На правах рукописи

Родионова Зинаида Валерьевна

МОДЕЛИРОВАНИЕ И РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ФОРМАЛИЗАЦИИ И АКТУАЛИЗАЦИИ ПРАВ ДОСТУПА

Специальность 05.25.05 – Информационные системы и процессы

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Новосибирск – 2011

Работа выполнена в Новосибирском государственном университете экономики и управления.

Научный руководитель:	кандидат технических наук, доцент Пестунова Тамара Михайловна
Официальные оппоненты:	доктор технических наук Жижимов Олег Львович
	кандидат технических наук Вейсов Евгений Алексеевич
Ведущая организация:	Томский государственный университет систем управления и радиоэлектроники

Защита состоится 01.02.2012 в 10^{00} часов на заседании диссертационного совета ДМ 003.046.01 в Институте вычислительных технологий СО РАН по адресу 630090, г. Новосибирск, проспект Академика М. А. Лаврентьева, 6 (dsovet@ict.nsc.ru).

С диссертацией можно ознакомиться в специализированном читальном зале вычислительной математики и информатики отделения ГПНТБ СО РАН (630090, г. Новосибирск, проспект академика М. А. Лаврентьева, д. 6).
Автореферат разослан 29.12.2011.

Ученый секретарь
диссертационного совета
доктор физико-математических наук,
профессор Л. Б. Чубаров

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования. 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.

Диссертационная работа посвящена вопросам моделирования и разработки информационной системы формализации и актуализации прав доступа, которая позволяет формировать множество прав доступа с точки зрения их необходимости и достаточности для выполнения пользователем его функций исходя из потребностей бизнес-процесса, а также своевременно корректировать эти права при внесении изменений в бизнес-процесс.

Тема диссертации является актуальной, так как предложенная информационная система обеспечивает унифицированное и конструктивное решение проблемы формализации и актуализации необходимых и достаточных прав доступа, эффективно работающее в условиях частых организационных изменений, характерных в наше время и для бизнеса, и для госструктур.

Цель и задачи исследования. Целью исследования является создание модели информационной системы, предназначенной для формализации и актуализации прав доступа пользователей к ресурсам автоматизированных информационных систем на основе моделей бизнес-процессов предприятия, а также разработка программных компонентов на ее основе.

Для достижения цели исследования были поставлены следующие задачи.

1. Определить структурные и функциональные требования к информационной системе формализации и актуализации прав доступа на основе анализа проблемы формализации и актуализации прав доступа пользователей к ресурсам АИС.
2. Предложить модель информационной системы формализации и актуализации прав доступа, реализующую принципы организации и структурирования данных в рамках концептуального, логического и физического проектирования систем.
3. Выполнить практическую реализацию предложенной модели информационной системы формализации и актуализации прав доступа.

Объект и предмет исследования. Объектом исследования является автоматизированная информационная система. Предметом – процесс формализации и актуализации прав доступа пользователей к ресурсам АИС.

Методы исследования. В качестве основных методов исследования применялись: методы анализа бизнес-процессов, теории множеств, теории построения и анализа алгоритмов, теории реляционных баз данных, теории построения объектно-ориентированных программных средств.

Основные положения, выносимые на защиту.

1. Модель информационной системы, обеспечивающая формализацию и актуализацию прав доступа в условиях применения систем разграничения прав доступа, функционирующих с использованием различных формальных моделей.
2. Программные компоненты, позволяющие автоматизировано формировать и поддерживать в актуальном состоянии права доступа.
3. Информационная система формализации и актуализации прав доступа, разработанная с применением методов объектно-ориентированного программирования, а также концептуальных и нормализованных реляционных моделей данных.

Научная новизна работы заключается в следующем.

1. Предложена оригинальная модель информационной системы, практическая реализация которой позволяет транслировать информацию о полномочиях сотрудников, содержащуюся в модели бизнес-процессов в настройки прав системы разграничения доступа АИС.
2. Разработан новый алгоритм автоматизированного формирования элементов обобщенной модели разграничения прав доступа из модели бизнес-процесса на основе разработанных правил преобразования.
3. Разработан новый алгоритм актуализации прав доступа к ресурсам автоматизированных информационных систем на основе изменений в моделях бизнес-процессов предприятия.

Достоверность научных результатов обеспечивается полнотой анализа теоретических разработок, результатами функционально-стоимостного анализа и имитационного моделирования, положительными результатами апробации и внедрения, а также положительной оценкой результатов на научных конференциях.

Практическая значимость. Разработанная информационная система формализации и актуализации прав доступа внедрена в рабочий процесс ряда предприятий. По результатам проведенного функционально-стоимостного анализа и имитационного моделирования, внедрение информационной системы формализации и актуализации прав доступа позволяет сократить финансовые затраты на управление доступом в 3,5–8 раз, что подтвердили и результаты внедрения в рабочий процесс. За счет внесения изменений в бизнес-процесс по результатам анализа угроз и уязвимостей снижается риск инсайдерских угроз. Результаты диссертационного исследования применяются в процессе создания систем защиты для информационных систем персональных данных.

Представление работы. Результаты диссертационной работы докладывались и обсуждались на следующих конференциях, школах и семинарах: «Компьютерная безопасность и криптография» (Красноярск, 2008); ПЕРСПЕКТИВА – 2009 (Таганрог, 2009); «Управление информационными ресурсами образовательных, научных и производственных организаций» (Магнитогорск, 2009); «Актуальные проблемы безопасности информационных технологий» (Красноярск, 2009); «Проблемы информационной безопасности в системе высшей школы» (Москва, 2011); Научно-практическая конференция преподавателей и аспирантов «Новосибирский государственный университет экономики и управления» (Новосибирск, 2007–2011); «Проблемы информационной безопасности государства, общества и личности» (Барнаул – Томск, 2010).

Результаты диссертационного исследования были использованы в ходе проведения научно-исследовательских работ:

- «Russian Higher Education in Information Technology: an international APProach» в рамках гранта по программе «Tempus» (2009);
- Стипендиальная программа мэрии г. Новосибирска (2006–2007);
- Грант НГУЭУ «Разработка интегрированной информационной системы «Университет» Новосибирского государственного университета экономики и управления» (2006–2008);
- Грант НГУЭУ «Проектирование системы защиты персональных данных» (2010–2011).

Кроме того, результаты исследования применяются в учебном процессе Новосибирского государственного университета экономики и управления и Новосибирского государственного медицинского университета.

Публикации. По теме диссертации опубликовано 15 работ, в том числе (в скобках в числителе указан общий объем этого типа публикаций, в знаменателе – объем, принадлежащий лично автору) 2 статьи в изданиях, рекомендованных ВАК для представления основных научных результатов диссертаций на соискание ученой степени доктора или кандидата наук (0,9/0,78), 1 свидетельство о государственной регистрации программы для ЭВМ, 2 свидетельства о государственной регистрации электронных ресурсов, 1 статья в тематическом рецензируемом научном журнале (0,38/0,2), 2 учебных пособия; 7 работ в трудах и сборниках тезисов (1, 2/1,1).

Личный вклад автора. Все результаты, приведенные в диссертации, получены автором лично или в неделимом соавторстве с Пестуновой Т. М. Из печатных работ, опубликованных диссертантом в соавторстве, в текст диссертации вошли только те результаты, которые содержат непосредственный творческий вклад автора на всех этапах – от постановки задач до разработки правил, моделей, программных компонентов.

Структура и объем диссертации. Диссертация включает введение, три главы, заключение, библиографический список, содержащий 104 наименования, и 14 приложений. Общий объем работы 161 страница, в том числе 39 рисунков и 7 таблиц.

ОСНОВНЫЕ ПОЛОЖЕНИЯ РАБОТЫ

Во введении обоснована актуальность вопросов, связанных с моделированием и разработкой информационной системы формализации и актуализации прав доступа пользователей к ресурсам АИС, сформулирована цель исследования и его задачи, раскрыты элементы научной новизны и практическая значимость.

Первая глава содержит результаты анализа проблемы формализации и актуализации прав доступа пользователей к ресурсам современных АИС.

Для проведения анализа представленной проблематики были введены следующие термины. В диссертационной работе под пользователем понимается человек, использующий ресурсы АИС предприятия. Формализация прав доступа обеспечивает разделение информации на части и определение каждому пользователю доступа к той и только к той части информации, которая ему необходима и достаточна для выполнения своих функциональных обязанностей. Актуализация прав доступа представляет собой своевременное внесение изменений в права доступа пользователей АИС в случае изменения деятельности предприятия.

В научной литературе выделяют два подхода к формализации и актуализации прав 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 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 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 становится бизнес-процесс. 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 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 формализации и актуализации прав доступа, подчеркивает и международный стандарт ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования» (раздел 0.2 «Процессный подход»). Обеспечить непрерывное и эффективное решение задачи формализации и актуализации прав доступа позволяет соответствующая специализированная информационная система.

Для реализации возможности формализации и актуализации прав 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). Данная модель описывает структуру, принципы действия различных моделей доступа. Цель разработки обобщенной модели заключается в организации функционирования различных моделей доступа в одном информационном пространстве.

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. Следующие шаги описывают процесс создания обобщенной модели.

1. Идентификация элементов каждой из моделей доступа.
2. Определение сходных и различных по значению элементов.
3. Добавление сходных элементов в обобщенную модель разграничения прав доступа.
4. Добавление различных элементов, которые могут быть добавлены в обобщенную модель. Если добавление невозможно, то выполняется модификация элементов.
5. Графическое представление обобщенной модели.

Элементы моделей дискреционного, мандатного и ролевого доступов, сгруппированные по значению, представлены в табл. 1.

Таблица 1.

Элементы моделей дискреционного, мандатного и ролевого доступов

RBAC	DAC	MAC
пользователь	пользователь	пользователь
объект	объект	объект
тип доступа	тип доступа	тип доступа

RBAC	DAC	MAC
привилегия		иерархия уровней безопасности
роль		уровень безопасности субъекта
иерархия ролей		уровень безопасности объекта
административная роль		
иерархия административных ролей		
административный объект		
административный тип доступа		
административная привилегия		
сессия		
ограничение		

Пользователи, объекты, типы доступа используются во всех моделях и понимаются одинаково: пользователь (***U***); объект (***O***), под которым понимаются множества физических (элемент базы данных: кортежи, атрибуты, представление и др.) и логических (сущность системы в восприятии пользователя) объектов; тип доступа (***T***), который напрямую зависит от используемой в АИС разновидности СУБД и/или системы разграничения прав доступа.

Элементы «привилегия, роль», «иерархия ролей», «административная роль», «иерархия административных ролей», «административный объект», «административный тип доступа», «административная привилегия», «сессия», «ограничение» были добавлены в обобщенную модель разграничения прав доступа в следующем виде:

- привилегия (***P***) – это право на выполнение определенного типа доступа к одному или несколькими объектам системы, $P=\{p_1, p_2, \ldots, p_{Np}\}$ $\forall p \in PP = (ta, o)$, где $ta \in TA, o \in O$;
- *роль* (***R***) – это название совокупности привилегий, которые выполняются в АИС;
- иерархия ролей (***HR***) – это средства для структурирования ролей, чтобы удобно отражать полномочия и ответственности в организации;
- административная роль (***AR***) используется для решения задач администрирования;
- административный объект (***AO***) – множество физических объектов, доступ к которым возможно изменить: роли, пользователи, объекты,

привилегии и т. д.;
- административный тип доступа (***AT***);
- административная привилегия (***AP***);
- сессия (***S***) – подмножество активированных в течение некоторого интервала времени ролей пользователя. Установление сессии возможно только после регистрации пользователя в АИС. Активация каких-либо ролей вне сессии невозможна;
- ограничение (***C***) – предикаты, которые накладываются на отношения и функции и возвращают значения «можно» или «нельзя»;
- элемент уровень (***L***) 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.

Описанные ниже выражения показывают отношения между элементами обобщенной модели:
- ***User-authorized-roles*** – множество ролей, ассоциированных с пользователем ***u***;
- ***Session-user*** – пользователь, ассоциированный с конкретной сессией ***s***;
- ***Role-permission*** – множество ролей, ассоциированных с привилегией ***p***, ***role – permission*** $\subseteq R \times P$;
- ***Permission-type*** – множество типов доступа, ассоциированных с привилегией ***p***;
- ***Permission-object*** – множество объектов, ассоциированных с привилегией ***p***;
- ***Mutually-exclusive-authorization-role*** – множество ролей, взаимоисключающих роль ***r***;
- ***Mutually-exclusive-authorization-permission*** – множество прав доступа, взаимоисключающих права доступа ***p***;
- ***Cardinal-role*** – множество активных ролей ***r***, емкость которых не превышена, $\forall$ ***r : R:, membership-limit(r)*** $\geq$ ***number-of-members(r)***;
- ***User-level*** – множество пользователей, ассоциированных с уровнем ***l***;
- ***Administrative-role-member*** – множество пользователей, ассоциированных с административными ролями ***ar***;
- ***HAR*** $((AR_{I+1}, AR_I)>)$, где AR_{I+1} является непосредственным наследником AR_I;
- $(L_{I+1}, L_I)<)$, где L_{I+1} является непосредственным наследником L_I, и знак < означает «содержит». Например: L={UL (неклассифицированное), CL(конфиденциально), SL (секретно), TL (совершенно секретно)}HL= UL< CL< SL< TL;
- ***Object-level*** – множество объектов, ассоциированных с уровнем ***l***;

- ***Cardinal-level*** – множество активных ролей пользователей соответствующего уровня;
- ***Administrative role-administrative permission*** – множество административных ролей, ассоциированных с административной привилегией ***ap***;
- ***Administrative permission-administrative type*** – множество административных типов доступа, ассоциированных с административной привилегией ***p***;
- ***Administrative permission-administrative object*** – множество административных объектов, ассоциированных с административной привилегией ***pa***.

Графически разработанная модель представлена на рис. 1.

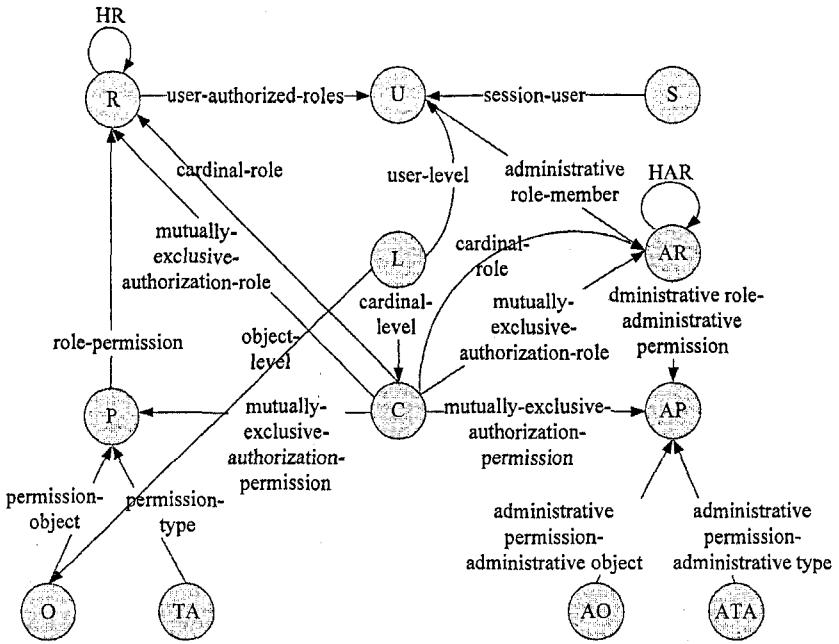

Рис. 1. Обобщенная модель разграничения прав доступа

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.

Вторая глава посвящена описанию процесса и результатов проектирования информационной системы формализации и актуализации прав доступа.

Разработана концептуальная модель системы, позволяющая получить общее представление о причинно-следственных связях, присущих системе, ее структуре и свойствах элементов. Концептуальная модель (рис. 2) обладает следующими основными свойствами: независимость от программно-технических особенностей конкретной АИС; единство системы по отношению ко всем АИС предприятия; использование подхода на основе анализа бизнес-процессов для формализации и актуализации прав доступа; разграничение прав доступа в рамках разработанной ранее обобщенной модели доступа.

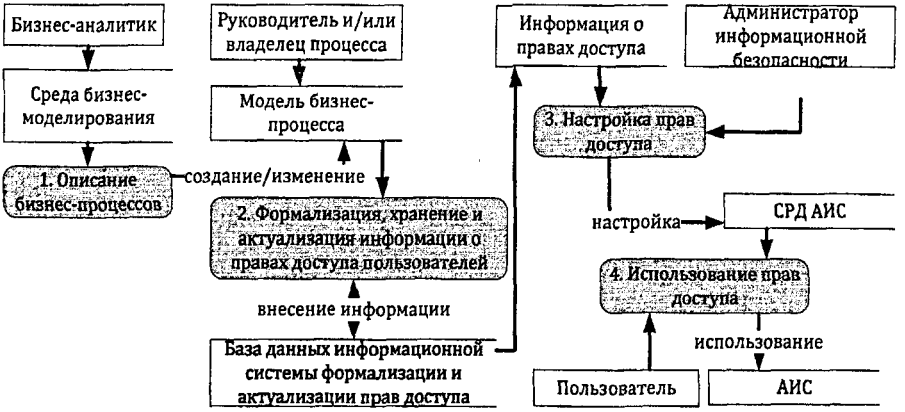

Рис. 2. Потоки данных в информационной системе формализации и актуализации прав доступа

Для определения требований к информационной системе поэтапно рассмотрен процесс формализации и актуализации прав доступа пользователей к ресурсам АИС на основе анализа бизнес-процессов предприятия (рис. 3). Построена графическая модель бизнес-процесса «Формализации и актуализации прав доступа» в нотациях IDEF0 и EPC.

Формализованы следующие основные требования к характеру проведения работ по описанию бизнес-процессов.

1. Общие требования (применение уже существующих на предприятии моделей бизнес-процессов в рамках известных методик; использование графического способа описания в качестве основного; использование комплексного подхода к описанию процессов).
2. Требования к системе бизнес-моделирования (автоматизированное извлечение данных из модели бизнес-процесса; использование методологий организационного, функционального и информационного моделирования).
3. Требования к моделям, которые определяют содержание описания бизнес-процессов (проведение описания в двух направлениях: описание процессов предприятия, которые осуществляются с помощью

АИС, описание процесса управления правами доступа к АИС, которое будет использовано для построения административной модели доступа; принятие решения об уровне детализации объектов АИС (логический – модель бизнес-процессов строится в терминах предметной области, происходит абстрагирование от физических объектов АИС; физический – модель бизнес-процесса строится в терминах предметной области с учетом содержания, строения и структуры АИС; логико-физический – строится одновременно два варианта моделей доступа).

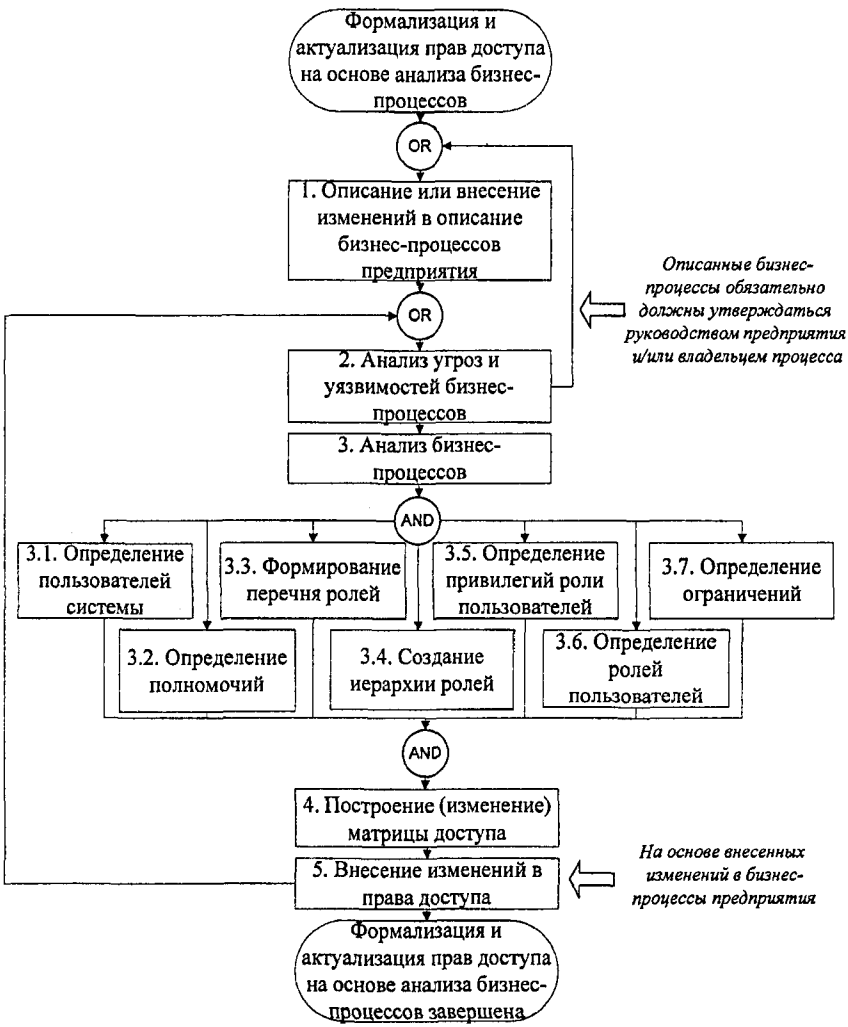

Рис. 3. Этапы формализации и актуализации прав доступа на основе анализа бизнес-процессов предприятия

В табл. 2 представлены возможные инструментальные средства и соответствующие им методологии для проведения работ по формализации и актуализации прав доступа.

Таблица 2.

Комбинации методологий бизнес-моделирования

Функциональная методология		Организационная методология	Среда моделирования
Верхний уровень	Нижний уровень		
IDEF0	IDEF3	Organization Chart	AllFusion Process Modeler
IDEF0	EPC	Организационная диаграмма; Оргдиаграмма	Business Studio
VAD	eEPC	Organization Diagram	ARIS

Как упоминалось выше, бизнес-процессы анализируются в целях получения необходимых данных для определения пользователей системы, их полномочий, формирования перечня ролей, создания иерархии ролей, определения привилегий конкретного пользователя, его ролей и ограничений. Рассмотрим основные компоненты данной модели.

Пусть $FF = \{ff_1, ff_2, \ldots, ff_a\}$ – конечное непустое множество функций, выполняемых участниками бизнес-процесса (исполнителями). Для каждой функции $ff \in FF$ в бизнес-процессе определено множество исполнителей $PP(ff) = \{pp_1(ff), pp_2(ff), \ldots, pp_d(ff)\}$. Множество исполнителей (должность, функциональная роль) функций обозначим $PP = \{pp_1, pp_2, \ldots, pp_e\}$, $PP \neq 0$ и $PP = \bigcup_{ff \in FF} PP(ff)$. Введем отношение подчиненности $<$ на множестве PP. Будем считать, что $pp_1 < pp_2$, если выполняется одно из двух условий:

а) pp_2 является непосредственным руководителем pp_1;

б) $\exists$цепочка $pp_1 = pp^{(0)}, pp^{(1)}, pp^2, \ldots, pp^n = pp_2$, т.ч. pp_1^i есть непосредственный руководитель pp_1^{i-1} для всех $i = \overline{1,n}$.

С каждым исполнителем pp связывается множество $FI(pp) = \{fi_1(pp), fi_2(pp), \ldots, fi_g(pp)\}$ – Ф.И.О. исполнителя, совокупность всех Ф.И.О. исполнителей обозначим $FI = \bigcup_{pp \in PP} FI(pp)$. Каждый элемент «ФИО исполнителя» $fi \in FI$ имеет метку $sfi(pp)$, которая содержится в его свойствах и будет ассоциирована с уровнем доступа. Множество свойств Ф.И.О. исполнителя обозначим $SFI = \{sfi_1, sfi_2, \ldots, sfi_y\}$.

Определено $IS = \{is_1, is_2, \ldots, is_o\}$ – конечное множество информационных систем. Поскольку ряд функций выполняется автоматизированным образом, и это получает свое отражение на модели бизнес-процесса, то можно ввести

бинарное отношение ***fis = {(ff, is), где ff ∈ FF, is ∈ IS, такие, что ff выполняется в информационной системе is}.***

Посредством автоматизированных функций выполняются операции над некоторым конечным множеством информационных объектов ***IO = {io$_1$, io$_2$, …, io$_u$}***. Каждый информационный объект ***io ∈ IO*** имеет метку ***sio(io)***, которая содержится в его свойствах и будет ассоциирована с уровнем доступа. Множество свойств обозначим ***sio = (sio$_1$, sio$_2$, …, sio$_j$)***. Информационная система связана с информационным объектом множество ***IS(io) = (is$_1$(io), is$_2$(io), …, is$_k$(io))***.

Вид операций определяется типом доступа исполнителя к информационному объекту, множество типов доступов обозначим ***AT***. Выполнение операции исполнителем над информационным объектом определяется тройкой ***Op = {op=(pp, io, at)}***, где ***pp ∈ PP***, ***io ∈ IO***, ***at ∈ AT***, такие, что ***pp*** выполняет операцию посредство ***at*** к ***io***.

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 каждое предприятие определяет самостоятельно исходя из специфики своего функционирования и принятой политики безопасности либо на основе законодательно утвержденных нормативно-методических документов. Тем не менее, его основу составляет классификация возможных угроз. В соответствии со спецификой функционирования АИС в ходе диссертационного исследования рассмотрены типовые угрозы при осуществлении бизнес-процессов и соответствующих им уязвимостей, описание которых представлено в основном тексте.

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. 4). 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.

Рис. 4. Классификация изменений деятельности предприятия в контексте актуализации прав доступа пользователей к ресурсам АИС

В результате анализа модели бизнес-процесса «Формализация и актуализация прав доступа» были выявлены следующие автоматизируемые функции: добавление информации о модели бизнес-процесса; импорт данных; ввод информации о несовместимых ролях; ввод информации о несовместимых привилегиях; проверка корректности прав доступа; обновление данных; настройка информационной системы; формирование отчетности.

Для реализации представленной функциональности разработан алгоритм автоматизированного формирования элементов обобщенной модели разграничения прав доступа из модели бизнес-процесса, который представлен в общем виде в нотации UML Activity Diagram (рис. 5).

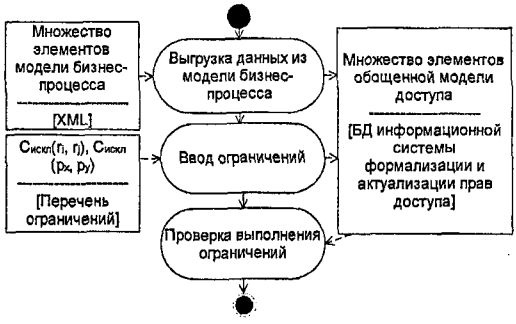

Рис. 5. Алгоритм автоматизированного формирования элементов обобщенной модели разграничения прав доступа из модели бизнес-процесса

Частичная детализация блока «Выгрузка данных из модели бизнес-процесса» представлена на рис. 6.

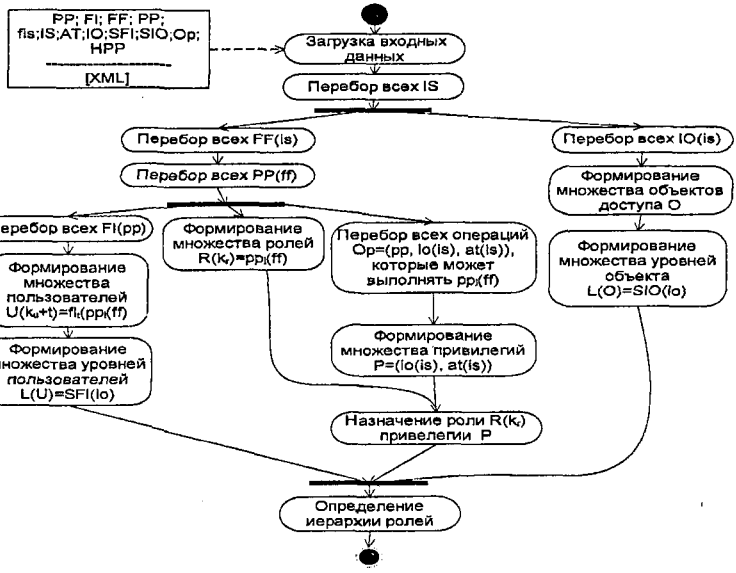

Рис. 6. Детализация блока «Выгрузка данных из модели бизнес-процесса»

Данный алгоритм должен быть детализирован для использования в конкретной среде бизнес-моделирования.

После изначальной формализации прав доступа наступает этап их актуализации, осуществляемый на основе сравнения состояния модели бизнес-процессов до и после внесения каких либо изменений. Актуализация прав доступа производится в соответствии с ранее разработанной классификацией деятельности предприятия. Для каждого классификационного признака были определены правила реагирования. Схематично алгоритм актуализации прав доступа к ресурсам автоматизированных информационных систем на основе изменений в моделях бизнес-процессов предприятия представлен на рис. 7.

Блок загрузки входных данных и фиксация факта изменений значения элемента бизнес-процесса осуществляется аналогично блоку выгрузки данных из модели бизнес-процесса алгоритма автоматизированного формирования элементов обобщенной модели разграничения прав доступа из модели бизнес-процесса. Производится перебор всех множеств элементов модели доступа. Проведена оценка сложности алгоритмов, согласно которой они попадают в категорию эффективных.

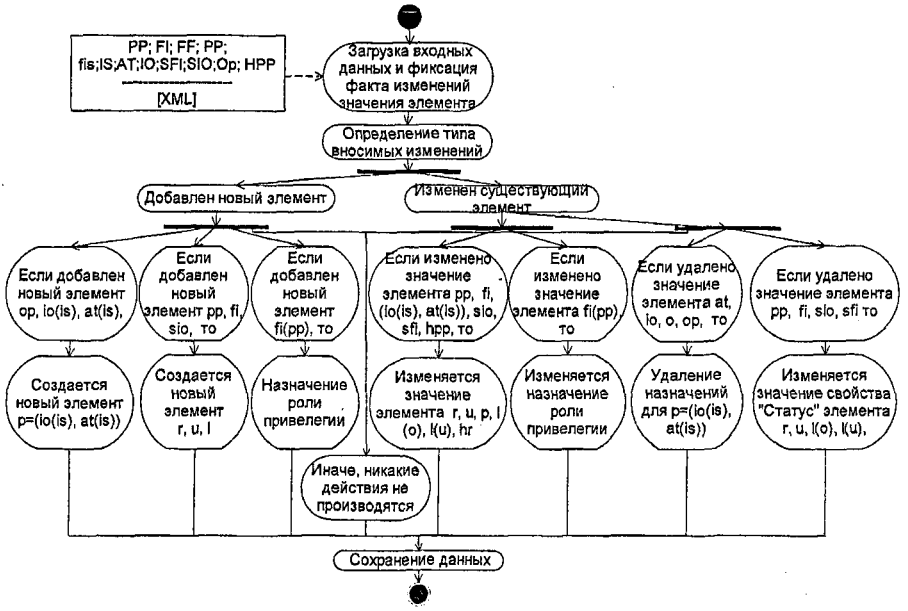

Рис. 7. Алгоритм актуализации прав доступа к ресурсам автоматизированных информационных систем на основе изменений в моделях бизнес-процессов

Разработана концептуальная модель базы данных (рис. 8). Представленная концептуальная модель была переведена в логическую и физическую модели базы данных.

Третья глава посвящена описанию результатов процесса разработки информационной системы формализации и актуализации прав доступа на основании полученного во второй главе проекта информационной системы.

В качестве средств реализации информационной системы формализации и актуализации прав доступа были выбраны: среда бизнес-моделирования – Business Studio 3.0.; СУБД – Microsoft SQL Server 2008; среда разработки – Microsoft Visual Studio 2008 (язык программирования C#); средство для построения отчетов – FastReport.

В связи с использованием для разработки информационной системы формализации и актуализации прав доступа объектно-ориентированного языка программирования была разработана диаграмма классов, отражающая классы, используемые непосредственно в программном коде.

Для создания базы данных на сервере базы данных был разработан соответствующий скрипт на языке Transact-SQL, который запускается в процессе установки информационной системы формализации и актуализации прав доступа.

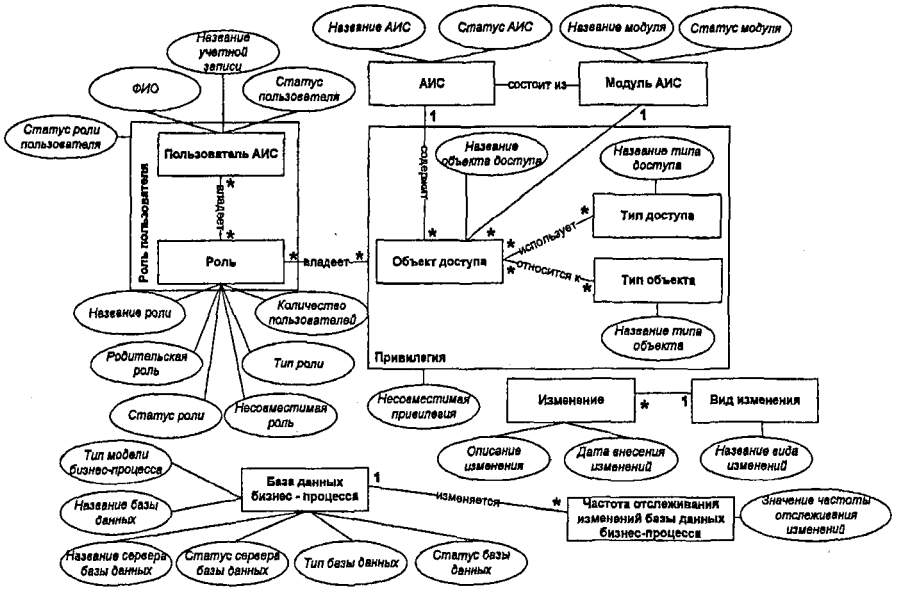

Рис. 8. Концептуальная модель базы данных информационной системы формализации и актуализации прав доступа

Алгоритм автоматизированного формирования элементов обобщенной модели разграничения прав доступа из модели бизнес-процессов реализован в виде двух процедур, одна – для формирования функциональных элементов обобщенной модели, вторая – для административных. Процедуры имеют одинаковую структуру. Работа процедуры начинается с определения действующей базы данных, имеющей определенный тип («функциональная» или «административная»). Далее выполняется ряд распределенных запросов на выборку (select) из таблиц базы данных модели бизнес-процесса в Business Studio. Данные, удовлетворяющие определенным условиям, сохраняются в базе данных информационной системы формализации и актуализации прав доступа посредством конструкции «insert into». Для формализации прав доступа потребовалось разработать двенадцать распределенных запросов.

Алгоритм актуализации прав доступа к ресурсам АИС на основе изменений в моделях бизнес-процессов предприятия был реализован с помощью девяти триггеров (добавление нового пользователя; установление пользователю статуса «не действующий»; изменение логина пользователя; создание новой роли; установление роли статуса «не действующая»; изменение названия роли; добавление новой АИС; установление АИС статуса «не действующая»; изменение названия АИС; добавление новой АИС; установление АИС статуса «не действующая»; изменение названия АИС; добавление нового модуля АИС; установление модулю АИС статуса «не

действующий»; изменение названия модуля АИС; добавление привилегии; назначение пользователя на роль; снятие назначения пользователя на роль; изменение привилегии). Каждый из триггеров запускается при добавлении (insert), изменении (update) или удалении (delete) данных в таблицах базы данных модели бизнес-процесса в Busienss Studio. Затем с помощью условных конструкций (if … then … else) определяется, какие изменения необходимо внести (insert into) в базу данных информационной системы формализации и актуализации прав доступа. После разработки алгоритмов была реализована информационная система формализации и актуализации прав доступа. Используя методы функционально-стоимостного анализа и имитационного моделирования, произведена оценка эффективности ее внедрения.

Основные результаты исследования

В диссертационной работе решены все поставленные задачи и достигнута цель исследования. Получены следующие основные результаты.

1. Основываясь на результатах проведенного анализа проблемы формализации и актуализации прав доступа пользователей к ресурсам АИС, построена модель информационной системы для решения указанной проблемы.

2. Разработаны и зарегистрированы программные компоненты информационной системы формализации и актуализации прав доступа в виде алгоритмов.

3. По результатам проведенных исследований создана и зарегистрирована информационная система формализации и актуализации прав доступа, реализующая подход на основе анализа бизнес-процессов предприятия. Указанная система внедрена на ряде предприятий, в том числе для формирования матриц доступа в рамках создания и обеспечения функционирования систем защиты информационных систем персональных данных.

4. Проведен функционально-стоимостной анализ и получены оценки эффективности применения подхода управления правами доступа на основе анализа бизнес-процессов, которые подтверждены результатами практического внедрения и свидетельствуют о сокращении финансовых и временных затрат на процесс формализации и актуализации прав доступа.

ПЕРЕЧЕНЬ ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИОННОЙ РАБОТЫ

Публикации в изданиях, рекомендованных ВАК для представления основных научных результатов диссертации

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

2. Родионова, З. В. Технология управления изменениями прав доступа на основе анализа бизнес-процессов / З. В. Родионова // Вестн. НГУЭУ. – 2011. – № 1 – С. 16–21.

Свидетельство РОСПАТЕНТа РФ:

3. Родионова З.В., Пестунова Т.М. Программа для ЭВМ. Информационная система формализации и актуализации прав доступа «BusinessProcessSecurity» // Свидетельство об официальной регистрации № 2011615409 от 19.10.2011.

Свидетельства ОФЕРНиО:

4. 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.
5. Родионова З.В., Пестунова Т.М. Алгоритм актуализации прав доступа к ресурсам автоматизированных информационных систем на основе изменений в моделях бизнес-процессов предприятия // Свидетельство о регистрации электронного ресурса Объединенного фонда электронных ресурсов «Наука и образование» № 17400 от 08.09.2011.

Учебные пособия, труды конференций, публикации в научных сборниках

6. Родионова, З. В. Технологии управления проектами : учеб. пособие / З. В. Родионова, О. М. Проталинский, Ю. В. Проталинская ; Сарат. гос. техн. ун-т. – Саратов : СГТУ, 2009. – 201 с.
7. Родионова, З. В. Управление проектами и программами : учеб. Пособие / З В. Родионова ; Сиб. гос. акад. гос. службы. – Новосибирск : СибАГС, 2010. – 156 с.
8. 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 науч.-техн. лит., 2008. – С. 91–96.
9. Родионова, З. В. Практические аспекты управления правами доступа / З. В. Родионова, Т.М. Пестунова // Научно-методические и нормативные материалы и документы IV Пленума СибРОУМО по образованию в области информационной безопасности : Материалы Пленума и доклады конференции. – Томск: «В-Спектр», 2010. – С. 204–209.

Родионова Зинаида Валерьевна

МОДЕЛИРОВАНИЕ И РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ ФОРМАЛИЗАЦИИ И АКТУАЛИЗАЦИИ ПРАВ ДОСТУПА

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 13.12.2011 г. Формат 60x84$^{1}/_{16}$. Тираж 100 экз.
Гарнитура Times New Roman. Усл. печ. л. 1,5.

Новосибирский государственный университет экономики и управления
630099, г. Новосибирск, ул. Каменская, 56