U.D.C. 004.94

USER ACCESS RIGHTS MANAGEMENT ON THE BASIS OF ANALYSIS OF THE COMPANY'S BUSINESS-PROCESSES FUNCTIONS

Z. Rodionova, Candidate of Technical sciences, Senior Lecturer
Novosibirsk State University of Economics and Management, Russia

The author considers the issues of management of the users' access rights to resources of the automated information systems: formation of a set of access rights from the standpoint of their necessity and sufficiency for the user to fulfill his/her functions, proceeding from the requirements of the business process; timely adjustment of these rights in the course of modification of the business process.

Keywords: access rights management, process approach, business-processes, access model, information system.

Conference participant,
National Research Analytics Championship

УДК 004.94

УПРАВЛЕНИЕ ПРАВАМИ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ АНАЛИЗА ФУНКЦИЙ БИЗНЕС-ПРОЦЕССОВ ПРЕДПРИЯТИЯ

Родионова З.В., канд. техн. наук, ст. преподаватель
Новосибирский государственный университет экономики и управления, Россия

В статье рассматриваются вопросы управления правами доступа пользователей к ресурсам автоматизированных информационных систем: формирование множества прав доступа с точки зрения их необходимости и достаточности для выполнения пользователем его функций исходя из потребностей бизнес-процесса, а также своевременная корректировка этих прав при внесении изменений в бизнес-процесс.

Ключевые слова: управление правами доступа, процессный подход, бизнес-процесс, модель доступа, информационная система.

Участник конференции,
Национального первенства по научной аналитике

http://dx.doi.org/10.18007/gisap:tsca.v0i8.1424

Эффективность функционирования современных автоматизированных информационных систем (далее АИС) предприятия напрямую зависит от того, насколько соответствуют полномочия пользователя системы его должностным функциям. Признанным фактом является то, что расширение полномочий сверх необходимых приводит к увеличению непреднамеренных ошибок пользователя, 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 своей системой разграничения доступа.

Формализованные полномочия в виде прав доступа получают свое отражение в настройках системы разграничения доступа АИС (например, Windows Active Directory, «КУБ», Microsoft SQL Server и др.), безопасное построение которых определяется формальной моделью. Существенный вклад в разработку формальных моделей внесли Гайдамакин Н.А., Герасименко В.А., Грушо А.А., Девянин П.Н., Зегжда П.Д., Ивашко А.М., Neumann P., Ravi S. Sandhu, Ferraiolo D. и др. Несмотря на достаточно высокий уровень теоретических исследований в области формальных моделей доступа, их практическая реализация наталкивается на существенные трудности, связанные с формализацией, т. е. обеспечением соответствия абстрактных сущностей и процессов модели реальным объектам и правилам функционирования автоматизированных информационных систем и актуализацией прав доступа ввиду постоянных изменений бизнес-процессов.

Рис. 1. Этапы управления правами доступа на основе анализа функций бизнес-процессов предприятия

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 серьезным недостатком является человеческий фактор: помимо оши-

бок, 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 в организации. Так же возникают проблемы с мониторингом изменений, а типизированный подход к разработке должностных инструкций 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 ИСО 9000 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 программного обеспечения. Таким образом, первоисточником для назначения прав доступа фактически становятся функции бизнес-процесса. Должностные инструкции утрачивают здесь свою определяющую роль, превращаясь в промежуточный фиксирующий документ. Руководство утверждает права доступа посредством утверждения описания бизнес-процесса. Такой подход основывается на самой сути деятельности предприятия, ее бизнес-процессах.

Подход на основе анализа бизнес-процессов позволяет выйти на более формальный уровень принятия решения о предоставлении прав доступа и обеспечить следующие преимущества:

– снижение человеческого фактора при определении доступа к информации, так как права доступа определяются исходя из требований

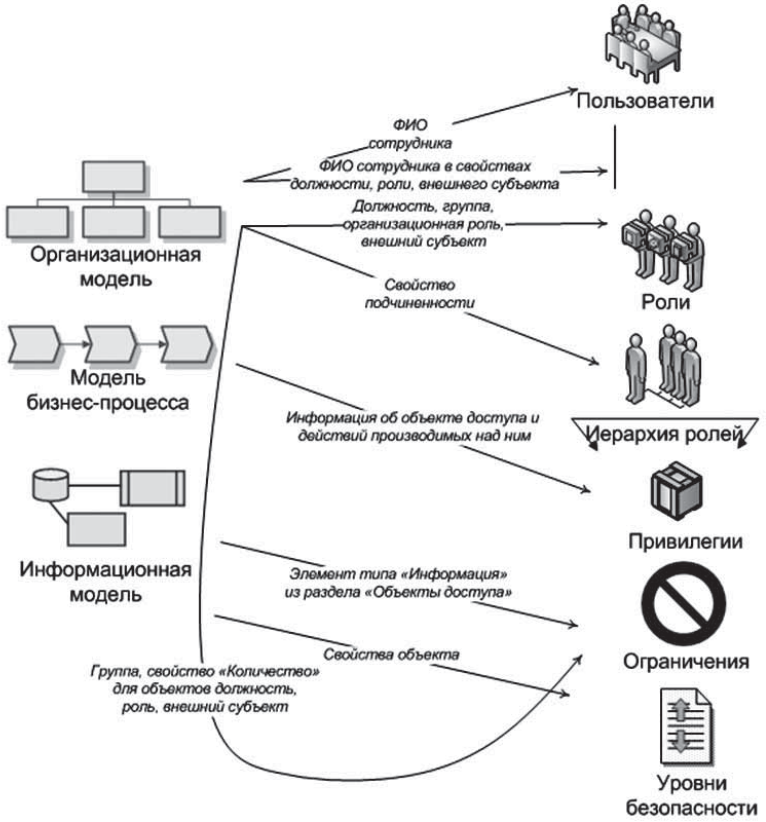

Рис. 2. Схема извлечения данных

процесса, а не из должностных инструкций (часто устаревших) и / или личного мнения руководителя подразделения;

– возможность оперативного внесения изменений в права доступа при изменении бизнес-процессов предприятия;

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

– снижение рисков за счет выявления возможных проблем процесса до настройки прав доступа в СРД.

Важность применения именно процессного подхода для создания и эксплуатации системы управления информационной безопасностью предприятия, неотъемлемой частью которой является процесс управления правами доступа, подчеркивает и международный стандарт ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования» (раздел 0.2 «Процессный подход»).

Для реализации возможности управления правами доступа в условиях систем разграничения доступа, функционирующих на основе различных формальных моделей (ролевой – RBAC, дискреционной – DAC, мандатной – MAC), разработана обобщенная модель разграничения прав доступа (далее – обобщенная модель) [1]. Данная модель описывает структуру, принципы действия различных моделей доступа. При разработке обобщенной модели было учтено главное требование современных АИС – наличие механизма администрирования прав доступа. Основой обобщенной модели является административная ролевая модель, которая так же позволяет эмулировать мандатный и дискреционный доступ. Проверка корректности обобщенной модели разграничения прав доступа проведена путем последовательного изъятия из нее элементов и отношений, не входящих в две из трех формальных моделей и доказательства того, что оставшиеся элементы функционируют в соответствии с правилами данной модели разграничения прав доступа.

Рис. 3. Классификация изменений деятельности предприятия в контексте актуализации прав доступа пользователей к ресурсам АИС

Этапы управления правами доступа на основе анализа функции бизнес-процессов предприятия можно представить в следующем виде (Рис. 1).

Для реализации первого этапа по описанию бизнес-процессов предприятия практическую значимость имеют методологии организационного, функционального и информационного моделирования. Организационная модель определяет «где» исполняется бизнес-процесс и самое главное «кто» его исполняет, функциональная отвечает на вопрос «как?», информационная «с помощью чего?».

Анализ угроз и уязвимостей бизнес-процессов позволяет оценить информационные риски и определить меры по противодействию, тем самым повысив безопасность функционирования системы на организационном уровне. Подобный алгоритм построения модели угроз каждая организация определяет самостоятельно исходя из специфики своего функционирования и принятой политики безопасности либо на основе законодательно утвержденных нормативно-методических документов.

Процесс анализа бизнес-процессов можно производить автоматически (например, с помощью языка XML), извлекая все необходимые данные из среды бизнес – моделирования. Алгоритм извлечения данных можно представить в общем виде, как схему потоков (Рис. 2).

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 процесса актуализации прав доступа такие изменения необходимо отслеживать и интерпретировать на изменение прав доступа к ресурсам АИС.

Разработана классификация, нацеленная на определение сущности и параметров изменения деятельности предприятия в контексте их влияния на управление правами доступа к ресурсам АИС (Рис. 3). Основой для данной классификации послужили категории данных, необходимые для формализации и актуализации прав доступа, которые содержатся в обобщенной модели. Данная классификация не претендует на полноту и может быть расширена с учетом особенностей функционирования отдельно взятого предприятия.

В заключение хотелось бы еще раз подчеркнуть, что предлагаемый 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. Для промышленного использования предложенного подхода была разработана информационная система формализации и актуализации прав доступа [2, 3].

References:

1. Rodionova Z.V., Pestunova T.M. Algoritm avtomatizirovannogo formirovanijajelementovobobshhennojmodeli razgranichenija prav dostupa na osnove modeli biznes-processov predprijatija [Algorithm of the automated formation of elements of the generalized model of access rights differentiation on the basis of the company's business processes model]., Svidetel'stvo o registracii jelektronnogo resursa Obedinennogo fonda jelektronnyh resursov «Nauka i obrazovanie» [Article of incorporation of an electronic resource of the Joint fund of the electronic resources «Science and education»]., No. 16615 from 13.01.2011.

2. Rodionova Z.V., Pestunova T.M. Programma dlja JeVM. Informacionnaja sistema formalizacii i aktualizacii prav dostupa «BusinessProcessSecurity» [Computer program. Information system of formalization and actualization of access rights «Business Process Security»]., Svidetel'stvo ob oficial'noj registracii ROSPATENT RF [Certificate of official registration] No. 2011615409 from 19.10.2011.

3. Rodionova Z.V. [and others] Informacionnaja sistema upravlenija pravami dostupa na osnove analiza biznes-processov [Information system of access rights management on the basis of business processes analysis]., T.M. Pestunova, Z.V. Rodionova Dok-lady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki [Reports of the Tomsk State University of Control Systems and Radioelectronics]. – 2010., No. 2 (22)., Part 2., pp. 253-256.

Литература:

1. Родионова З.В., Пестунова Т.М. Алгоритм автоматизированного формирования элементов обобщенной модели разграничения прав доступа на основе модели бизнес-процессов предприятия // Свидетельство о регистрации электронного ресурса Объединенного фонда электронных ресурсов «Наука и образование» № 16615 от 13.01.2011.

2. Родионова З.В., Пестунова Т.М. Программа для ЭВМ. Информационная

система формализации и актуализации прав доступа «Business Process Security» // Свидетельство об официальной регистрации РОСПАТЕНТ РФ № 2011615409 от 19.10.2011.

3. Родионова З.В. [и др.] Информационная система управления правами доступа на основе анализа бизнес-процессов / Т.М. Пестунова, З.В. Родионова // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2010. – № 2 (22). – Ч.2. – С. 253 - 256.

Information about author:

1. Zinaida Rodionova – Candidate of Technical sciences, Senior Lecturer, Novosibirsk State University of Economics and Management; address: Russia, Novosibirsk city; e-mail: rodionova_z@ngs.ru