МОДЕЛЬ ВЕБ-ПОРТАЛА С ГРУППОРОЛЕВЫМ РАЗГРАНИЧЕНИЕМ ПРАВ ДОСТУПА

С. В. Иванов[1], С. В. Перминов[2]

Санкт-Петербургский институт информатики и автоматизации РАН

СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178

[1]<stan.ivanov@mail.ru>, [2]<sv.perminov@gmail.com>

УДК 004.4

Иванов С. В., Перминов С. В. **Модель веб-портала с группоролевым разграничением прав доступа** // Труды СПИИРАН. Вып. 7. — СПб.: Наука, 2009.

Аннотация. *В статье описана модель веб-портала с группо-ролевым разграничением доступа к ресурсам, хранимым в системе. Приведена диаграмма классов системы разграничения прав доступа. Описаны методы поддержания многоязычности веб-портала, приведены идеи по его дальнейшему развитию. Описываемая модель веб-портала используется в официальном портале Санкт-Петербургского научного центра РАН.* — Библ. 6 назв.

UDC 004.4

Ivanov S.V., Perminov S. V. **Model of web-portal with data access control system, based on groups and roles** // SPIIRAS Proceedings. Issue 7. — SPb.: Nauka, 2009.

Abstract. *This article describes model of web-portal with data access control system, based on groups and roles. Class diagram of access control system and methods of multilingual support are presented. Some ideas about further model development of this model are described. Described model is embedded in official web-portal of Saint Petersburg Scientific Center of the Russian Academy of Sciences.* — Bibl. 6 items.

1. Введение

Развитие веба в настоящее время предоставляет все более ценные и интересные возможности. Основная задача, которая ставилась перед вебом в прошлом — предоставление информации пользователям — перерастает в совместную обработку пользователями информации с целью накопления знаний. Средства веб-коммуникаций сейчас обеспечивают не только эффективное взаимодействие групп пользователей, но могут использоваться для увеличения интеграции внутри крупных географически распределенных организаций.

До настоящего времени веб-портал Санкт-Петербургского научного центра РАН не мог справиться с задачей своевременного и достоверного донесения информации до пользователей, что было связано с невозможностью обработки и предоставления информации самими сотрудниками РАН «от первого лица» с использованием средств портала. Нашей задачей явилась разработка веб-портала СПбНЦ РАН, который бы мог предоставить возможность создания сайтов подразделений РАН, управляемых сотрудниками этих подразделений. Кроме того, важно также было предусмотреть, чтобы портал не был слишком специфичным и мог использоваться различными организациями, не входящими в состав СПбНЦ РАН — университетами, школами и другими образовательными, научными и ненаучными организациями.

В данной статье описывается веб-портал Санкт-Петербургского научного центра РАН, в котором реализованы требования, описанные выше. Также описываются идеи дальнейшего развития функциональности веб-портала.

2. Требования, предъявляемые к веб-порталу

Портал должен предоставлять средства для совместного использования его ресурсов пользователями, в то же время обеспечивать для владельца ресурса механизмы управления разграничением доступа к этому ресурсу. Портал должен обеспечивать совместную и безопасную обработку данных группами пользователей и отдельными пользователями, предоставлять владельцам данных неограниченные права по их изменению, ограничению доступа или распространению, в рамках, не нарушающих права других пользователей портала.

Основные механизмы обеспечения безопасности:

1. Любой объект должен иметь владельца — группу пользователей, в контексте которой был создан объект, что обеспечивает более компетентное управление объектами портала.
2. Возможность ограничения доступа пользователей к данным для обеспечения их целостности и достоверности, а в некоторых ситуациях и приватности.
3. Наличие группы компетентных пользователей с различными правами доступа для обеспечения контроля над всеми данными и ресурсами портала и его отдельных пользователей и групп, включая законность данных, управление доступом к ресурсам, разрешение различных конфликтных ситуаций и блокировку нарушителей.

Портал должен в полной мере удовлетворять принципам открытых систем, не должен быть требовательным к вычислительным ресурсам и быть доступным в управлении.

3. Структура ресурсов портала

В основе архитектуры веб-портала лежит древовидная структура, которую можно также назвать системой каталогов.

Каждый раздел сайта может содержать подразделы. Каждый подраздел имеет только один родительский раздел, что исключает множественное наследование. Связывание разделов, между которыми нет зависимости родитель – потомок, происходит простыми гиперссылками.

Разделы мы будем называть ресурсами портала, а множество ресурсов, принадлежащее какой-либо группе пользователей веб-портала, сайтом этой группы. Вершина дерева ветки этих ресурсов – главная страница сайта группы пользователей.

Ресурсы в портале подразделяются на различные типы, от которых зависит набор возможных действий, предоставляемых по отношению к ресурсу, а также результат применения этих действий. В настоящий момент мы не определяем строго объекты, которые могут являться ресурсами портала, оставляя их достаточно абстрактными для дальнейшего расширения функциональности портала различными приложениями, в том числе грид-приложениями, и для его наполнения различными ресурсами, используемыми и создаваемыми этими приложениями.

Все пользовательские ресурсы портала (ресурсы, создаваемые его пользователями, в том числе администраторами) представлены набором строк в таблице «Resources» базы данных портала. Каждое свойство ресурса описывается одной строкой таблицы базы данных. Строка таблицы содержит тип ресурса, идентификатор ресурса, имя свойства ресурса, значение этого свойства и язык, для которого задано это значение (в случае, если значение свойства не

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

требует особого языка, является числом, датой, адресом файла и т.д., язык для него устанавливается в значение «any»).

Таким образом, база данных способна хранить любой тип ресурса без изменения своей структуры.

4. Система разделения прав доступа веб-портала

4.1. Обзор некоторых существующих моделей разделения прав доступа в процессе их эволюции

Самой распространенной и в то же время первой из появившихся моделей разграничения прав доступа (РПД) для веб-порталов является модель «один администратор, остальные — гости», в которой администрирование портала и управление его содержанием осуществляется единственным пользователем. Модель проста в реализации, прозрачна при определении зон ответственности пользователей, исключает проблему различия степени компетентности пользователей, но ограничена по объему выполняемых работ по администрированию портала и управлению его содержанием; организация портала с таким РПД — длительный процесс. Модель «один администратор, остальные – гости» легко расширяема до модели «много администраторов, остальные — гости», которая позволяет производить больший объем работ по администрированию и управлению содержанием портала. В то же время наличие у нескольких пользователей одинаковых прав по управлению всеми ветвями веб-портала зачастую приводит к несогласованным действиям. Ситуация еще более осложняется, когда различие степени компетентности администраторов ощутимо.

Поиск решения проблемы разделения зон ответственности в предыдущей модели РПД приводит к двум новым моделям: «один администратор, субадминистраторы, остальные — гости» и «один администратор, пользователи с различными правами доступа».

В модели «один администратор, субадминистраторы, остальные — гости» администратор назначает субадминистраторов, выполняющих функции администратора в разных ветвях портала, что позволяет производить большой объем работ по управлению веб-порталом. Портал, основанный на такой модели, прозрачен в определении сфер ответственности пользователей, проблема различия степени компетентности пользователей менее ощутима. Масштабируемость данной модели осложнена, модель имеет низкий уровень открытости для остальных пользователей — гостей.

В модели «один администратор, пользователи с различными правами» администратор распределяет зоны ответственности пользователей и назначает им права по управлению порталом в зоне их ответственности (в разных ветвях веб-портала). Модель имеет наименьшее количество минусов. Администратор в этом случае определяет роли пользователей (классы пользователей, обладающих определенными правами по управлению порталом). Основными проблемами этой модели является высокий уровень сложности ее реализации, более трудоемкий процесс отбора пользователей на те или иные роли.

Описываемая нами модель портала имеет систему РПД, основанную на последней модели.

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

4.2. Архитектура системы РПД веб-портала

Модель «один администратор, пользователи с различными правами доступа» имеет существенный недостаток — сложность при распределении ролей и масштабировании. Создание групп пользователей, каждая из которых имеет своих администраторов, могло бы решить эту проблему.

В нашем веб-портале каждая группа пользователей ответственна за определенную ветвь ресурсов и имеет свой набор ролей, а также системные роли «администратор» (обычно имеет полный набор прав на управление разделом) и гость (обычно не имеет никаких прав по отношению к ветви ресурсов или имеет только право на чтение некоторых типов ресурсов).

Пример разграничения полномочий между группами пользователей приведен на рис. 1. «Корневые» ресурсы групп обозначены дополнительным серым квадратом с названием группы; линиями показаны связи «родитель – потомок» между ресурсами: контроль над ресурсами осуществляется одной группой — черными линиями; контроль над ними осуществляется разными группами — серыми линиями.

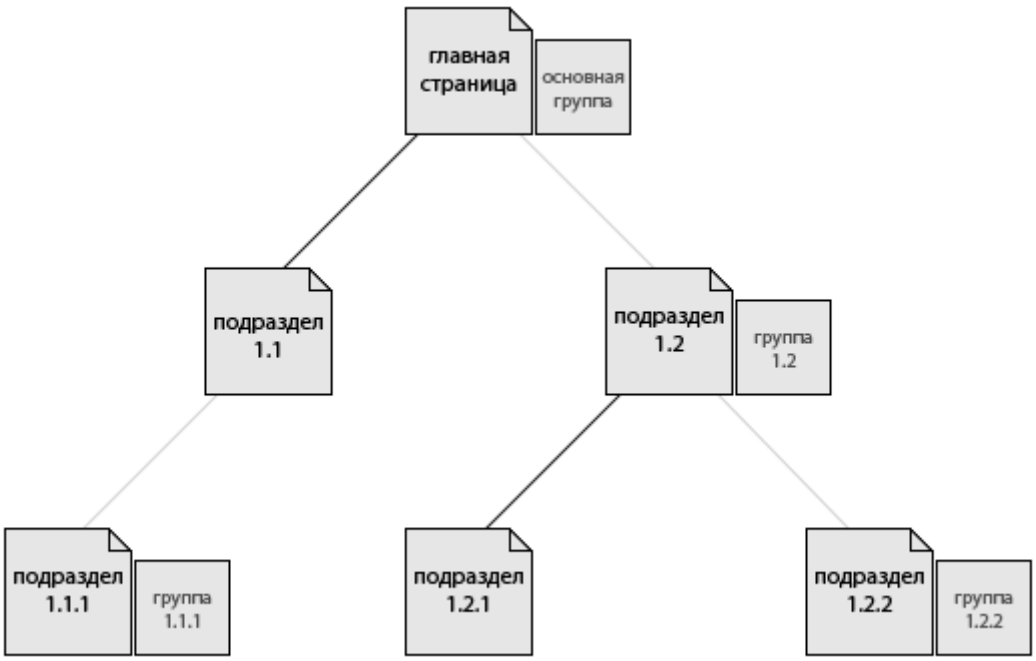

Рис. 1. Пример разграничения полномочий между группами пользователей.

При таком распределении полномочий могут возникнуть ситуации, когда та или иная группа пользователей не справляется со своими обязанностями по управлению вверенной ей ветвью ресурсов, что ведет к нарушению целостности веб-портала, низкому качеству предоставляемых им сервисов. В этой ситуации необходимо вмешательство в действия этой группы. Исходя из этих соображений, права пользователей родительской группы распространяются на ресурсы дочерней группы.

Таким образом, на нашем рисунке группы 1.2 и 1.1.1 управляются основной группой. А группа 1.2.2 управляется группой 1.2 и основной группой. Дан-

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ный подход приближает структуру групп веб-портала к структуре подразделений организации.

Кратко система характеризуется следующими высказываниями: группа пользователей обладает ресурсами, группа пользователей обладает ролями; роль обладает правами доступа; пользователь обладает ролями; группа пользователей управляет пользователем. Данные утверждения отражены в диаграмме классов системы РПД веб-портала, изображенной на рис. 2.

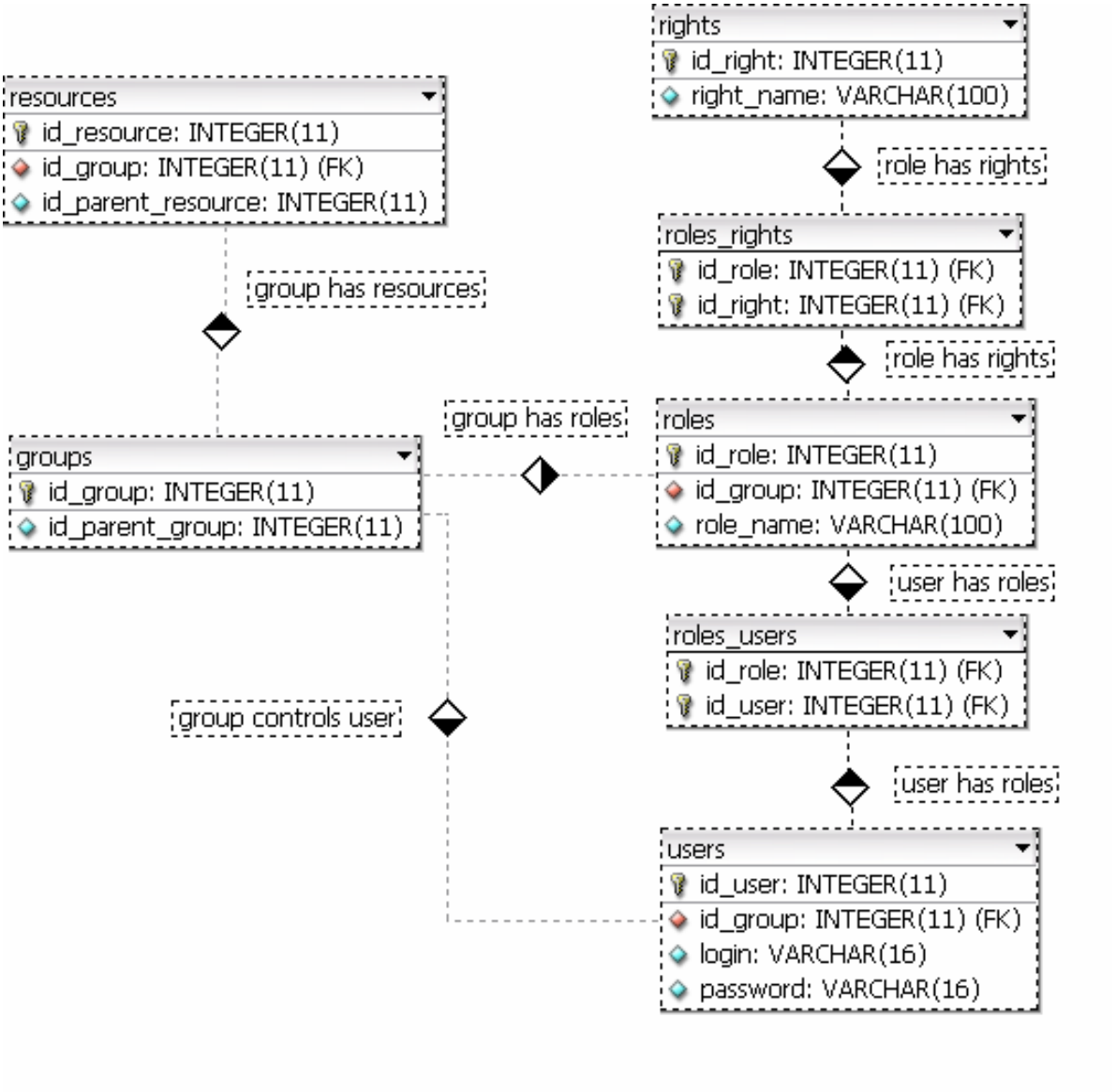

Рис. 2. Диаграмма классов системы разделения прав доступа.

Центральным объектом, создающим другие объекты, является группа пользователей. Она создает ресурсы и становится их владельцем, создает пользователей и получает права на управление ими, создает роли, которые действуют в рамках группы и ее дочерних групп, наполняет их правами доступа и распределяет между своими пользователями. Она также может создавать аккаунты пользователей или добавлять в свою группу существующих пользователей.

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Опишем процесс создания простой группы, ее ролей, пользователей и распределения ролей между пользователями группы.

Пользователь родительской группы, имеющий право на создание дочерних групп, создает дочернюю группу (изначально этот процесс начинается с создания корневой группы портала его root-пользователем — главным администратором портала, действия которого не ограничиваются системой разграничения доступа). Он создает в ней администратора и наделяет его всеми правами по отношению к созданной группе.

Администратор создает роль редактора, имеющего права доступа на создание и изменение ресурсов типа «новость» и «статья» данной группы, и роль сотрудника, имеющего права на чтение новостей и статей группы.

После этого он создает аккаунты для новых пользователей или добавляет существующих пользователей в группу и распределяет им роли.

В группе появляется сотрудники, которые могут читать новости и статьи группы, и редакторы, которые эти новости и статьи создают.

4.3. Оценка полученных результатов

Модель системы РПД веб-портала является масштабируемой и открытой для пользователей портала. Каждая ветвь портала всегда находится под управлением одной из групп пользователей, что позволяет четко разграничивать зоны ответственности. При этом каждая группа пользователей сохраняет свои права по отношению к ресурсам дочерних групп, что позволяет сохранять компетентный контроль над веб-порталом.

Модель классов системы РПД не представляется сложной, что упрощает реализацию и позволяет максимально оптимизировать ее работу. Управление веб-порталом организации, имеющей большое количество подразделений и четкую иерархию, представляется эффективным и рациональным процессом.

5. Обеспечение многоязычности

5.1. Обеспечение многоязычности пользовательских текстов

В описываемом портале текст, который должен представляться на различных языках в зависимости от выбора пользователя, разделяется на два типа:

1) пользовательские тексты — тексты, созданные пользователями портала и хранящиеся в ее базе данных;
2) тексты интерфейса — тексты, обеспечивающие доступность пользовательского интерфейса.

При обеспечении многоязычности этих двух типов используются два разных подхода.

Обеспечение многоязычности пользовательского текста во многом ложится на пользователя, создающего ресурс, — при публикации ресурса ему необходимо продублировать все свойства ресурса, которые могут быть многоязычными, на тех языках, на которых он хочет представить ресурс.

Далее, значения многоязычных свойств ресурса снабжаются в базе данных отметкой о языке, для которого они предназначены.

При работе с ресурсом значения его свойств выбираются в зависимости от того, какой язык в данный момент использует пользователь.

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Такой подход в сочетании с описанной выше структурой ресурсов портала позволяет снять ограничение на количество используемых порталом языков, не приводя к разрастанию функциональности или к изменению и дополнению структуры базы данных

5.2. Обеспечение многоязычности интерфейса

При обеспечении многоязычности важно, чтобы пользовательский интерфейс был представлен на том языке, который пользователь выбрал для работы с порталом.

Являясь в большей мере статичным, интерфейс не позволяет использовать при обработке его текстов те же методы, что и при обработке пользовательских текстов.

В портале эта проблема также решена достаточно эффективно. Все многоязычные тексты интерфейса определяются в нем шаблонами — адресами, по которым эти строки можно найти в библиотеках текстов интерфейса. Шаблон окружен специальными символами и представляет собой адрес значения в библиотеке, например «__First_name__», «__Title__», . В библиотеках все строки представляют собой элементы, однозначно определяемые адресами-шаблонами.

Все данные, выводимые порталом в стандартный поток в процессе подготовки ответа на запрос пользователя, буферизируются. После окончания обработки запроса все шаблоны в буфере заменяются их строковыми значениями на нужном языке, после чего содержимое буфера отдается в стандартный исходящий поток (отсылаются браузеру пользователя).

Чтобы использовать язык в интерфейсе, шаблоны должны иметь значения в библиотеке этого языка.

6. Заключение

Описанная нами модель веб-портала в настоящее время представлена веб-порталом Санкт-Петербургского научного центра РАН, расположенного по адресу <http://www.spbrc.nw.ru>.

В дальнейших планах — дополнение модели портала для создания на его основе платформы для веб- и грид-приложений, что позволит пользователям обрабатывать информацию не только в рамках функциональности, которую предлагает портал, но и с использованием приложений, реализованных самими пользователями. Эта задача требует еще более глубокой проработки вопросов безопасности системы и исследования тонкостей при взаимодействии различных приложений и совместной обработке ими данных. В то же время задача облегчается теми предпосылками, которые были заложены в портал уже сейчас — достаточная абстрактность типов ресурсов и эффективное разделение прав доступа, способное удовлетворить нужды виртуальных организаций.

Литература

Труды СПИИРАН. 2008. Вып. 7. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2008. Issue 7. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

1. *Kesselman C.,Foster I.* The Grid: Blueprint for a new computing infrastructure. Morgan Kaufmann Publishers, 1998. 701 c

2. *Гутманс Э, Баккен С.* PHP 5. Профессиональное программирование. СПб.: Символ-Плюс, 2006. 704 с.

3. *Ferraiolo D., Kuhn R., Chandramouli R.* Role-based access control. Artech House, 2003. 338 c.

4. *Balladelli M., Clercq J.* Mission-critical active directory: Architecting a secure and scalable infrastructure. Digital Press, 2001. 640 c.

5. *Siddiqui S.* Linux security. Course Technology PTR, 2002. 512 c.

6. *Тахагхогхи С., Вильямс Х.* Руководство по MySQL. Русская редакция, 2007. 544 с.