ИНФОРМАТИКА

2008 **октябрь-декабрь** **№ 4**

УДК 004.056:061.68

Д.Л. Можейко, К.Г. Киселев

РЕАЛИЗАЦИЯ ПОДСИСТЕМЫ БЕЗОПАСНОСТИ В МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ «КЛИНИКА»

Рассматриваются преимущества и недостатки различных подходов к регистрации пользователей в информационных системах на основе баз данных. Проводится обзор подсистем распределения прав доступа ведущих российских медицинских информационных систем. Описывается реализация управления доступом к объектам на примере информационной системы лаборатории медицинского учреждения. Рассматриваются перспективы использования электронной цифровой подписи в медицинских информационных системах.

Введение

Многие медицинские учреждения применяют или планируют применять в своей деятельности системы на базе современных информационных технологий. Однако при использовании информационных технологий в медицине возникает ряд проблем в области обеспечения информационной безопасности. Легкость и доступность информации, которые принесли с собой компьютерные технологии, имеют и свою обратную сторону: использование компьютеров резко обострило проблемы сохранности и конфиденциальности данных. Утечка данных в медицинских информационных системах (МИС) постепенно переходит в разряд насущных проблем сферы здравоохранения.

По данным компании InfoWatch, за последние два года каждое второе медицинское учреждение допустило утечку информации о пациентах [1]. Основные факты утечки информации происходят не по каналам связи, а через конкретных людей, которые выносят сведения за пределы учреждения [2]. В связи с этим актуальными представляются следующие задачи: регистрация пользователей в системе, разграничение прав доступа к информации и подписание электронного документа.

Описанные ниже вопросы рассматриваются на примере разработанной в Объединенном институте проблем информатики НАН Беларуси медицинской информационно-аналитической системы «Клиника».

1. Регистрация пользователей в системе

Каждый пользователь МИС имеет учетную запись, для которой соответствующим образом настроены полномочия. Полномочия могут объединяться в роли и назначаться пользователям с одинаковыми обязанностями.

Существуют два подхода для регистрации пользователей: с разграничением полномочий на уровне СУБД и с разграничением полномочий на уровне приложения.

Разграничение полномочий на уровне СУБД. При создании учетной записи пользователя используется стандартный механизм безопасности используемой в МИС СУБД – полномочия отслеживаются на уровне доступа к объектам сервером БД. Достоинством этого подхода является мощный механизм ведения пользователей, предоставляемый разработчиками СУБД, а недостатком – малая гибкость при определении полномочий объектов (полномочия задаются на физические объекты БД).

Разграничение полномочий на уровне приложения. За регистрацию пользователя отвечает отдельный модуль клиентского приложения; полномочия задаются для логических объектов системы, и их ведение осуществляется приложением. При таком подходе обеспечивается большая гибкость при настройке – возможность задавать полномочия на семантически определенные объекты и определять произвольные уровни доступа. Однако механизм регистрации пользователей должен быть реализован разработчиками МИС. При этом возникает проблема при подключении приложения к БД. Поскольку все подключения производятся под одним

именем пользователя и паролем, данные этой учетной записи должны в явном виде задаваться в приложении или храниться в настроечных файлах. В случае хранения этих данных прямо в коде приложения и при смене пароля рабочей учетной записи СУБД (что рекомендуется делать регулярно) возникает необходимость перекомпиляции приложения. Это крайне нежелательно, так как смена пароля – администраторская функция, пригодная к выполнению силами заказчика, в то время как перекомпиляция приложения – дело разработчиков. Следовательно, при такой реализации МИС будет неспособна функционировать без ущерба для своей безопасности без помощи разработчиков. Хранение же данных подключения к БД в настроечном файле делает их доступными любому пользователю, что с точки зрения безопасности еще более неприемлемо. Выход из этой ситуации такой: хранить данные подключения в настроечном файле в зашифрованном виде, а ключевое слово для шифрации явно задавать в коде приложения.

В разработанной МИС «Клиника» используется именно такой подход, т. е. приложение работает с базой данных под одним (единым) пользователем. При этом в базе данных хранится список пользователей, которым разрешен доступ к приложению. После аутентификации пользователя загружается соответствующий ему набор библиотек и ведется протоколирование.

2. Управление доступом к объектам

Общим подходом для всех моделей управления доступом является разделение множества сущностей, составляющих систему, на множества объектов и субъектов. Будем подразумевать, что объекты являются некоторыми контейнерами с информацией, а субъекты – пользователями, которые выполняют различные операции над этими объектами.

2.1. Базовые модели

Безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с заданным набором правил и ограничений, которые образуют политику безопасности.

Одна из особенностей МИС состоит в большом количестве объектов и разнообразии прав доступа к ним, что существенно усложняет администрирование системы [3, 4].

Выделяют три основные модели управления доступом к объектам: мандатную, дискреционную и ролевую. Ролевая модель контроля доступа является компромиссным решением, обеспечивающим неплохие возможности в задании политики безопасности при достаточной простоте администрирования [5]. Это позволяет рассматривать ролевую модель как наиболее подходящую для применения в прикладных программах.

Суть ролевого управления доступом состоит в том, что между пользователями и их привилегиями появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права.

2.2. Реализация подсистемы распределения прав доступа в существующих МИС

Задача разграничения доступа к информации в МИС имеет ключевое значение. Для этого есть две причины:

1. Хранящаяся информация в МИС является базисом для принятия решения лечащим врачом. От ее корректности зависит, насколько верным будет решение, а это влияет на здоровье и даже жизнь пациента. Поэтому крайне важно разграничить доступ к внесению и изменению этой информации.

2. Информация в МИС является конфиденциальной, и ее разглашение может причинить ущерб пациенту. В связи с этим даже просмотр документов в МИС должен быть разрешен только тем пользователям, чьи служебные обязанности того требуют.

Большинство разработчиков МИС включают в базовый состав своих систем модули для обеспечения безопасности и целостности данных. Так, в системе Интерин распределение прав доступа осуществляется на основании поддержки иерархического аппарата метапользователей с наследованием полномочий. Метапользователь – это понятие, объединяющее множество исполнителей и использующееся для наделения их одинаковыми правами. Конкретный исполнитель может одновременно относиться к нескольким метапользователям и обладать суммарны-

ми правами. Все элементы системы реализованы в виде информационных объектов, для которых определяются режимы владения, делегирования и пересылки. Безопасность на уровне данных обеспечивается средствами Oracle. Для фиксирования всех действий пользователей ведется журнал транзакций [6, 7].

В МИС «Кондопога» система распределения прав представлена трехмерной моделью. На оси X отображаются уровни доступа к объектам: «нет доступа», «только чтение», «чтение и изменение», «модификация на уровне кода», «администрирование», на оси Y – иерархия прав на доступ к системе: «нет доступа», «немедицинские работники», «врачи», «администраторы» и др., на оси Z – специальности пользователя, группы по специальности (например, группа «врачи» включает терапевтов, хирургов, гинекологов и др.). Организация распределения прав доступа построена на основе групп. Зарегистрированные в системе пользователи включаются в группы. В списке доступа каждого объекта указываются группы, которым разрешен доступ, и уровень этого доступа.

2.3. Реализация подсистемы распределения прав доступа в МИС «Клиника»

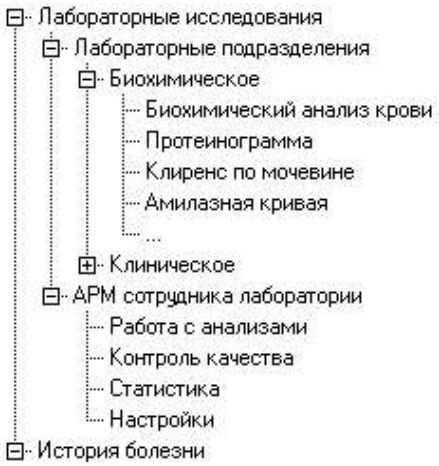
Перед авторами стояла задача разработать модель управления доступом к объектам системы, позволяющую реализовывать максимально удобную в администрировании политику безопасности приложения. Исходя из сравнительной простоты администрирования, модель разграничения прав доступа на основе ролей является наиболее предпочтительной к использованию в прикладных программах [5].

Разработанную модель распределения прав доступа рассмотрим на примере клинико-диагностической лаборатории медицинского учреждения.

В данной модели все объекты системы объединяются в единое дерево. У каждого объекта, кроме корневого, есть один родительский объект и любое количество дочерних. Роль может быть назначена пользователю в контексте любого объекта. Таким образом, любой объект приложения может образовать домен, в который будут входить он сам и все его дочерние объекты. Любой из дочерних объектов может также образовать домен, являющийся подчиненным по отношению к домену родительского объекта.

Например, корневой объект «лабораторные исследования» имеет подчиненные объекты «лабораторные подразделения» (например, биохимическое, клиническое), каждый из которых включает определенные анализы, относящиеся к определенному подразделению (рисунок).

Тогда пользователь, которому назначена роль «начальник» в контексте конкретного подразделения, имеет полный доступ ко всем анализам своего подразделения, но не имеет доступа к исследованиям других подразделений, так как там он не играет соответствующей роли. Пользователь же, являющийся начальником корневого объекта системы, имеет полный доступ ко всем исследованиям лаборатории.



Иерархия объектов клинико-диагностической лаборатории

В системе определен набор из пяти основных уровней доступа к объектам: «полный», «изменение», «создание», «только чтение» и «скрыть». Для объектов, не предназначенных для изменения (статистика, контроль качества), используется сокращенный набор уровней доступа: «только чтение» и «скрыть».

Ограничение на доступ к информации организовано так, что ненужные документы пользователь не видит, поэтому и не может выполнять недопустимые действия.

Правом на удаление объекта обладает субъект, создавший данный объект. Поэтому для большинства объектов системы фиксируется их создатель.

Для электронных документов, создание и изменение которых происходит в различных отделениях, применяется модель переходящего владельца. Типичным примером такого документа является «лабораторный анализ», направление на который создается медсестрой или врачом лечебного отделения, а наполнение результатами исследования (изменение) осуществляется сотрудниками лаборатории.

Для выяснения текущего состояния документа используется признак «статус документа». Тогда в каждый момент времени медицинский документ имеет одно из определенных состояний (например: «создан», «в работе», «подписан», «удален»), что указывает на его актуальность. Документ, утративший свою актуальность, не удаляется из системы (помечается признаком «удален»), так как на него могут быть ссылки и его нужно показать при доступе по ссылке из других документов. Так, при статусе документа «создан» медсестра, создавшая направление на лабораторный анализ, имеет право его удалить, а как только статус документа изменен на «в работе» или «проведен», право на удаление данного документа переходит к сотруднику лаборатории, который проводит исследование.

В системе «Клиника» привилегии определяются типовой ролью (описывает полномочия группы пользователей одной специализации, обладающих одинаковыми правами по отношению к информации) и элементарными привилегиями (вносят дополнительные коррективы в стандартное меню какой-либо типовой роли). Привилегии пользователю выделяет администратор информационной безопасности.

3. Протоколирование рабочего процесса

Наличие системы четкого протоколирования рабочего процесса позволяет проследить всю историю изменения данных.

В журнале протоколирования лабораторных исследований фиксируются три события: создание, изменение и удаление. Для каждого события учитываются его время и исполнитель. Для события «изменение» в журнал вносится дополнительная информация.

Шаблон записи на изменение лабораторного исследования:

Edit (время записи в БД; код пользователя, производившего запись; код врача-лаборанта; код фельдшера-лаборанта; признак CITO исследования; n(код показателя – значение показателя), где n – число показателей в лабораторном исследовании).*

Пример записи в журнале протоколирования:

Edit (24.12.07 12:35; 165; 172; 176; 1; 1-5,6; 3-128; 24-146,2; 27-3,46; 31-17; 32-5,46).

Таким образом, для любого исследования можно проследить историю его изменения и при необходимости восстановить результаты.

4. Электронно-цифровая подпись как средство легализации медицинского электронного документа

Одной из основных задач, без решения которых полноценная компьютеризация здравоохранения невозможна, является определение юридического статуса электронных медицинских документов [8].

История болезни является основным документом, по которому можно судить, получил ли пациент надлежащее лечение. В ней содержится информация о действиях медицинских работников и основаниях для этих действий. Для медицинского работника, втянутого в судебное

разбирательство, содержание истории болезни может быть защищающим или инкриминирующим фактором.

Рассмотрим на примере истории болезни несколько ситуаций, которые на сегодняшний момент могут поставить врача в затруднительное положение:

1. Медицинский документ сформирован в электронной форме, затем распечатан, подписан и подклеен в традиционную историю болезни. История болезни, содержащая этот документ, зачастую недоступна или труднодоступна, однако врач может найти его электронный аналог в электронном архиве. Это значительно повышает информированность врача, но никакими нормативными документами не определено, имеет ли он право принять важное медицинское решение на основании электронной версии медицинского документа.

2. Анализы, выполненные в другом (удаленном) подразделении, распечатываются, подписываются и попадают к лечащему врачу со значительным опозданием. С другой стороны, их электронные версии становятся доступны значительно раньше. Врач может их распечатать, однако не может использовать (в частности, подклеить в историю болезни), так как на них нет обязательной подписи лица, выполнившего анализы.

С одной стороны, классическая история болезни не соответствует нынешнему времени (взрывной рост числовых показателей, коллективная работа, высокая скорость оборота информации, телемедицина и т. д.). С другой стороны, электронные системы пытаются полностью подстроиться под идеологию традиционных бумажных технологий: распечатали документ, подписали, подшили в историю болезни. На сегодняшний день юридическая сила электронных документов, хранящихся в большинстве используемых МИС, не обеспечена. Таким образом, возможности электронных (безбумажных) технологий в медицине не используются в полной мере, так как их статус не определен.

В настоящее время одним из лучших решений для обеспечения неизменности и достоверности данных является использование электронной цифровой подписи (ЭЦП).

ЭЦП – реквизит электронного документа, предназначенный для защиты электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

Для признания ЭЦП необходимо наличие в информационных системах сертифицированных программно-технических средств, обеспечивающих идентификацию подписи, и соблюдение установленного режима их использования. Сложность сертификации ЭЦП приводит к использованию разработчиками МИС готовых решений ЭЦП.

В Республике Беларусь задачи по формированию нормативной и аппаратно-программной базы для широкого внедрения ЭЦП в электронный документооборот планируется выполнить в 2007–2008 гг. в рамках программы «Электронная Беларусь».

Заключение

Одна из особенностей МИС состоит в большом количестве информационных объектов и разнообразии прав доступа к ним, что существенно усложняет администрирование системы. Модель разграничения прав доступа на основе ролей является наиболее предпочтительной к использованию в прикладных программах, так как добавление/удаление пользователей не связано с процессом добавления/удаления ролей и уровней доступа. При изменении прав у группы пользователей нет необходимости модифицировать права у каждого из них, достаточно сменить права на доступ у роли.

Разработанная модель управления доступом позволяет создавать простые в администрировании политики безопасности, обеспечивая необходимый уровень защиты информации. В ней осуществлена привязка пользовательских полномочий к иерархии объектов системы. Подобная привязка позволяет ограничить область действия выданных пользователю полномочий и как следствие упростить схемы доступа к объектам.

Надежная защита информации может быть реализована только в случае, когда организационные мероприятия и технические средства защиты опираются на прочную правовую базу в области использования информационных систем.

Наличие в МИС сертифицированных программно-технических средств, идентифицирующих подпись, позволило бы наилучшим образом обеспечить неизменность и достоверность данных. В дальнейшем планируется расширение подсистемы безопасности до использования ЭЦП.

Список литературы

1. Граванова, Ю. Информационные системы и проблема защиты данных / Ю. Граванова // Cnews. Издание о высоких технологиях [Электронный ресурс]. – 2006. – Режим доступа : http://www.cnews.ru/reviews/free/national2006/articles/datasecure/. – Дата доступа : 03.03.2008.

2. Лукашев, В.М. Внутренняя безопасность информационных систем / В.М. Лукашев // Управление защитой информации. – 2004. – Т. 8, № 2. – С. 183–187.

3. Медицинские информационные технологии и системы / С.В. Абламейко [и др.]. – Минск : ОИПИ НАН Беларуси, 2007. – 176 с.

4. Гулиев, Я.И. Интегрированная распределенная информационная система лечебного учреждения (Интерин) / Я.И. Гулиев [и др.] // Программные продукты и системы. – 1997. – № 3.

5. Майоров, А.В. Улучшенная ролевая модель доступа к объектам / А.В. Майоров // Моделирование и анализ информационных систем. – 2007. – Т. 11, № 2. – С. 22–32.

6. Гулиев, Я.И. Медицинская информатика в ИПС РАН / Я.И. Гулиев // Программные системы: теория и приложения. В 2 т. ; под ред. С.М. Абрамова. – М. : Физматлит, 2004. – Т. 1. – С. 59–100.

7. Проблемы информационной безопасности в медицинских информационных системах – теоретические исследования и практические разработки / И.А. Фохт [и др.] // Программные системы: теория и приложения. В 2 т. ; под ред. С.М. Абрамова. – М. : Физматлит, 2006. – Т. 1. – С. 107–112.

8. Эльянов, М. Что делать? Или двадцать шестой сон Веры Павловны / М. Эльянов // PC Week [Электронный ресурс]. – 2007. – Режим доступа : http://www.pcweek.ru/themes/detail.php?ID=103279. – Дата доступа: 03.03.2008.

Поступила 22.04.08

Объединенный институт проблем информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: mdl@newman.bas-net.by

D.L. Mozheyko, K.G. Kiselev

INFORMATION SECURITY IMPLEMENTATION IN THE MEDICAL INFORMATION SYSTEM «KLINIKA»

The implementation of medical information systems has been hindered by inadequate security support. Strong points and disadvantages of various approaches to registration of users in information systems utilizing database technologies are considered. The access control subsystems in leading Russian medical information systems are reviewed. Implementation of the access control to objects on an example of laboratory information system of hospital scale is described. Actual questions of the electronic document implementation and the prospects of the usage of electronic digital signature in medical information systems are considered.