с установленным порядком. Не предоставляются полномочия и права доступа к информационным и вычислительным ресурсам МИС ЛПУ. Не предоставляются полномочия и права доступа к техническим средствам МИС ЛПУ.

Потенциальные внутренние нарушители третьей категории не заинтересованы в нарушении конфиденциальности информации, содержащей сведения, которые составляют врачебную тайну и касаются их самих. Тем не менее, они могут осуществлять попытки нарушения конфиденциальности подобной информации о других лицах, а также доступности и целостности информационных ресурсов МИС ЛПУ в целом.

В модели нарушителя по отношению к внутренним нарушителям третьей и четвертой категорий принимаются следующие ограничения:

- нарушитель не может реализовывать угрозы, зная, что подобные попытки будут обнаружены другими сотрудниками, сопровождающими и эксплуатирующими МИС ЛПУ, а также лицами, уполномоченными осуществлять контроль доступа к техническим средствам и ресурсам МИС ЛПУ;
- возможность установки и использования нарушителем компактных технических средств съема и передачи информации, в том числе замаскированных под штатные технические средства (путем подмены), исключается общережимными мерами по противодействию техническому проникновению на территорию, где функционирует МИС ЛПУ;
- нарушитель не будет использовать возможно имеющиеся особенности ПО (включая прикладное ПО), которые потенциально позволяют нарушить защищенность системы, но не описаны в документации на ПО и не известны сотрудникам, обеспечивающим эксплуатацию и сопровождение МИС ЛПУ.

Принимаются следующие предположения об уровне знаний и возможностях внутреннего нарушителя ИБ:

- нарушитель обладает высоким уровнем знаний в области программирования, проектирования и эксплуатации МИС ЛПУ, технико-программного обеспечения в целом;
- нарушитель знает структуру, функции и механизм действия средств защиты, их место в системе ИБ МИС ЛПУ;
- нарушитель правильно представляет функциональные особенности работы МИС ЛПУ, основные закономерности формирования в ней информационных массивов и потоков запросов к ним;
- нарушитель может использовать непреднамеренные действия других пользователей МИС ЛПУ (эти действия могут быть как случайными, так и обусловленными необходимостью выполнения пользователями своих служебных обязанностей).

При этом нарушитель может использовать:

- штатные технические средства, входящие в состав МИС ЛПУ (при получении к ним доступа);
- штатные носители информации и технические средства, которые разрешается легально проносить через посты охраны ЛПУ;
- компактные носители информации и технические средства (например, сотовый телефон, беспроводные средства передачи информации и т.п.), непосредственно не относящиеся к СВТ.

3.2.2. *Внешние нарушители ИБ МИС ЛПУ*

В рамках построения ПИБ МИС ЛПУ возможны действия внешнего нарушителя, принадлежащего к любой из следующих трех категорий лиц:

(1) лица, разрабатывающие и поставляющие ПО для МИС ЛПУ, — сотрудники фирм–разработчиков и фирм–поставщиков ПО;
(2) лица, разрабатывающие и поставляющие технические средства для МИС ЛПУ, — сотрудники фирм–разработчиков и фирм-поставщиков технических средств и оборудования;

(3) посторонние — лица, не относящиеся ко всем вышеперечисленным категориям.

В модели нарушителя по отношению к внешним нарушителям принимаются следующие ограничения:

- доступ посторонних лиц к информационным и вычислительным ресурсам МИС ЛПУ с территории объектов и из помещений, где расположены технические средства МИС, исключается мерами по охране территории и организации пропускного режима ЛПУ;
- нарушитель не может реализовывать угрозы, зная, что подобные попытки будут обнаружены сотрудниками, сопровождающими и эксплуатирующими МИС ЛПУ, а также лицами, уполномоченными осуществлять контроль доступа к оборудованию и ресурсам МИС;
- возможность установки и использования нарушителем компактных технических средств съема и передачи информации, в том числе замаскированных под штатные технические средства (путем подмены), исключается общережимными мерами по противодействию техническому проникновению на территорию объектов и в помещения, где расположены технические средства МИС ЛПУ.

Принимаются следующие предположения об уровне знаний и возможностях внешнего нарушителя ИБ:

- нарушитель обладает высоким уровнем знаний в области программирования, проектирования и эксплуатации МИС, технико-программного обеспечения в целом;
- нарушитель знает структуру, функции и механизм действия средств защиты, их место в системе ИБ МИС ЛПУ;
- нарушитель правильно представляет функциональные особенности работы МИС ЛПУ, основные закономерности формирования в ней информационных массивов и потоков запросов к ним;
- нарушитель может использовать непреднамеренные действия пользователей МИС ЛПУ (эти действия могут быть как случайными, так и обусловленными необходимостью выполнения пользователями своих служебных обязанностей).

При этом нарушитель может использовать штатные технические средства, входящие в состав МИС ЛПУ (при получении к ним доступа), средства сетевой атаки (при попытках доступа к данным при их передаче по сетям), а также компактные носители информации и технические средства (например, сотовый телефон, беспроводные средства передачи информации и т.п.), непосредственно не относящиеся к СВТ.

4. Подсистема информационной безопасности МИС

Иголка в стогу сена

Однажды Цербер пришел к Диогену за советом:

— У меня есть большая ценность. Посоветуй, как мне надежно укрыть ее от посягательств жадного и нечистого на руку народа?

— А ты положи свою ценность в прочный золотой сейф и запри его прочным алмазным ключом, и не спускай с него глаз ни днем, ни ночью...

— Но Диоген! — вскричал Цербер, — все мое сокровище уйдет на оплату такого хранилища, и что за жизнь будет у меня, если я должен буду караулить его, не смыкая глаз?!!

И предложил Диоген другой вариант:

— Тогда ты спрячь свою драгоценность под один из ста тысяч камней, которые лежат на пляже. Запомни то место и храни это знание в тайне. Вор устанет переворачивать камни, под которыми ничего нет, и не сможет похитить твое сокровище.

Закатные лучи окрашивали седину мудреца в невероятные оттенки пурпура и багрянца...

ПИБ при функционировании МИС обеспечивает защиту информации от несанкционированного доступа и мониторинг за действиями пользователей.

Взаимосвязь ПИБ и МИС представлена схемой (Рис. 7).

ПИБ МИС представляет собой комплекс организационных, технологических, технических и программных мер и средств защиты информации [3]:

- Программные меры защиты информации реализованы программными компонентами и механизмами ПИБ.

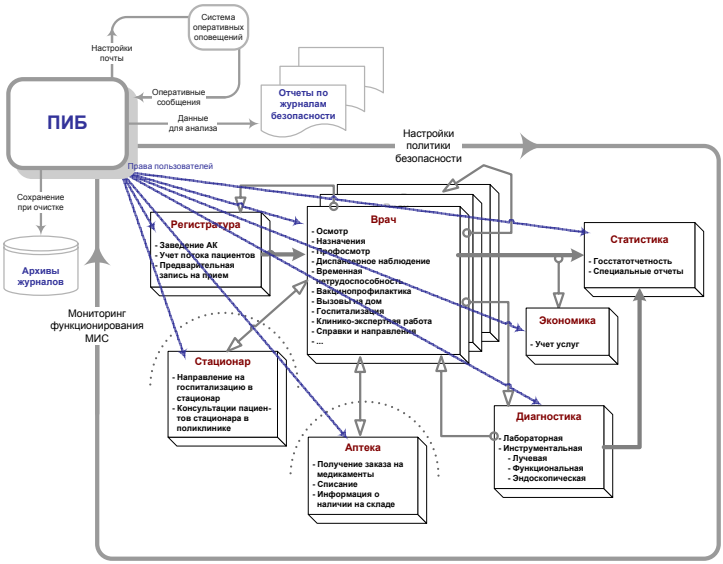

Рис. 7. Структура взаимосвязи компонент ПИБ и МИС

- Технические меры защиты информации обеспечены использованием технических средств защиты. Описание необходимых для использования средств защиты и их настроек приводится в эксплуатационной документации МИС.
- Организационные меры защиты информации обеспечены выполнением персоналом порядков и регламентов для различных действий при эксплуатации МИС. Описание необходимых организационных мер и регламентов работы приводится в эксплуатационной документации МИС.
- Управление полномочиями пользователей, настройка политики безопасности, а также оперативный и ретроспективный контроль действий пользователей МИС и потенциально опасных событий обеспечивается выделенным рабочим местом — АРМ администратора ИБ. Для независимости функционирования от МИС ПО АРМа АИБ строится на системных таблицах БД и для выполнения своих функций использует встроенные механизмы СУБД.

Следующая схема иллюстрирует взаимодействие технических, организационных и программных компонент ПИБ МИС (Рис. 8).

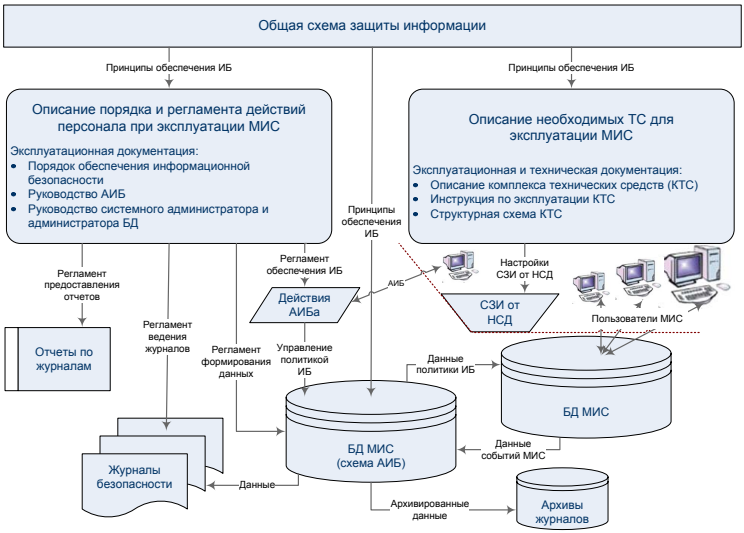

Рис. 8. Взаимодействие технических, организационных и программных компонент ПИБ МИС

5. Опыт внедрения и эксплуатации

Блажен кто верует

Однажды Диоген с Цербером, обнявшись, шли по полю, обозревая окрестности.

Вокруг них, куда ни глянь, громоздились закрытые двери. С замками. Большие двери с большими замками. Маленькие — с маленькими замочками. Большие с маленькими замочками. И маленькие — с большими. И ворота с засовами. Возле некоторых лежали коврики, под коими угадывались контуры ключей. Иные были снабжены аварийными выходами. А какие-то и вовсе стояли в чистом поле, являя собой дверь без забора. Много было дверей и замков много — хороших и разных. И шли мимо них Диоген с Цербером, и было им хорошо.

С требованием обеспечения конфиденциальности данных ИПС РАН как разработчик медицинских информационных систем столкнулся еще в самом начале своей деятельности в области медицинской

информатики — в 1995 году. При разработке МИС Технологии ИНТЕРИН (разработка ИПС РАН, технология создания, адаптации к нуждам конкретного ЛПУ и внедрения МИС ЛПУ) изначально применялись отдельные фрагменты средств информационной защиты в виде общесистемных механизмов [4], [5] и средств СУБД Oracle.

В отдельный самостоятельный блок подсистема информационной безопасности была выделена в рамках реализации специализированного медицинского программного обеспечения для автоматизации деятельности ведомственной амбулатории Главного управления Банка России по Вологодской области в 2005 году.

В настоящее время ПИБ разработки ИПС РАН представляет собой завершенное решение, работоспособное для типовой МИС семейства Интерин.

В статье описана подсистема информационной безопасности, которая была запущена в эксплуатацию почти три года назад. Опыт ее использования позволяет делать выводы об адекватности примененных технологических решений возникающим при функционировании МИС ЛПУ задачам обеспечения информационной безопасности.

Список литературы

[1] Гулиев Я.И., Ермаков Д.Е., Назаренко Г.И. Медицинские информационные системы: теория и практика / Под редакцией Г. И. Назаренко, Г. С. Осипова. — М.: Физматлит, 2005. — 320 с. ↑1

[2] Горбунов П.А., Фохт И.А. Проблемы информационной безопасности в медицинских информационных системах - теоретические решения и практические разработки // Тр. междунар. конф. «Программные системы: теория и приложения», ИПС РАН, Переславль-Залесский, 2006: В 2 т. / Под ред. С.М. Абрамова. — М.: Наука. Физматлит, 2006. — т.1 с.107-112 с. ↑3.1

[3] Горбунов П.А., Гулиев Я.И., Михеев А.Е., Назаренко Г.И., Фохт И.А., Фохт О.А. Проблемы информационной безопасности в медицинских информационных системах — теоретические решения и практические разработки // Врач и информационные технологии № 4, 2007. — 39-43 с. ↑4

[4] Малых В.Л., Пименов С.П., Хаткевич М.И. Объектно-реляционный подход к созданию больших информационных системх // Программные системы: Теоретические основы и приложения. / Под ред. А.К. Айлмазяна. — М.: Наука. Физматлит, 1999. — 177 с. ↑5

[5] Гулиев Я.И., Комаров С.И., Малых В.Л., Осипов Г.С, Пименов С.П, Хаткевич М.И. Интегрированная распределенная информационная система лечебного учреждения (Интерин) // Программные продукты и системы, 1997. ↑5

Исследовательский центр медицинской информатики ИПС РАН

Ya. I.–O. Guliev, I. A. Vogt, O. A. Vogt, A. J. Belyakin. *Healthcare Information System and Information Safety. Problems and solutions* // Proceedings of Program Systems institute scientific conference "Program systems: Theory and applications". — Pereslavl-Zalesskij, v. **2**, 2009. — p. 175–206. — ISBN 978-5-901795-18-7 (*in Russian*).

Abstract. The article describes results of the theoretical research and developments of the Medical Informatics Research Center PSI RAS applicable to the information security providing for healthcare information systems. Data composition, primary threats and approaches to a data protection were examined.