УДК 004.7

Т.М. Пестунова, З.В. Родионова

Информационная система управления правами доступа на основе анализа бизнес-процессов

Рассматриваются вопросы построения информационной системы управления правами доступа пользователей к ресурсам автоматизированных информационных систем, основываясь на бизнес-процессах организации. Описаны концептуальная, информационная, функциональная модели системы, а также метамодель, которая позволяет реализовать возможность управления в условиях использования различных формальных моделей (RBAC, DAC, MAC).

Ключевые слова: автоматизированная информационная система (АИС), бизнес-процесс, управление правами доступа, модель доступа, метамодель управления правами доступа.

Безопасность функционирования современных АИС предприятий напрямую зависит от того, насколько соответствуют полномочия пользователя системы его должностным функциям. Общеизвестно, что расширение полномочий сверх необходимых приводит к увеличению случайных ошибок, росту рисков несанкционированного доступа к данным. При недостаточных полномочиях возникают затруднения в выполнении сотрудником своей работы. Формализованные полномочия в виде прав доступа отображаются в настройках системы разграничения доступа (далее СРД) АИС, построение которых определяется формальной моделью. Несмотря на высокий уровень теоретических исследований в области формальных моделей доступа, их практическая реализация наталкивается на трудности интерпретации (обеспечения соответствия абстрактных сущностей и процессов модели реальным объектам и правилам функционирования АИС и актуализации прав доступа ввиду постоянных изменений бизнес-процессов) [1].

Таким образом, актуальной является задача разработки системы, которая позволяла бы формировать множество прав доступа с точки зрения их необходимости и достаточности для выполнения пользователем его функций, исходя из потребностей бизнес-процесса, и своевременно корректировать эти права при внесении изменений в бизнес-процесс.

Для решения этой проблемы можно использовать информационную систему управления правами доступа (далее СУПД), в которой формируются и хранятся описания правил доступа и динамика изменений. Основное назначение этих правил заключается в разделении информации на части и организации такой работы, при которой пользователи имеют доступ к той и только той части информации, которая им необходима и достаточна для выполнения своих обязанностей в рамках бизнес-процесса.

Концептуальную модель системы можно рассматривать как:

– подход к определению прав доступа, позволяющий получить изначальные сведения о правах доступа, а впоследствии управлять их изменениями;

– формальную модель для оценки свойства безопасности АИС;

– модель взаимодействия СУПД с СРД для непосредственного разграничения прав доступа.

В СУПД права доступа пользователей к ресурсам АИС определяются на основе анализа бизнес-процессов, что обеспечивает четкие ответы на вопросы: «кто делает?», «что делает?», «в какой последовательности?», «что получает на входе и предоставляет на выходе?», «кто за все это отвечает?». Этот подход позволяет выйти на более формальный уровень принятия решения о предоставлении прав доступа (по сравнению с подходами на основе владельца процесса или должностной инструкции) и обеспечить следующие преимущества:

– снижение человеческого фактора при определении доступа к информации, так как права доступа определяются исходя из требований процесса, а не из должностных инструкций (часто устаревших) и/или личного мнения руководителя подразделения;

– возможность оперативного внесения изменений в СУПД при изменении бизнес-процессов организации;

– возможность выявления и устранения узких мест процесса с точки зрения безопасности информации;

– снижение рисков за счет выявления возможных проблем процесса до внедрения СУПД.

Для реализации возможности управления правами доступа в условиях СРД, функционирующих на основе различных формальных моделей, была разработана метамодель управления правами доступа для RBAC, MAC и DAC (далее метамодель), представленная на рис. 1.

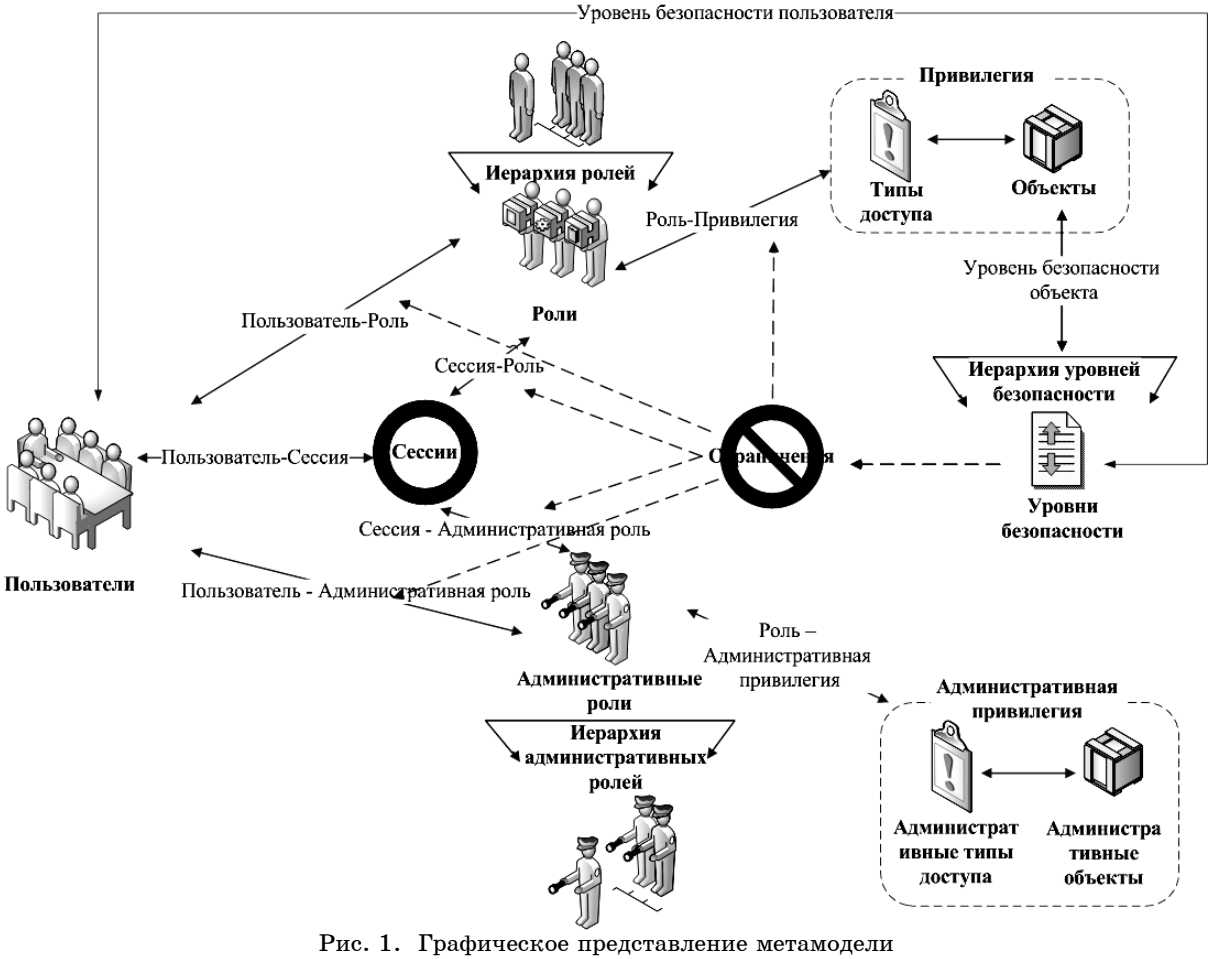

Рис. 1. Графическое представление метамодели

В метамодели не учитываются разновидности дискреционной и мандатной моделей, так как состав элементов в них остается неизменным. В рамках семейства RBAC ориентация сделана на административную модель, поскольку она предоставляет широкий спектр элементов, охватывающих RBAC 0, RBAC 1 и RBAC 2, и содержит наибольшее количество элементов. Основой метамодели является административная ролевая модель, так как именно она позволяет эмулировать мандатный и ролевой доступ. Так как речь идет об управлении правами доступа пользователей, то понятие «субъекта» сужено до понятия «пользователь» независимо от модели доступа.

Модели, входящие в метамодель, содержат следующие элементы [1–3] (таблица):

RBAC 3	DAC	MAC
Пользователь	Пользователь	Пользователь
Объект	Объект	Объект
Тип доступа	Тип доступа	Тип доступа
Административная роль	Администратор	Администратор
Роль		Иерархия уровней безопасности
Иерархия ролей		Уровень безопасности пользователя
Привилегия		Уровень безопасности объекта
Иерархия административных ролей		
Административный объект		
Административный тип доступа		
Административная привилегия		
Ограничение		
Сессия		

Пользователи, объекты, типы доступа используются во всех моделях и понимаются одинаково. Административная роль является близким по значению элементом к администратору, так как администратор – это пользователь с правами, соответствующими административной роли. Элементы: уровень, роль, административная роль, привилегия и ограничение – встречаются только в MAC или RBAC. Элементы: роль, административная роль и ограничение – добавляются в метамодель. Элемент уровень можно трактовать как одно из ограничений вида: пользователь может быть назначен на роль, если его уровень безопасности не ниже, чем уровень безопасности всех объектов, входящих в привилегию роли.

Методику создания и организации функционирования СУПД на основе анализа бизнес-процессов можно представить в виде совокупности взаимосвязанных этапов на рис. 2.

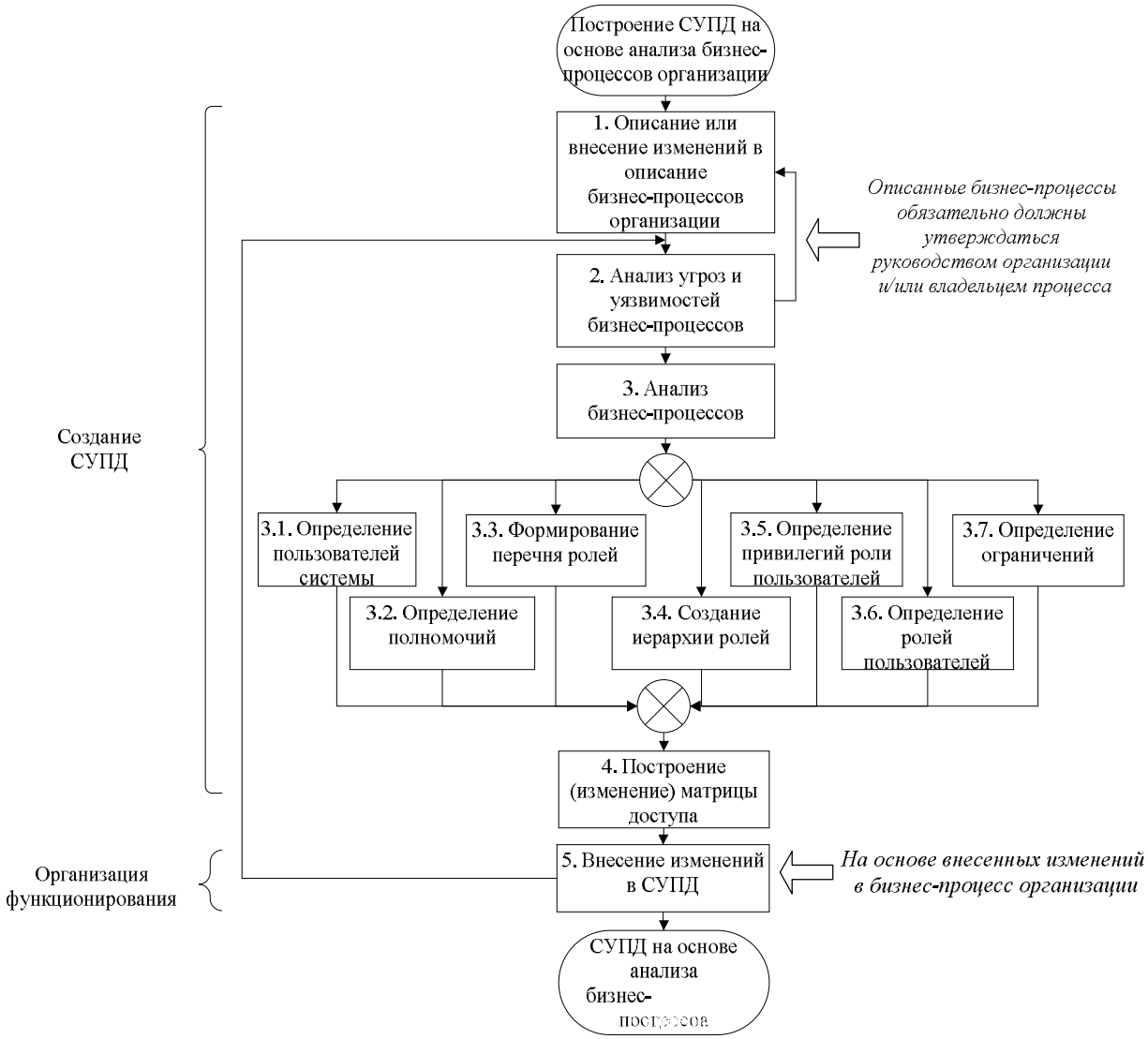

Рис. 2. Этапы построения СУПД на основе анализа бизнес-процессов организации

В результате реализации первых четырех этапов производится создание и первичное заполнение СУПД. Пятый этап позволяет организовать актуализацию системы.

При построении СУПД использованы методологии организационного, функционального и информационного моделирования. Организационная модель определяет, где исполняется бизнес-процесс и кто его исполняет, функциональная отвечает на вопрос «как?», информационная – «с помощью чего?». После ввода в действие СУПД управление правами доступа осуществляется на основе сравнения состояния модели бизнес-процессов до и после внесения каких-либо изменений.

В заключение хотелось бы еще раз подчеркнуть, что используемый в СУПД подход, с одной стороны, характеризуется выделением пользователей, ролей, их иерархии и

объектов доступа на основе анализа бизнес-процесса, с другой стороны – ассоциацией действий и событий бизнес-процесса с совершением доступа.

Литература

1. Зегжда Д.П. Общая схема мандатных моделей безопасности и ее применение для доказательства безопасности систем обработки информации // Проблемы информационной безопасности. Компьютерные системы. – 2000. – № 2. – С. 28–32.

2. Девянин П.Н. Модели безопасности компьютерных систем. – М.: Изд. центр «Академия», 2005. – 144 с.

3. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. – Екатеринбург: Изд-во Урал. ун-та, 2003. – 328 с.

4. Родионова З.В. Управление процессом предоставления прав доступа на основе анализа бизнес-процессов / З.В. Родионова, Т.М. Пестунова // Прикладная дискретная математика. – Красноярск: Изд-во научно-технической литературы, 2008. – С. 91–96.

Пестунова Тамара Михайловна
Канд. техн. наук, доцент каф. информационной безопасности
Новосибирского государственного университета экономик и управления (НГУЭУ), г. Новосибирск
Тел.: (383-2) 24-53-67
Эл. почта: ptm@nsuem.ru

Родионова Зинаида Валерьевна
Аспирант НГУЭУ
Тел.: (383-2) 24-27-83
Эл. почта: rodionova@nsuen.ru

Pestunova T.M., Rodionova Z.V.
An information system for access rights distribution based on analysis of business-processes

The main aspects of development of the information system, which grants users the rights for access to automated information system resources on the basis of the organization business-processes, are considered. The conceptual, informational, functional models of the system, as well as a meta-model, which allows to realize control while using various formal models (RBAC, DAC, MAC), are described.
Keywords: automated information system, business-process, access rights distribution, access model, access rights distribution meta-model.
