УДК 004.7

ТЕХНОЛОГИЯ УПРАВЛЕНИЯ ИЗМЕНЕНИЯМИ ПРАВ ДОСТУПА НА ОСНОВЕ АНАЛИЗА БИЗНЕС-ПРОЦЕССОВ

З.В. Родионова
Новосибирский государственный университет
экономики и управления – «НИНХ»
E-mail: rodionova_z@ngs.ru

Рассматривается технологическое решение проблемы актуализации прав доступа пользователей к ресурсам автоматизированных информационных систем в условиях частых изменений деятельности предприятия. В качестве источника информации об изменениях используется модель бизнес-процесса деятельности предприятия. Описаны классификация изменений, правила реагирования информационной системы управления правами доступа на изменения в бизнес-процессе.

Ключевые слова: бизнес-процесс, управление изменениями, права доступа, информационная система управления правами доступа.

THE TECHNOLOGY OF ACCESS RIGHTS CHANGE MANAGEMENT ON THE BASIS OF THE BUSINESS-PROCESSES ANALYSIS

Z.V. Rodionova
Novosibirsk State University of Economics and Management
E-mail: rodionova_z@ngs.ru

The technological solution of the actualization issue of users access rights to resources of automated information systems in conditions of frequent changes in enterprise activities is considered. The business-process model of enterprise activities was used as an information source. The classification of changes, rules of response of the information system of the access rights management to the changes in the business-process are described.

Key words: business-process, change management, access rights, information system of the access rights management.

1. Введение

Эффективность функционирования современных автоматизированных информационных систем (АИС) предприятия зачастую зависит от того, насколько соответствуют полномочия пользователя системы его должностным функциям.

Формализованные полномочия в виде прав доступа получают свое отражение в настройках системы разграничения доступа (СРД) АИС (например: Oracle, Microsoft SQL Server, Microsoft Active Directory, встроенный механизм разграничения доступа 1С:Предприятие и др.), безопасное построение которых определяется формальной моделью. Несмотря на достаточно высокий уровень теоретических исследований в области формальных моделей доступа, их практическая реализация наталкивается на существенные трудности, связанные с актуализацией прав доступа ввиду постоянных изменений бизнес-процессов.

Признанным фактом является то, что расширение полномочий сверх необходимых приводит к увеличению случайных ошибок, росту рисков, связанных с несанкционированным доступом к данным. При недостаточных полномочиях

возникают затруднения в выполнении сотрудником своей работы. Ситуация многократно усложняется, если на предприятии функционирует несколько АИС, каждая из которых обладает собственной СРД.

Данные CNews Analytics 2009 года показали, что за 60% всех инцидентов утечки информации из АИС несут ответственность нынешние, бывшие и временные сотрудники предприятия. Статистика оценки ущерба выглядит еще более устрашающе: более 65% инцидентов закончились для предприятия потерей бизнеса.

Таким образом, актуальной является задача своевременной корректировки прав доступа пользователей к ресурсам АИС при внесении изменений в бизнес-процесс.

Для решения обозначенной проблемы можно использовать информационную систему управления правами доступа (далее СУПД). Под СУПД понимается информационная система, в которой формализуются и хранятся описания правил доступа (с учетом динамики изменений). Основное назначение этих правил заключается в разделении информации на части и организации такой системы работы с информацией, при которой пользователи имеют доступ к той и только к той части информации, которая им необходима и достаточна для выполнения своих обязанностей в рамках бизнес-процесса.

2. Подход к управлению правами доступа на основе анализа бизнес-процессов

В научной литературе выделяют два подхода к управлению правами доступа: на основе решения владельца и на основе должностных инструкций.

В первом случае права доступа определяет владелец процесса, исходя из своих личных знаний о деятельности предприятия. Этот подход прост и требует малых затрат при внедрении, но серьезный негативный оттенок несет в себе человеческий фактор. Помимо ошибок, которые может допустить владелец процесса, принимая решение о доступе, проблемы возникают тогда, когда объекты используются на пересечении процессов двух владельцев.

Механизм мониторинга изменений слабо формализован и ведется вручную, что создает сложности в его реализации.

Во втором случае права доступа определяются в соответствии с обязанностями, закрепленными в должностной инструкции. Эффективность применения этого подхода напрямую зависит от степени актуализации таких документов на предприятии. Опять же возникают проблемы с мониторингом изменений, а типизированный подход к разработке должностных инструкции может существенно снизить степень корректности интерпретации должностных обязанностей.

С приходом современной модели управления, основанной на применении процессного и системного подходов, процедура формирования должностной инструкции изменилась. Группа стандартов ИСО9000 содержит требования о том, что должностные инструкции должны рождаться и формализовываться исходя из функций бизнес-процесса. Как правило, должностные инструкции генерируются автоматически на основе модели бизнес-процесса с помощью специализированного ПО (Business Studio, ARIS, «ИНТАЛЕВ» и т.д.).

Таким образом, первоисточником для назначения прав доступа фактически становится бизнес-процесс. Должностные инструкции утрачивают здесь свою определяющую роль, превращаясь в промежуточный фиксирующий документ. Руководство утверждает права доступа посредством описания бизнес-процесса.

Такой подход основывается на самой сути деятельности предприятия, ее бизнес-процессах, позволяет выйти на более формальный уровень принятия решения о предоставлении прав доступа [1] и обеспечить такие преимущества, как 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.

3. Информационная система управления правами доступа

Цель СУПД заключается в том, чтобы обеспечивать динамическое согласование настроек СРД с правами доступа, определенными моделью бизнес-процесса.

Для реализации возможности управления правами доступа в условиях СРД, функционирующих на основе различных формальных моделей (ролевой – RBAC, дискреционной – DAC, мандатной – MAC), была разработана обобщенная модель разграничения прав доступа. Данная модель описывает структуру, принципы действия различных моделей доступа. Цель разработки обобщенной модели заключается в организации функционирования различных моделей доступа в одном информационном пространстве.

СУПД формирует права доступа, не осуществляя их разграничения для конкретной подсистемы, для этих целей существуют системы разграничения доступа. Система разграничения доступа зависит от программно-технических особенностей конкретной информационной системы управления, СУПД же является независимой и может/должна быть единой для всех АИС организации.

Для создания и последующей организации функционирования СУПД на вход системы должны поступить описания бизнес-процессов и информация об их изменении. На выходе формируется каталог ролей, иерархия ролей и матрица доступа [2].

Алгоритм построения СУПД на основе анализа бизнес-процессов можно представить в виде совокупности взаимосвязанных этапов (рис. 1).

Процесс анализа бизнес-процессов можно производить автоматически (например, с помощью языка XML), извлекая все необходимые данные из среды бизнес-моделирования.

После того как СУПД построена и введена в действие, на первый план выходит проблема актуализации прав доступа.

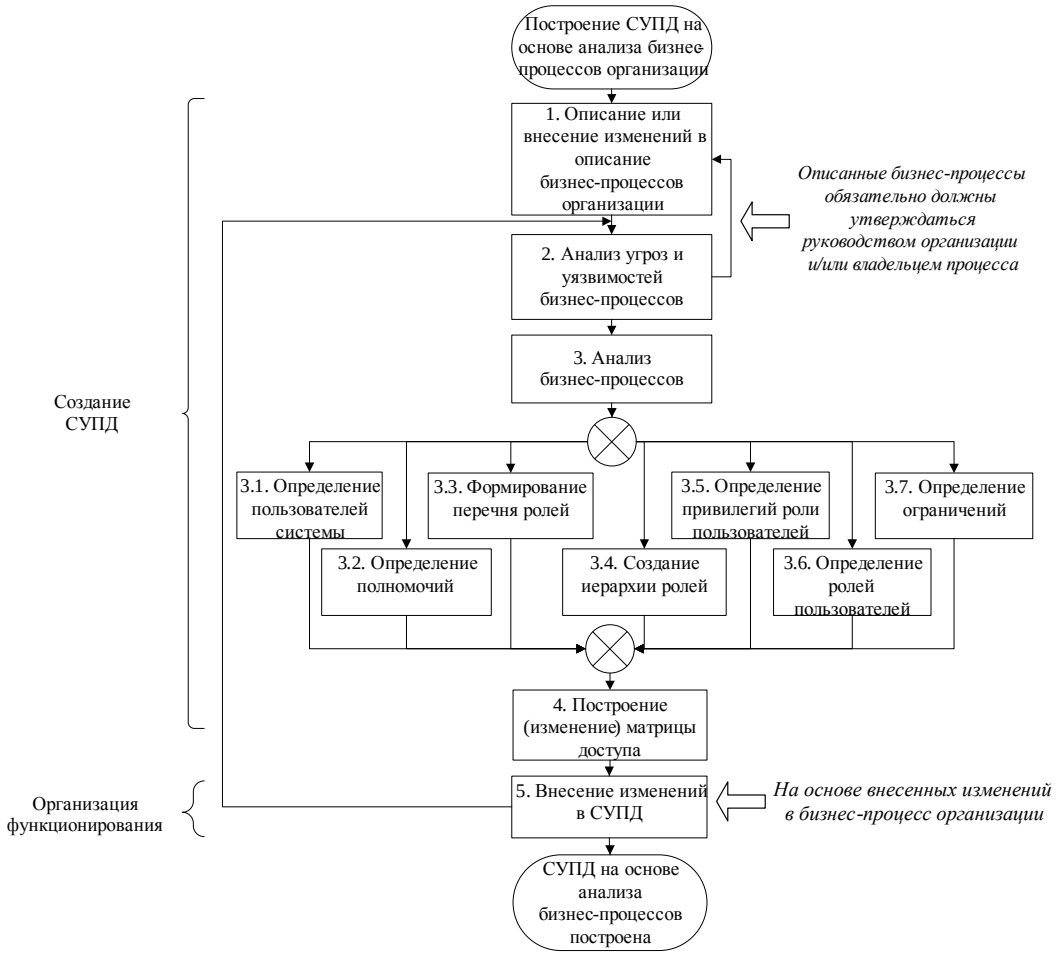

Рис. 1. Этапы создания и организации функционирования СУПД

4. Внесение изменений в СУПД

Постоянно меняющиеся окружение, стремление получить конкурентные преимущества заставляют предприятие перестраивать свою деятельность, что, в свою очередь, неизменно отражается на правах пользователей информационных систем. Для организации непрерывного и эффективного функционирования СУПД такие изменения необходимо отслеживать и интерпретировать на изменение прав доступа к ресурсам АИС.

В 60–70-е годы XX в. появилось новое направление менеджмента – управление изменениями (change management). В рамках этого направления были разработаны следующие модели: модель изменений К. Левина, модель управления изменениями Л. Грейнера, модель преобразования бизнеса Ф. Гуияра и Дж. Келли, модель «От хорошего к великому» Дж. Коллинза, модель «Кривая перемен» Дж. Дак и многие другие.

Все многообразие разработанных моделей изменений направлено на обеспечение своевременной адаптации организации к изменениям внутренней и внешней среды. При использовании процессного подхода управление изменениями производится в условиях изменения существующих моделей бизнес-

процессов с последующим их внедрением в систему функционирования организации.

При внесении изменений в СУПД наиболее важным аспектом является фиксация факта изменения прав доступа, состава ролей, их иерархии, типов и объектов доступа. Поэтому возникла необходимость разработать собственную модель управления изменениями в рамках организации функционирования СУПД.

Для разработки указанной модели, прежде всего, необходимо определить основные виды и содержание изменений. Преобразование бизнес-процессов организации можно рассматривать с самых различных точек зрения, поэтому в современной литературе можно встретить множество классификаций организационных изменений, но все они не учитывают специфику управления правами доступа. В связи с этим была разработана классификация, нацеленная на определение сущности и параметров изменения деятельности организации в контексте их влияния на управление правами доступа к ресурсам АИС (рис. 2). Основой для классификации послужили категории данных, необходимые для построения СУПД. Данная классификация не претендует на полноту и может быть расширена с учетом особенностей функционирования отдельно взятого предприятия.

Рис. 2. Классификация изменений деятельности организации

Приведенная классификация обусловлена различными взглядами на деятельность организации, а именно, с точки зрения:

- структурных изменений организации, которые затрагивают подразделения и/или сотрудников (организационные изменения);
- изменения самого бизнес-процесса, прежде всего его функций, так как последовательность их исполнения для управления правами доступа не важна (изменения в бизнес-процессах);
- изменений на информационном уровне (изменения в АИС).

Управление правами доступа осуществляется на основе сравнения состояния модели бизнес-процессов до и после внесения каких либо изменений (см. таблицу).

Управление правами доступа

Категория изменений	Название изменения	Действие в СУПД
Организационные изменения	Создание нового подразделения, создание новой проектной группы	Создание нового ограничения
	Создание новой должности	Создание новой роли
	Изменение иерархии подчиненности	Изменение информации о подчиненных ролях
	Прием нового сотрудника	Создание пользователя, назначение роли пользователю
	Увольнение сотрудника	Удаление пользователя из всех ролей
	Перевод сотрудника	Изменение ролей
	Изменение ФИО сотрудника	Изменение свойств пользователя
Изменения в бизнес-процессах	Появление новой функции*	Создание привилегии
	Изменение функции, связанной с работой в АИС	Изменение привилегии
	Изменение исполнителя функции, связанной с работой в АИС	Изменение привилегий роли и/или изменение назначений пользователя на роли
Изменения в АИС	Изменение функций АИС	Изменение обоснования назначения прав доступа
	Изменение СРД	Изменение типов доступа, изменение названий доступа
	Переход на другую СУПД	Изменение объектов и типов доступа

* Учитываются только те изменения, которые связаны с работой в АИС.

В заключение хотелось бы еще раз подчеркнуть, что описанная технология управления изменениями, с одной стороны, характеризуется выделением пользователей и их ролей, иерархии ролей и объектов доступа автоматизированных путем на основе анализа модели бизнес-процесса, с другой – ассоциацией действий и событий бизнес-процесса с совершением доступа и их изменениями.

Применение данной технологии позволит избежать противоречий в правилах доступа, исключить влияние субъективного фактора, повысить прозрачность управления правами доступа в СРД допускающих использование внешних правил присвоения прав.

Литература

1. *Пестунова Т.М., Родионова З.В.* Управление процессом предоставления прав доступа на основе анализа бизнес-процессов // Прикладная дискретная математика. Красноярск: Издательство научно-технической литературы, 2008. С. 91–96.
2. *Родионова З.В.* Информационная система управления правами доступа // Материалы II Всероссийской научной конференции «Научное творчество XXI века» с международным участием // В мире научных открытий. Красноярск: Научно-инновационный центр, 2010. № 4 (10). Ч. 11. С. 92–94.

Bibliography

1. *Pestunova T.M., Rodionova Z.V.* Upravlenie processom predostavlenija prav dostupa na osnove analiza biznes-processov // Prikladnaja diskretnaja matematika. Krasnojarsk: Izdatel'stvo nauchno-tehnicheskoj literatury, 2008. PP. 91–96.
2. *Rodionova Z.V.* Informacionnaja sistema upravlenija pravami dostupa // Materialy II Vserossijskoj nauchnoj konferencii «Nauchnoe tvorchestvo XXI veka» s mezhdunarodnym uchastiem // V mire nauchnyh otkrytij. Krasnojarsk: Nauchno-innovacionnyj centr, 2010. № 4 (10). Ch. 11. PP. 92–94.