УДК 004.056

РАЗРАБОТКА СРЕДСТВА АДМИНИСТРИРОВАНИЯ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА ДЛЯ ТИПОВОЙ МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Е.А. Оленников, к.т.н., доцент, olennikov@utmn.ru;
А.А. Захаров, д.т.н., профессор, azaharov@utmn.ru;
В.В. Варнавский, ассистент кафедры, vvv_90_08@mail.ru
(Тюменский государственный университет, ул. Перекопская, 12а, г. Тюмень, 625003, Россия);
А.А. Оленников, к.т.н., доцент, oaa@cirkul-m.ru
(Сибирский государственный индустриальный университет, ул. Кирова, 42, г. Новокузнецк, Кемеровская обл., 654007, Россия)

Аннотация. Статья посвящена разработке инструмента для администрирования системы контроля доступа для типовой медицинской информационной системы. В начале работы сформулированы проблемы разграничения доступа в медицинские информационные системы и задача, решение которой авторы видят в разработке средств для администрирования системы контроля и управления доступом в данных системах. Во второй части работы авторы предлагают инструмент администратора типовой медицинской информационной системы, описывают его, а в конце делают вывод об эффективности использования предложенного средства.

Ключевые слова: *информационная безопасность, защита информации, разграничение доступа, медицинские информационные системы, авторизация, защита данных, база данных, медицинская тайна.*

В настоящее время в учреждениях здравоохранения идет активный процесс внедрения *медицинских информационных систем* (МИС), количество которых ежегодно только увеличивается [1, 2].

Информация, обрабатываемая в МИС, является конфиденциальной, а процесс разграничения доступа к ней имеет специфичный характер в силу двух причин.

Во-первых, зависимость прав доступа от следующих факторов:

– времени доступа к данным: по истечении определенного времени доступ на изменение ранее сделанной записи должен быть закрыт;

– текущих взаимоотношений врач–пациент–лечащий врач: на время лечения пациента должен быть доступ к его медицинским данным в полном или ограниченном объеме;

– статуса пациента: доступ к информации ряда пациентов должен быть ограничен независимо от других факторов;

– места пребывания пациента: некоторые сотрудники подразделения, в которое переводится пациент, должны получать доступ к медицинским данным пациента в полном или ограниченном объеме;

– степени конфиденциальности информации: доступ к некоторым медицинским данным пациента должен быть открыт только узкому кругу лиц независимо от других условий.

Во-вторых, большое количество защищаемых объектов: доступ в МИС должен ограничиваться не только на уровне таблиц, но и на уровне записей [3–5].

Необходимо также принять во внимание требование предоставлять врачу доступ только к строго ограниченному объему информации о пациенте, которая ему нужна в данный момент времени для выполнения своих должностных обязанностей.

Таким образом, для обеспечения данного требования с учетом особенностей, указанных выше, необходимо практически постоянно переопределять права доступа пользователей МИС к данным пациента [6].

Учитывая огромное количество защищаемых объектов и субъектов в МИС, можно сделать вывод, что обеспечить такой режим работы штатными средствами довольно затруднительно.

В работе [7] авторы, основываясь на требованиях к разграничению доступа в МИС, предлагают модель системы безопасности обобщенной МИС и основанную на ней систему контроля и управления доступом, однако проблема администрирования разработанной системы рассматривается поверхностно.

Таким образом, актуальной задачей является разработка средства администрирования системы контроля управления и разграничения доступа для типовой медицинской информационной системы, предложенной в [7].

Предлагается консоль администратора, разработанная на языке C#. Эта консоль является основным средством администратора безопасности по управлению системой контроля и разграничения доступа.

Разработанный механизм администрирования позволяет удаленно управлять настройками любой БД, находящейся на сервере под управлением СУБД MS SQL Server, путем указания пути к БД и способу аутентификации в соответствующем файле настроек, имеющем следующую структуру:

```
[SqlServer]
ServerName=MyServer
User=MISUser
Password=qwerty1234
DataBase=MIS
```

Изменяя соответствующие поля в данном файле, администратор меняет строку подключения к серверу баз данных. В поле ServerName указывается имя экземпляра сервера MS SQL Server, на котором располагается база данных. Поле User содержит информацию об имени входа пользователя БД, обладающего правами администратора. В Поле Password необходимо указать пароль пользователя. Поле Database содержит информацию о БД, используемой в МИС.

Разработанная консоль администратора позволяет выполнять ряд стандартных функций по управлению БД, в том числе управление учетными записями и группами (рис. 1), управление листами контроля доступа, управление ролевой политикой.

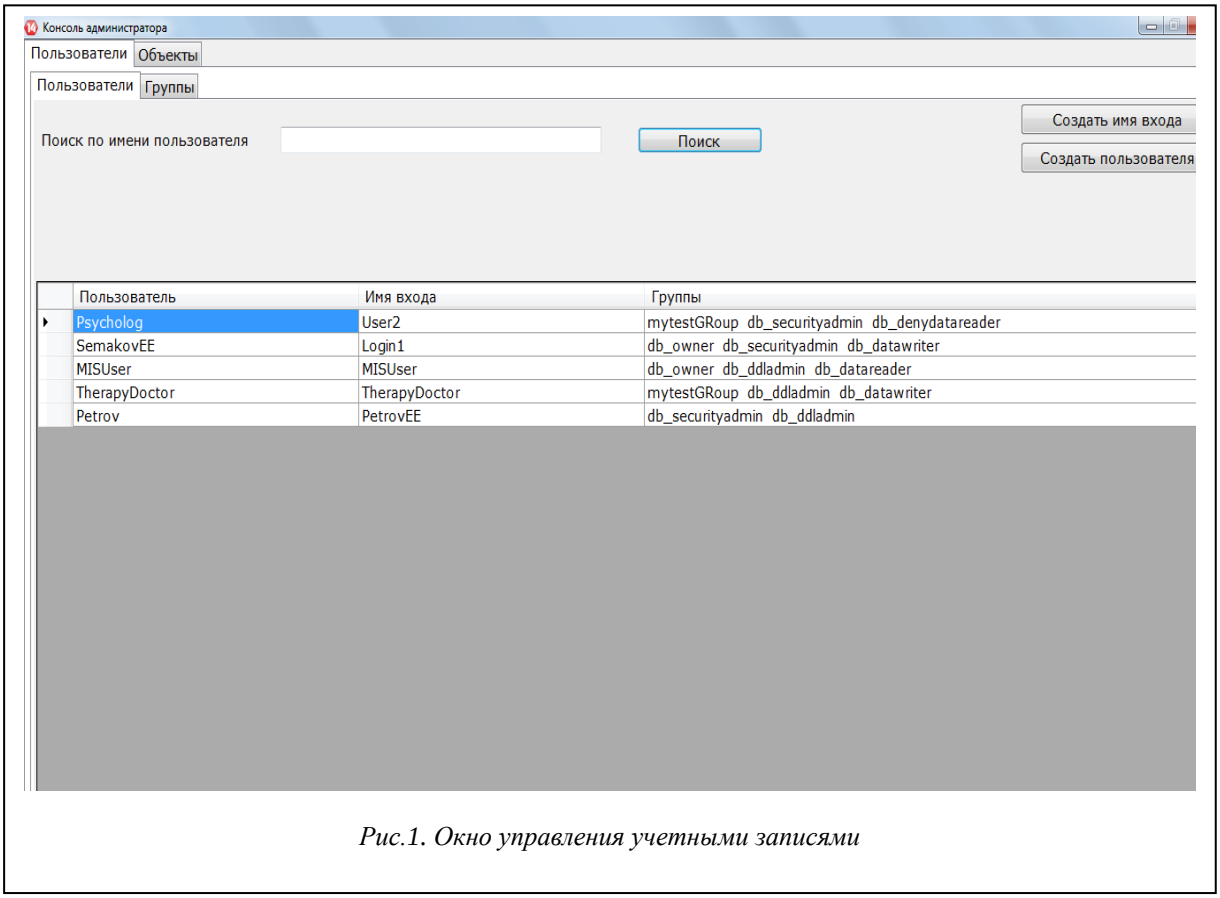

Рис.1. Окно управления учетными записями

В консоли администратора имеется возможность задать время доступности любого объекта (рис. 2) в соответствии с моделью доступа, предложенной в [7]. Предусмотрено включение/выключение временной политики напрямую из консоли администратора путем обращения к соответствующим триггерам, созданным на уровне СУБД.

Предлагаемое средство администрирования позволяет осуществлять управление политикой уровней безопасности. Предусмотрены возможность разграничения полномочий групп пользователей, а также включение/отключение указанной политики.

Таким образом, предлагаемое средство администрирования системы контроля доступа для типовой медицинской системы является инструментом администратора безопасности, позволяющим как выполнять стандартные операции по администрированию баз данных, так и централизованно управлять системой разграничения доступа, предложенной в [7].

На взгляд авторов, использование данного средства позволит сократить время, необходимое администратору безопасности МИС для изменения прав субъекта, благодаря возможности перемещения пользователей между группами, а также изменения меток конфиденциальности групп.

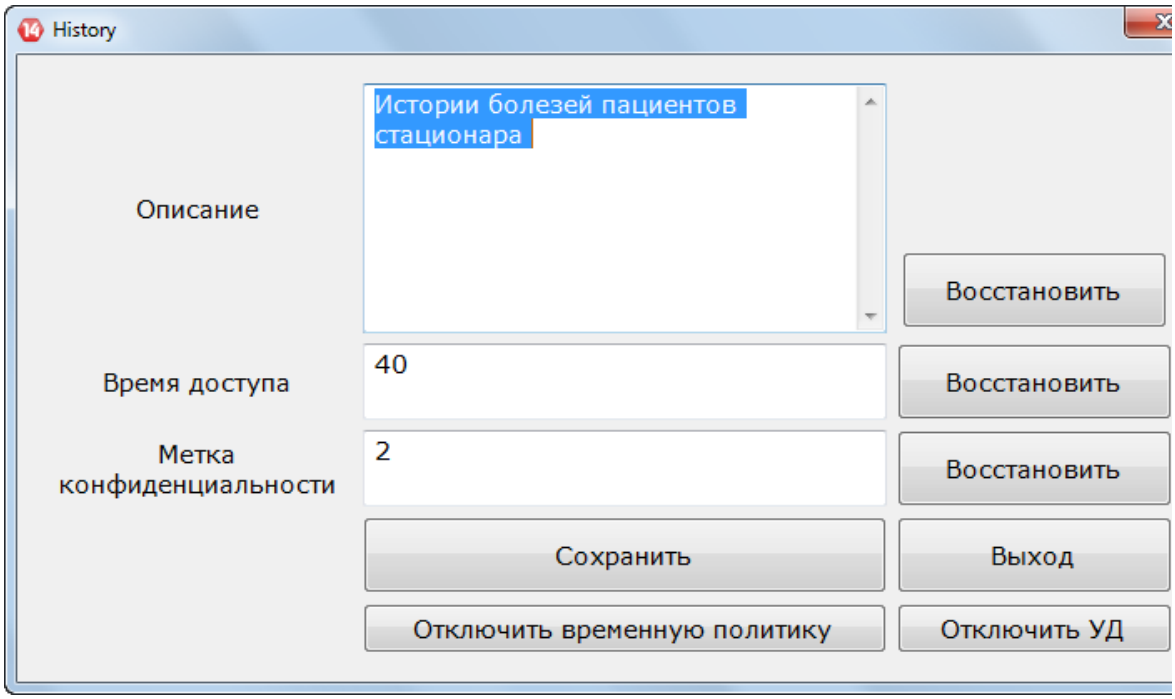

Рис.2. Управление временной политикой и политикой уровней безопасности

Динамическое назначение членства в результате срабатывания самых разнообразных триггеров (по времени, по заступлению на дежурство, по назначению врача пациенту и т.д.) позволяет существенно снизить объем работы, возлагаемой на администратора, влияние человеческого фактора, количество возникающих ошибок и время, необходимое на их устранение, повысить своевременность назначения прав доступа.

Литература

1. Каталог медицинских информационных систем // Ассоциация развития медицинских информационных технологий. URL: [http://www.armit.ru/catalog/] (дата обращения: 01.03.2016).
2. Гусев А., Романов Ф., Дуданов И. Медицинские информационные системы: анализ рынка // PCWeek/RussianEdition. 2005. № 47. С. 18–32.
3. Гулиев Я.И. и др. Медицинские информационные системы и информационная безопасность. Проблемы и решения // Программные системы: Теория и приложения: тр. Междунар. конф. Переславль-Залесский, 2009. С. 175–206.
4. Гусев А.В. Медицинские информационные системы в России: текущее состояние, актуальные проблемы и тенденции развития. М.: Радиотехника, 2012.
5. Назаренко Г.И., Назаренко И.Г., Михеев А.Е., Горбунов П.А., Гулиев Я.И., Фохт И.А., Фохт О.А. Особенности решения проблем информационной безопасности в медицинских информационных системах // Врач и информационные технологии. 2007. № 4. С. 39–43.
6. Дабагов А.Р. Информатизация здравоохранения и некоторые проблемы построения интегрированных медицинских информационных систем // Журнал радиоэлектроники. 2011. № 9. С. 1–57.
7. Оленников Е.А., Захаров А.А., Оленников А.А. и др. Разработка модели управления доступом для типовой медицинской информационной системы // Программные продукты и системы. 2016. № 1. С. 166–169.