Особенности решения проблем информационной безопасности в медицинских информационных системах

Назаренко Г.И., Михеев А.Е.
Медицинский центр Банка России, г. Москва, Россия
Горбунов П.А.
ГУ Банка России по Вологодской области, г. Вологда, Россия
Гулиев Я.И., Фохт И.А., Фохт О.А.
Институт программных систем РАН, г. Переславль-Залесский, Россия
e-mail: medicina2007@vogt.botik.ru

В докладе представлены результаты совместных исследований и разработок Банка России (БР), и Института программных систем Российской академии наук (ИПС РАН) в области обеспечения информационной безопасности в медицинских информационных системах. Предлагается общая схема защиты с учетом специфики медицинской информации, ее состава и участников ее обработки.

Ключевая слова: информационная безопасность, сохранность данных, несанкционированный доступ, медицинская информационная система, врачебная тайна.

Одна из главных проблем при создании медицинских информационных систем (МИС) является обеспечение информационной безопасности. При этом внимание уделяется как данным о здоровье пациентов и ходе лечебно-диагностического процесса, содержащимся в МИС, так и информации, составляющей сущность самой МИС – кодам ее модулей, организации хранения и обработки данных, содержимому общесистемных справочников и пр. Информационная безопасность (ИБ) обеспечивается защитой информации от несанкционированного доступа, а также от утраты и искажения данных.

Особенностью медицинской информации является ее конфиденциальность. Права граждан на конфиденциальность информации о факте обращения ко врачу и иных передаваемых ими при обращении за медицинской помощью сведений 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). Ряд данных, вводимых, обрабатываемых и хранимых в процессе функционирования медицинских информационных систем, являются персональными данными или могут составлять врачебную тайну.

Кроме того, база данных медицинской информационной системы содержит критически важную информацию, от которой, зачастую, может зависеть жизнь человека, поэтому ключевым фактором при создании МИС должно стать обеспечение целостности базы данных, а также возможность слежения за состоянием самой системы и ее безопасностью.

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.

На компромиссе, с учетом специфики работы ЛПУ как системы массового обслуживания, должна основываться концепция информационной безопасности МИС.

ОСОБЕННОСТИ МЕДИЦИНСКОЙ ИНФОРМАЦИИ

Для определения оптимального уровня информационной безопасности МИС необходимо исследовать специфику медицинской информации, изучить ее состав и определить участников ее обработки.

Авторами выделены следующие особенности медицинской информации, как сведений ограниченного распространения:

1. Медицинская информация, являясь порожденной личной тайной пациента, полностью находится в его распоряжении. То есть, он свободно может распоряжаться ею, предоставляя безо всякого ограничения любым третьим лицам.
2. Существует довольно жесткий временной регламент на работу с медицинскими документами, направленный на своевременность оказания медицинской помощи, сокращение т.н. «рабочего времени больного», удовлетворенность пациентов оказываемой медицинской помощью, ускорение оборачиваемости койки и улучшение полезного использование дорогостоящего медицинского оборудования.

   Ухудшение названных показателей (в частности, своевременности медицинской помощи) по причине усиления режима конфиденциальности информации в ущерб доступности данных для профессионалов может создать угрозу здоровью, а иногда и жизни больного, приведет к большим финансовым затратам, возникновению дополнительных юридических исков к ЛПУ со стороны пациентов и их родственников.
3. Медицинская информация может быть разделена на фрагменты – персональные данные (позволяющие однозначно идентифицировать пациента), информация о состоянии его здоровья, рекомендации и назначения, информация о проведенном лечении, статистические данные.

   Конфиденциальную информацию составляет только объединение всех или многих фрагментов данных. Тогда как отдельно, сами по себе, фрагменты медицинской информации тайны не составляют. Так, информация о диагнозе, о ходе заболевания и лечения может быть опубликована в открытой печати (медицинские статьи) даже в совокупности с фрагментами персональных данных (пол, возраст, принадлежность к группе), но без ФИО пациента. Медицинская информация о диагнозах, о количестве обращений, о нетрудоспособности вместе с данными о групповой принадлежности (регион проживания, пол, возрастная группа и пр.) составляют статистическую информацию, также не являющуюся конфиденциальной.
4. Как правило, отдельные фрагменты медицинской информации обрабатываются разными персоналиями ЛПУ – регистратор, врач, диагност, медсестра, статистик, лаборант и пр. Более того, многие из этих фрагментов могут обрабатываться по отдельности, представляя собой информацию, не ассоциированную однозначно с тем или иным человеком. Например, материал для анализа, а впоследствии и результат анализа может привязываться лаборантом к номеру медкарты (штрих-коду, уникальному ключу и пр.), и при этом не происходит идентификации персоны, которой медкарта принадлежит.

   Такой подход часто используется отдельными службами ЛПУ или в отношении отдельных пациентов (VIP-пациенты) – там, где анонимность или конфиденциальность особенно важны.

   В МИС эта идея может получить развитие и большую эффективность, так как информационная система позволяет выделять каждому своему пользователю полномочия на обращение к фрагментам медкарты, где будет содержаться только предназначенные для него категории данных.
5. При работе с медицинской информацией могут возникать угрозы трех типов: несанкционированное получение доступа к данным (нарушение конфиденциальности), утрата информации, а также искажение данных.

   В результате разглашения информации и здоровье пациента ему может быть нанесен ущерб, т.к. возможно злонамеренное использование этих сведений, а кроме того, нарушается право на тайну личной жизни.

   В результате утраты медицинских данных на их восстановление может быть потеряно время тогда, когда эти данные (информация о реакции на лекарства, об аллергии, о перенесенных заболеваниях, о показателях здоровья, о назначенном лечении и пр.) окажутся необходимыми для спасения жизни человека.

Искажение данных – вследствие ошибки, а тем более, злонамеренное – я является самой опасной угрозой для медицинской информации, т.к. наличие ошибочной информации медицинского характера (неверные назначения, неверные результаты исследований, неверные данные о переносимости лекарств и пр.) представляют непосредственную опасность для жизни и здоровья человека.

6. Взаимоотношения медиков, пациентов и их доверенных лиц/родственников не проработаны юридически. Законодательством на сегодняшний день не регламентируется принципиальный вопрос о необходимости сообщать сведения о здоровье больного самому пациенту или его доверенным лицам (даже без его согласия!) в случаях тяжких заболеваний, когда такие известия могут нанести вред состоянию здоровья больного.

   Представляется сомнительным, чтобы эти отношения были формально урегулированы с правовой точки зрения в обозримом будущем, т.к. данная ситуация слишком деликатна и индивидуальна, чтобы не оставлять ее на рассмотрение врача каждый раз, а единожды определить законодательно.

Все вышеуказанные особенности определяют политику безопасности для медицинской информационной системы.

ВОЗМОЖНЫЕ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В МИС

Информационная безопасность при функционировании медицинской информационной системы обеспечивается за счет взаимоувязанного комплексного использования организационных мер, программных и технических средств защиты.

Перечислим основные направления возможных нарушений ИБ:

- утечка данных (нарушение конфиденциальности – полное при получении злоумышленником доступа к БД или частичное – при получении злоумышленником доступа к не разрешенной для него информации);
- утрата данных (разрушение носителей, стирание информации при непосредственном доступе к данным или посредством Системы);
- несанкционированная модификация данных (посредством Системы или при непосредственном доступе к БД);
- отказ в предоставлении функциональности (в связи с повреждением Системы);
- некорректное функционирование Системы (вследствие несанкционированного изменения модулей Системы).

ОБЩАЯ СХЕМА ЗАЩИТЫ

На основе результатов исследований была предложена схема защиты данных, в которой используются:

- Элементы среды функционирования МИС (режим допуска сотрудников в ЛПУ, выделенные помещения под сервера СУБД, технические средства защиты от несанкционированного доступа (НСД), регламент обслуживания ПО МИС, возможности операционной системы по разграничению прав доступа к файлам МИС, возможности СУБД по санкционированию доступа к данным и пр.).
- Подсистема информационной безопасности (ПИБ) МИС. Общесистемные механизмы (тонкая организация санкционированного доступа к фрагментам медицинской информации, к объектам и функционалу МИС, а также контроля жизненного цикла информации и целостности кода модулей МИС).
- ПИБ МИС. Выделенное независимое рабочее место администратора информационной безопасности (АРМ АИБ), обеспечивающее оперативный контроль и ретроспективный анализ действий пользователей МИС.

В Технологии ИНТЕРИН построения медицинских информационных систем (разработка ИПС РАН) на уровне программного обеспечения защита данных МИС строится следующим образом:

1. **Ограничение доступа к файлам системы** на необходимым минимальном уровне обеспечивается операционной системой компьютеров, на которых располагаются фрагменты Системы (Sun/Solaris, Intel/WinServer 2003).

2. **Организация санкционированного доступа к данным** на уровне БД обеспечивается системой управления базами данных (СУБД Oracle Server).
3. **Вопросы безопасности на уровне МИС** (в МИС Технологии ИНТЕРИН) решаются с помощью общесистемных механизмов, которые позволяют:
   - Идентифицировать и аутентифицировать пользователя при входе в МИС.
   - Более тонко организовать санкционированный доступ с использованием механизма метапользователей и информационных объектов, дублируя, в какой-то мере контроль доступа со стороны БД. Доступ при этом задается как для групп пользователей, так и для отдельных пользователей, как к отдельным объектам. Так и к их группам или фрагментам.
   - Контролировать жизненный цикл информации при помощи механизма историчности.
   - Предотвращать возможность доступа к БД сторонними средствами в обход Системы с помощью механизмов предотвращения непосредственного доступа к БД с паролем пользователя, а также механизма контроля целостности кода модулей МИС.
   - Предотвращать возможность отказа в предоставлении функциональности поврежденными модулями Системы или вредоносных действий с данными при помощи сторонних программных средств при помощи механизма контроля целостности кода модулей МИС.
   - Подтвердить авторство того или иного медицинского документа, сформированного в Системе при помощи функции регистрации оператора.
4. **Функции контроля за действиями и полномочиями пользователей** выносятся в отдельный блок – Рабочее место администратора информационной безопасности. Модуль позволяет контролировать действия пользователей в режиме реального времени, проводить ретроспективный анализ, а также оперативно оповещать администратора ИБ о попытках информационных атак. Данный программный блок должен быть максимально независим от программного обеспечения Системы. Поэтому он строится на системных таблицах БД ORACLE и для выполнения своих функций пользуется встроенными механизмами аудита СУБД.

ЗАКЛЮЧЕНИЕ

Предлагаемые решения по организации информационной безопасности функционирования медицинских информационных систем позволяют обеспечить приемлемый уровень информационной защиты, без существенных ограничений пользователей МИС в их действиях.

ЛИТЕРАТУРА

1. Горбунов П.А.,.Фохт И.А. Проблемы информационной безопасности в медицинских информационных системах - теоретические решения и практические разработки Программные системы: теория и приложения / Под редакцией С.М. Абрамова. В двух томах. — М.: Физматлит, 2006, т.1 с.107-112
2. Назаренко Г.И., Гулиев Я.И., Ермаков. Д.Е. Медицинские информационные системы: теория и практика. Под редакцией Г. И. Назаренко, Г. С. Осипова. Москва: ФИЗМАТЛИТ, 2005. — с.320 — ISBN 5-9221-0594-9
3. 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 №3, 1997