

(19)



**Евразийское
патентное
ведомство**

(11) **045814**

(13) **B1**

(12) **ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ**

(45) Дата публикации и выдачи патента
2023.12.28

(51) Int. Cl. **G06F 21/45** (2013.01)

(21) Номер заявки
201992218

(22) Дата подачи заявки
2018.04.19

(54) **СПОСОБ И СИСТЕМА ДЛЯ ПРЕДОСТАВЛЕНИЯ ПРАВ НА ОСНОВЕ ВЗАИМНО
ОДНОЗНАЧНОЙ СВЯЗИ РОЛИ С ПОЛЬЗОВАТЕЛЕМ**

(31) **201710268338.9**

(56) CN-A-107103228
CN-A-104919414
CN-A-1479232
CN-A-101667268
CN-A-103632082

(32) **2017.04.22**

(33) **CN**

(43) **2020.06.05**

(86) **PCT/CN2018/083812**

(87) **WO 2018/192557 2018.10.25**

(71)(73) Заявитель и патентовладелец:
**ЧЭНДУ ЦЯНЬНЮЦАО
ИНФОРМЕЙШН ТЕКНОЛОДЖИ
КО., ЛТД. (CN)**

(72) Изобретатель:
Чень Дачжи (CN)

(74) Представитель:
Носырева Е.Л. (RU)

(57) Согласно настоящему изобретению предложены способ и система для предоставления прав на основе взаимно однозначной связи роли с пользователем, при этом способ последовательно включает следующие этапы: S1: создание ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс; S2: предоставление прав для каждой роли, созданной на этапе S1; S3: связывание пользователей с ролями, при этом в один и тот же период одну роль можно связать лишь с одним пользователем, тогда как одного пользователя можно связывать с одной или несколькими ролями. Согласно настоящему изобретению роль представляет собой отдельную сущность, чем отличается от традиционной роли со свойствами группы/класса, при этом в один и тот же период одну роль можно связать лишь с одним пользователем, что значительно повышает эффективность управления правами при использовании системы, делает динамическое предоставление прав более простым, более удобным, а также более ясным и понятным и повышает эффективность и надежность установки прав.

045814
B1

045814
B1

Область техники

Настоящее изобретение относится к способам управления правами пользователей в системах административного программного обеспечения, таких как EPR, и, в частности, оно относится к способу и системе для предоставления прав на основе взаимно однозначной связи роли с пользователем.

Предпосылки изобретения

Управление доступом на основе ролей (RBAC) представляет собой механизм управления правами в отношении баз данных, который является наиболее изученным и наиболее сложившимся за последние годы, при этом оно считается наиболее подходящей заменой традиционному мандатному управлению доступом (MAC) и дискреционному управлению доступом (DAC). Основная идея управления доступом на основе ролей (RBAC) заключается в разграничении разных ролей на основании различных выполняемых обязанностей и занимаемых должностей в структуре организации предприятия, при этом роли предусматривают права доступа к ресурсам баз данных, и пользователи, которым присваиваются разные роли, опосредованно получают доступ к ресурсам баз данных.

В больших прикладных системах постоянно генерируется большое количество таблиц и схем, что очень усложняет управление и предоставление прав в отношении ресурсов баз данных. Поскольку пользователям весьма трудно непосредственно управлять получением и предоставлением доступа и прав, касающихся ресурсов баз данных, необходимо, чтобы пользователи предельно полно понимали структуру баз данных и были хорошо знакомы с применением языка SQL; кроме того, если структура прикладной системы или требования безопасности каким-либо образом изменяются, то требуется осуществить большое количество сложных и трудоемких изменений по предоставлению прав, при этом очень легко возникают слабые места в системе безопасности, обусловленные неожиданными ошибками в предоставлении прав. Поэтому разработка простого и высокоэффективного способа управления правами для больших прикладных систем уже стала общей необходимостью для систем и пользователей систем.

Посредством механизма управления правами на основе ролей можно осуществлять простое и высокоэффективное управление правами доступа к системе, значительно уменьшить нагрузку и стоимость управления правами в системе и сделать управление правами в системе еще более соответствующим стандартам оперативного управления прикладными системами.

Тем не менее, в традиционных способах управления правами пользователей на основе ролей применяется механизм связывания ролей с пользователями по принципу "один ко многим", в котором "роль" представляет собой свойство группы/класса, то есть одна роль может одновременно соответствовать нескольким пользователям/быть связанной с ними, и роль аналогична такому понятию, как должность/служебное положение/рабочая специальность и т.д.; в случае такого механизма связывания предоставление прав пользователю делится в основном на следующие три типа: 1) непосредственное предоставление прав пользователю, показанное на фиг. 1, недостатками которого являются большой объем работы и выполнение неоднократно повторяющихся и трудоемких операций; 2) предоставление прав для роли (со свойствами класса/группы/должности/рабочей специальности), показанное на фиг. 2 (одна роль может связывать несколько пользователей), при этом пользователи получают права на основании роли; 3) комбинация двух вышеуказанных способов, как показано на фиг. 3.

Как было указано выше, в типах 2 и 3 необходимо предоставлять права для роли со свойствами класса/группы, а способы, в которых права предоставляют на основании роли со свойствами класса/группы/должности/рабочей специальности, характеризуются следующими недостатками: 1. Операции, выполняемые при изменении прав пользователя, являются трудными: в процессе реального применения системы часто необходимо корректировать права пользователей в процессе ведения деятельности: например, при проведении изменений прав сотрудников изменяются права какого-либо сотрудника, с которым связана определенная роль, но нельзя изменить права для всей роли из-за изменения прав одного сотрудника, поскольку эта роль также связана с другими сотрудниками, права которых не изменились. Поэтому для решения этой ситуации либо создают новую роль в пользу сотрудника, права которого изменились, либо такому сотруднику непосредственно предоставляют права на основании потребности в правах (без привязки к роли). В двух вышеуказанных способах управления, если прав для роли относительно много, то при предоставлении прав для роли не только требуется много времени, но и легко совершить ошибки, поэтому работа пользователей становится более напряженной и трудоемкой, а также легко совершить ошибки, из-за которых у пользователей системы возникают проблемы.

2. Трудно долгое время сохранять в памяти конкретные права, отведенные для ролей: если функций прав для роли относительно много, то долгое время сохранять в памяти конкретные права очень тяжело и еще труднее не забыть разницу в правах для ролей со схожими правами, и если надо связать с ролью нового пользователя, то невозможно точно решить, как выбрать роль, с которой его связать.

3. Поскольку права пользователей изменяются, то будет создаваться все больше ролей (если не создавать новые роли, то непосредственное предоставление прав пользователям значительно участится), и станет еще труднее точно понимать конкретную разницу между правами для всех ролей.

4. При переводе, если много прав пользователя, которого переводят, надо распределить между другими пользователями, то при выполнении этого необходимо разделить права пользователя, которого переводят, и затем создать для них роли, которые связывают с другими пользователями; такая операция не

только характеризуется сложностью и требует времени, но при ее выполнении также очень легко совершить ошибки.

Краткое описание изобретения

Техническая задача.

Задача настоящего изобретения заключается в преодолении недостатков аналогов, известных из предшествующего уровня техники, и в предоставлении способа и системы для предоставления прав на основе взаимно однозначной связи роли с пользователем, при этом в один и тот же период одну роль можно связать лишь с одним пользователем, что значительно повышает эффективность управления правами при использовании системы, делает динамическое предоставление прав более простым, более удобным, а также более ясным и понятным и повышает эффективность и надежность установки прав.

Решение задачи. Технические решения.

Решение задачи настоящего изобретения обеспечивается следующими техническими решениями: способ предоставления прав на основе взаимно однозначной связи роли с пользователем, последовательно включающий следующие этапы: S1: создание ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс; S2: предоставление прав для каждой роли, созданной на этапе S1; S3: связывание пользователей с ролями, при этом в один и тот же период одну роль можно связать лишь с одним пользователем, тогда как одного пользователя связывают с одной или несколькими ролями.

Предоставление прав для роли включает предоставление прав в отношении списков, предоставление прав в отношении меню или предоставление прав в отношении функций.

При создании указанной роли необходимо выбрать одно отделение; после создания роли эта роль будет относиться к этому отделению и эта роль в этом отделении будет единственной, при этом для роли предоставляются права на основании должностных обязанностей роли.

Способ предоставления прав на основе взаимно однозначной связи роли с пользователем дополнительно включает этап управления переводом пользователя в другое отделение, в частности, включающий: (1) удаление связи пользователя с ролью в прежнем отделении; (2) связывание пользователя с ролью в новом отделении.

Назначение прав указанному пользователю возможно только на основании его связи с ролью.

Способ предоставления прав на основе взаимно однозначной связи роли с пользователем последовательно включает следующие этапы: S1: создание ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс; S2: связывание пользователей с ролями, при этом в один и тот же период одну роль можно связать лишь с одним пользователем, тогда как одного пользователя связывают с одной или несколькими ролями; S3: предоставление прав для каждой роли, созданной на этапе S1.

Предоставление прав для роли включает предоставление прав в отношении списков, предоставление прав в отношении меню или предоставление прав в отношении функций.

При создании указанной роли необходимо выбрать одно отделение; после создания роли эта роль будет относиться к этому отделению и эта роль в этом отделении будет единственной, при этом для роли предоставляются права на основании должностных обязанностей роли.

Способ предоставления прав на основе взаимно однозначной связи роли с пользователем дополнительно включает этап управления переводом пользователя в другое отделение, в частности, включающий: (1) удаление связи пользователя с ролью в прежнем отделении; (2) связывание пользователя с ролью в новом отделении.

Назначение прав указанному пользователю возможно только на основании его связи с ролью.

Система для предоставления прав на основе взаимно однозначной связи роли с пользователем содержит модуль для создания роли, модуль для предоставления прав для роли и модуль для связывания пользователя с ролью; указанный модуль для создания роли предназначен для обеспечения конфигурации ролей на основании должностей и создания системных ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс; указанный модуль для предоставления прав для роли предназначен для назначения прав роли на основании должностных обязанностей роли; указанный модуль для связывания пользователя с ролью предназначен для связывания пользователя с ролями и обеспечивает то, что в один и тот же период одну роль можно связать лишь с одним пользователем, тогда как одного пользователя связывают с одной или несколькими ролями.

Структура указанных системных ролей следующая: название должности плюс номер должности.

Положительные эффекты изобретения

Положительные эффекты.

1. В традиционных механизмах управления правами роль определяется как свойство группы, рабочей специальности, класса и т.д., и роль связывается с пользователем по принципу "один ко многим"; в процессе реального применения системы часто необходимо корректировать права пользователей в процессе ведения деятельности: например, при проведении изменений прав сотрудников изменяются права какого-либо сотрудника, с которым связана определенная роль, но нельзя изменить права для всей роли из-за изменения прав одного сотрудника, поскольку эта роль также связана с другими сотрудниками, права которых не изменились. Поэтому для решения этой проблемы либо создают новую роль в пользу сотрудника, права которого изменились, либо такому сотруднику непосредственно предоставляют права

на основании потребности в правах (без привязки к роли). В двух вышеуказанных способах управления, если прав для роли относительно много, то при предоставлении прав для роли не только требуется много времени, но и легко совершить ошибки, поэтому работа пользователей становится более напряженной и трудоемкой, а также легко совершить ошибки, из-за которых у пользователей системы возникают проблемы.

Тем не менее, в способе, представленном в этом документе, для решения этой проблемы просто можно выборочно изменить права для роли, поскольку роль представляет собой одну отдельную сущность. В способе, представленном в этом документе, несмотря на то, что кажется, что при инициации системы увеличится объем работы, тем не менее, за счет копирования и т.д., его эффективность в создании ролей или предоставлении прав может быть выше, чем в случае традиционных ролей со свойствами группы; поскольку не нужно учитывать общность ролей со свойствами группы при обеспечении связывания с пользователями; представленное в этом документе решение делает установку прав ясной и понятной; в частности, после применения системы определенное время (динамическое изменение пользователя/прав для роли) представленное в этом документе решение может значительно повысить для пользователей системы эффективность управления правами при применении системы, что делает динамическое предоставление прав более простым, более удобным, а также более ясным и понятным и повышает эффективность и надежность установки прав.

2. В традиционных способах на основе ролей со свойствами группы при предоставлении прав легко допустить ошибки, тогда как в представленном в этом документе способе вероятность допустить ошибки в предоставлении прав значительно снижается, поскольку в представленном в этом документе способе необходимо учитывать только роль, которая представляет собой отдельную сущность, и не надо учитывать, какими общностями характеризуются несколько пользователей, которые связываются с ролью со свойствами группы в традиционных способах. То есть допущенные ошибки в предоставлении прав также будут касаться только того одного пользователя, с которым связана эта роль, тогда как в случае традиционной роли со свойствами группы они будут касаться всех пользователей, с которыми связана эта роль. Даже если возникнут ошибки в предоставлении прав, то представленный в этом документе способ исправления является простым и требует мало времени, тогда как в случае традиционной роли со свойствами группы при исправлении ошибок необходимо учитывать общность прав всех пользователей, с которыми связана эта роль, и в случае большого количества функций внесение изменений является трудоемким и сложным, очень легко допустить ошибки и во многих ситуациях решением может служить только возможность создания новой роли.

3. В традиционных способах предоставления прав на основе ролей со свойствами группы, если функций прав для роли относительно много, то долгое время сохранять в памяти конкретные права очень тяжело и еще труднее не забыть разницу в правах для ролей со схожими правами, и если надо связать с ролью нового пользователя, то невозможно точно решить, как выбрать роль, с которой его связать. Роли, используемые в представленном в этом документе способе, сами по себе содержат свойство в виде номера должности/номера служебного положения, поэтому как выбирать понятно сразу.

4. При переводе, если много прав пользователя, которого переводят, надо распределить между другими пользователями, то при выполнении этого необходимо разделить права пользователя, которого переводят, и затем создать для них роли, которые связывают с другими пользователями; такая операция не только характеризуется сложностью и требует времени, но при ее выполнении также очень легко совершить ошибки.

В представленном в этом документе способе предусмотрено следующее: пользователь, которого переводят, связан с несколькими ролями, и при переводе сначала удаляют связи пользователя с ролями в прежнем отделении (эти несколько ролей, с которыми удаляют связи, можно снова связать с другими пользователями), а затем просто связывают пользователя с ролями в новом отделении. Такая операция является простой, и не будут допущены ошибки.

5. При создании роли необходимо выбрать одно отделение, и после создания этой роли отделение нельзя менять, при этом отделение для роли нельзя менять по следующим причинам: причина 1 - поскольку свойство представленной в этом документе роли отождествляется с одним номером служебного положения/номером должности, должностные обязанности/права под номерами разных служебных положений/номерами разных должностей являются разными: например, роль продавца 1 в отделе сбыта и роль разработчика 1 в техническом отделе содержат номера абсолютно разных служебных положений/должностей, поэтому права для них являются разными; причина 2 - если отделение (отдел сбыта), к которому относится роль продавца 1, поменять на технический отдел и при этом не изменить права для роли продавца 1, то в техническом отделе будет одна роль с правами сотрудника отдела сбыта, что приведет к беспорядку в управлении и возникновению слабых мест в системе безопасности.

Краткое описание прилагаемых графических материалов

Описание прилагаемых графических материалов:

на фиг. 1 представлено схематическое изображение способа непосредственного предоставления прав пользователю системой, известного из уровня техники;

на фиг. 2 представлено схематическое изображение способа предоставления системой прав для ро-

ли со свойствами группы/класса, известного из уровня техники;

на фиг. 3 представлено схематическое изображение известного из уровня техники способа, сочетающего в себе непосредственное предоставление прав пользователю системой и предоставление прав для роли со свойствами группы/класса;

на фиг. 4 представлено схематическое изображение способа предоставления системой пользователю прав на основе роли, представляющей собой отдельную сущность, согласно настоящему изобретению;

на фиг. 5 представлена блок-схема способа предоставления прав согласно настоящему изобретению.

Варианты осуществления изобретения

Способы осуществления настоящего изобретения.

Ниже технические решения согласно настоящему изобретению описаны более подробно со ссылкой на прилагаемые графические материалы, однако объем защиты настоящего изобретения изложенным ниже не ограничивается.

Вариант осуществления 1. Как показано на фиг. 1, способ предоставления прав на основе взаимно однозначной связи роли с пользователем последовательно включает следующие этапы: S1: создание ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс; S2: предоставление прав для каждой роли, созданной на этапе S1; S3: связывание пользователя с ролями, при этом в один и тот же период одну роль можно связать лишь с одним пользователем, тогда как одного пользователя связывают с одной или несколькими ролями; после связывания пользователя с ролью этот пользователь будет обладать всеми правами на выполнение деятельности, отведенными для этой роли. Кроме того, права пользователя могут определяться только его связью с ролью, и если необходимо изменить права пользователя, то изменение прав пользователя, связанного с этой ролью, выполняют корректировкой прав, предоставленных для роли; Пользователю права предоставляются не непосредственно, и предоставление прав пользователю осуществляется на основании связанной с ним роли.

Связь роли с пользователем является взаимно однозначной (после связывания роли с одним пользователем другие пользователи больше не могут быть связаны с ролью, а если роль не связана с каким-либо пользователем, то она может быть выборочно связана с другими пользователями). Связь пользователя с ролью представляет собой связь "один ко многим" (один пользователь может быть одновременно связан с несколькими ролями).

Определение роли: роль характеризуется не свойствами группы/класса/категории/должности/служебного положения/рабочей специальности и т.п., а лишь свойством отсутствия коллективности, для роли характерна уникальность, и роль представляет собой отдельную сущность, существующий независимо; при применении в производственных и непроизводственных организациях она соответствует номеру должности (в этом документе номер должности не является должностью, одну должность одновременно может занимать несколько сотрудников, но в один и тот же период один номер должности может соответствовать лишь одному сотруднику).

Например, в системе некоторой фирмы могут быть введены следующие роли: генеральный директор, заместитель генерального директора 1, заместитель генерального директора 2, управляющий отделом продаж в Пекине 1, управляющий отделом продаж в Пекине 2, управляющий отделом продаж в Пекине 3, специалист по организации сбыта в Шанхае 1, специалист по организации сбыта в Шанхае 2, специалист по организации сбыта в Шанхае 3, специалист по организации сбыта в Шанхае 4, специалист по организации сбыта в Шанхае 5 и т. д. Отношение связи пользователя с ролью: если сотрудник этой фирмы Чжан Сань назначен на должность заместителя генерального директора 2 в этой фирме и одновременно назначен на должность управляющего отделом продаж в Пекине 1, то роли, с которыми Чжан Саня необходимо связать, являются заместитель генерального директора 2 и управляющий отделом продаж в Пекине 1, и Чжан Сань будет обладать правами для этих двух ролей.

Предоставление прав для роли: система для предоставления прав для роли содержит без ограничения предоставление прав в отношении списков, предоставление прав в отношении меню или предоставление прав в отношении функций. Предоставление прав на операции со списками содержит без ограничения добавление, удаление, вставку и изменение.

Понятие традиционной роли предполагает свойства группы/класса/должности/служебного положения/рабочей специальности, при этом одна роль может соответствовать нескольким пользователям. В этой заявке понятие "роль" соответствует номеру должности/номеру служебного положения, а также похоже на роль в кино и телесериалах: одна роль в один и тот же период (в детстве, юности, зрелом возрасте и т. д.) может быть исполнена лишь одним актером, а один актер может быть способен исполнить несколько ролей.

Предоставление прав для роли включает без ограничения предоставление прав в отношении списков, предоставление прав в отношении меню или предоставление прав в отношении функций.

При создании указанной роли необходимо выбрать одно отделение; после создания роли эта роль будет относиться к этому отделению и эта роль в этом отделении будет единственной, при этом для роли предоставляются права на основании должностных обязанностей роли.

Если пользователь хочет сменить отделение, то имеет место перевод в другое отделение, и конкретная операция, выполняемая при этом, включает: (1) удаление связи пользователя с ролью в прежнем отделении; (2) связывание пользователя с ролью в новом отделении.

После создания роли роль можно связывать в процессе создания пользователя, а также ее можно связывать в любое время после создания пользователя. После связывания пользователя с ролью отношение связи с ролью можно в любое время удалить и также можно в любое время создать отношение связи с другими ролями.

Вариант осуществления 2. Способ предоставления прав на основе взаимно однозначной связи роли с пользователем последовательно включает следующие этапы: S1: создание ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс; S2: связывание пользователя с ролями, при этом в один и тот же период одну роль можно связать лишь с одним пользователем, тогда как одного пользователя связывают с одной или несколькими ролями; S3: предоставление прав для каждой роли, созданной на этапе S1.

Вариант осуществления 3. Для выполнения рассмотренного выше способа предоставления прав предложена система для предоставления прав на основе взаимно однозначной связи роли с пользователем, которая должна содержать по меньшей мере модуль для создания роли, модуль для предоставления прав для роли и модуль для связывания пользователя с ролью; указанный модуль для создания роли предназначен для обеспечения конфигурации ролей на основании должностей и создания системных ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс; структура указанных системных ролей следующая: название должности плюс номер должности; например, производственный рабочий цеха 1, производственный рабочий цеха 2, производственный рабочий цеха 3 и т.д.; роль представляет собой отдельную сущность, соответствует понятию номер должности и номер служебного положения и отличается от роли в традиционных системах управления правами: в традиционных системах понятие роли предполагает свойства групп/классов, например должность/служебное положение/рабочая специальность и т.д.

Указанный модуль для предоставления прав для роли предназначен для назначения прав роли на основании должностных обязанностей роли; указанный модуль для связывания пользователя с ролью предназначен для связывания пользователя с ролями и обеспечивает то, что в один и тот же период одну роль можно связать лишь с одним пользователем, тогда как одного пользователя связывают с одной или несколькими ролями.

Вариант осуществления 4. Ниже приведен пример связывания сотрудников и пользователей с ролями, после того как Чжан Сань стал сотрудником некоторой фирмы: 1. Вступление в новую должность: сотрудник вступает в новую должность, и достаточно непосредственно выбрать для пользователя (сотрудника) роль с соответствующим номером должности/номером служебного положения и связать их: например, Чжан Сань приходит на фирму (фирма назначает Чжан Саня пользователем Чжан Санем), при этом в его должностные обязанности входит отвечать за сбыт холодильников в отделе сбыта 1 в области Пекина (соответствующая роль представляет собой роль "специалиста по организации сбыта 5" в отделе сбыта 1), и непосредственно выбирают связать пользователя Чжан Саня с ролью "специалиста по организации сбыта 5".

2. Увеличение количества обязанностей: после того как Чжан Сань проработал некоторое время, фирма назначает Чжан Саня отвечать также за сбыт телевизоров в области Пекина (соответствующая роль представляет собой роль "специалиста по организации сбыта 8" в отделе сбыта 1) и по совместительству главным менеджером отдела послепродажного обслуживания (что соответствует роли главного менеджера отдела послепродажного обслуживания 1), и пользователя Чжан Саня дополнительно связывают с ролью "специалиста по организации сбыта 8" в отделе сбыта 1 и ролью "главного менеджера отдела послепродажного обслуживания 1" в отделе послепродажного обслуживания; теперь сотрудник Чжан Сань связан с тремя ролями как "специалист по организации сбыта 5" и "специалист по организации сбыта 8" в отделе сбыта 1 и как "главный менеджер отдела послепродажного обслуживания 1" в отделе послепродажного обслуживания соответственно, поэтому пользователь Чжан Сань обладает правами для этих трех ролей.

3. Уменьшение количества обязанностей: по прошествии некоторого периода времени фирма решает сделать Чжан Саня управляющим отделом послепродажного обслуживания (что соответствует роли "управляющий отделом послепродажного обслуживания" в отделе послепродажного обслуживания) без совместительства с другими должностями. Тогда пользователя Чжан Саня связывают с ролью "управляющего отделом послепродажного обслуживания" в отделе послепродажного обслуживания и при этом удаляют три связанные с ним ранее роли ("специалист по организации сбыта 5" и "специалист по организации сбыта 8" в отделе сбыта 1 и "главный менеджер отдела послепродажного обслуживания 1" в отделе послепродажного обслуживания), и теперь пользователь Чжан Сань обладает правами только для роли "управляющего отдела послепродажного обслуживания" в отделе послепродажного обслуживания.

4. Корректировка прав для роли (касается корректировки прав, предусмотренных для самой роли): если фирма решает расширить права управляющего отдела послепродажного обслуживания, то необходимо лишь добавить права для роли управляющего отделом послепродажного обслуживания, и в резуль-

тате увеличения объема прав для роли пользователя Чжан Саня как управляющего отделом послепродажного обслуживания объем прав пользователя Чжан Саня тоже увеличится.

5. Уход с должности: по прошествии года Чжан Сань увольняется, и тогда просто удаляют связь пользователя Чжан Саня с ролью "управляющего отделом послепродажного обслуживания" в отделе послепродажного обслуживания.

Например, в ходе динамического ведения деятельности фирмы назначение на должность и уход с должности сотрудников обычно происходят постоянно, тогда как номера должности/номера служебного положения изменяются крайне редко (и даже остаются без изменений в течение определенного периода времени).

Традиционный способ предоставления прав: в случае большого количества системных функций предоставление прав для традиционных ролей со свойствами группы/класса характеризуется не только большим объемом сложной работы по предоставлению прав, но и высокой вероятностью допущения ошибок, вплоть до того, что у пользователя системы легко возникают проблемы, поскольку допущенные ошибки тяжело обнаружить за короткий период времени.

Способ предоставления прав согласно настоящему изобретению: согласно настоящему изобретению права предоставляются для ролей с номером должности/номером служебного положения, при этом для назначения прав пользователя связывают с ролями, и управление правами пользователя осуществляется просто на основании отношения связи пользователя с ролью; это позволяет упростить управление правами и облегчить работу, а также обеспечивает ясность, что значительно повышает эффективность и надежность предоставления прав.

Рассмотренное выше представляет собой только предпочтительные способы осуществления настоящего изобретения, и следует понимать, что настоящее изобретение вовсе не ограничивается вариантами, раскрытыми в этом документе, которые не должны рассматриваться как исключающие другие варианты осуществления, но могут применяться для любых других комбинаций, изменений и среды, поэтому без отклонения от рассмотренной сути настоящего изобретения в него можно вносить изменения на основании указанных выше идей или же технологий или знаний из смежных областей. Кроме того, если не имеет места отступление от идеи и объема настоящего изобретения, изменения и модификации, предложенные специалистами в данной области техники, должны входить в объем защиты настоящего изобретения, определяемый прилагаемой формулой изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Компьютерно-реализуемый способ предоставления прав на основе взаимно однозначной связи роли с пользователем, отличающийся тем, что последовательно включает следующие этапы:

S1: создание ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс;

S2: предоставление прав для каждой роли, созданной на этапе S1;

S3: связывание пользователей с ролями, при этом в один и тот же период связывание одной роли возможно лишь с одним пользователем, тогда как одного пользователя связывают с одной или несколькими ролями;

при этом во время создания роли выбирают одно отделение, при этом после создания роли эта роль относится к выбранному отделению, эта роль в этом отделении является единственной, и для роли предоставляют права на основании должностных обязанностей роли, и при этом после создания роли отделение для роли менять нельзя;

при этом способ дополнительно включает этап управления переводом пользователя в другое отделение, включающий:

(1) удаление связи пользователя с ролью в прежнем отделении;

(2) связывание пользователя с ролью в новом отделении.

2. Способ по п.1, отличающийся тем, что назначение прав указанному пользователю возможно только на основании его связи с ролью.

3. Компьютерно-реализуемый способ предоставления прав на основе взаимно однозначной связи роли с пользователем, отличающийся тем, что последовательно включает следующие этапы:

S1: создание ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс;

S2: связывание пользователей с ролями, при этом в один и тот же период связывание одной роли возможно лишь с одним пользователем, тогда как одного пользователя связывают с одной или несколькими ролями;

S3: предоставление прав для каждой роли, созданной на этапе S1;

при этом во время создания роли выбирают одно отделение, при этом после создания роли эта роль относится к выбранному отделению, эта роль в этом отделении является единственной, и для роли предоставляют права на основании должностных обязанностей роли, и при этом после создания роли отделение для роли менять нельзя;

при этом способ дополнительно включает этап управления переводом пользователя в другое отделение, включающий:

- (1) удаление связи пользователя с ролью в прежнем отделении;
- (2) связывание пользователя с ролью в новом отделении.

4. Способ по п.3, отличающийся тем, что назначение прав указанному пользователю возможно только на основании его связи с ролью.

5. Компьютеризированная система для предоставления прав на основе взаимно однозначной связи роли с пользователем, отличающаяся тем, что содержит модуль для создания роли, модуль для предоставления прав для роли и модуль для связывания пользователя с ролью; при этом

указанный модуль для создания роли выполнен с возможностью обеспечения конфигурации ролей на основании должностей и создания системных ролей, при этом каждая роль представляет собой отдельную сущность, а не группу/класс;

указанный модуль для предоставления прав для роли выполнен с возможностью назначения прав роли на основании должностных обязанностей роли;

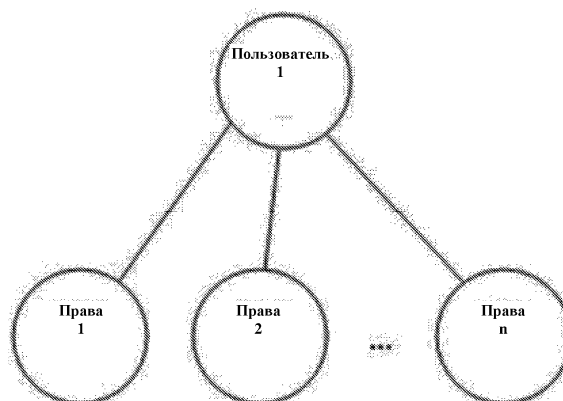
указанный модуль для связывания пользователя с ролью выполнен с возможностью связывания пользователя с ролями и обеспечивает то, что в один и тот же период связывание одной роли возможно лишь с одним пользователем, но при этом связывание одного пользователя возможно с одной или несколькими ролями;

при этом во время создания роли выбирают одно отделение, при этом после создания роли эта роль относится к выбранному отделению, эта роль в этом отделении является единственной, и для роли предоставляют права на основании должностных обязанностей роли, и при этом после создания роли отделение для роли менять нельзя;

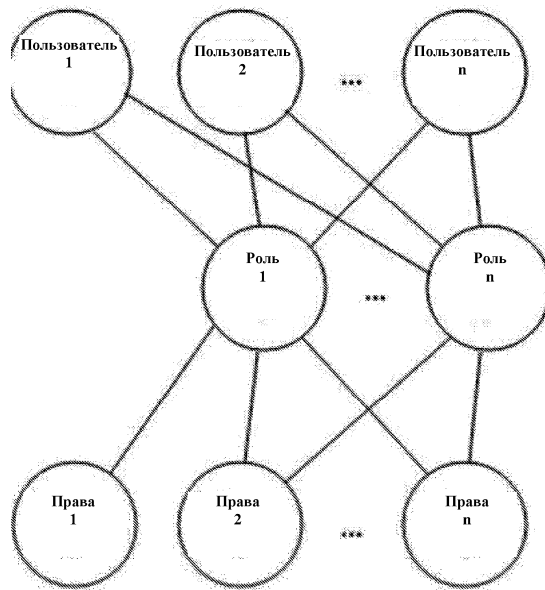
при этом система дополнительно выполнена с возможностью управления переводом пользователя в другое отделение, где указанное управление включает:

- (1) удаление связи пользователя с ролью в прежнем отделении;
- (2) связывание пользователя с ролью в новом отделении.

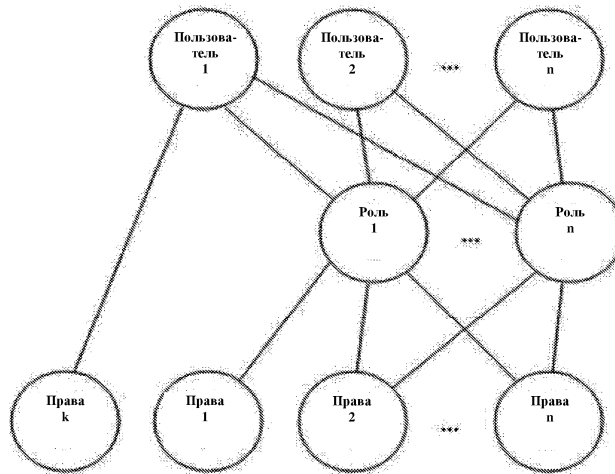
6. Система по п.5, отличающаяся тем, что структура указанных системных ролей следующая: название должности плюс номер должности.



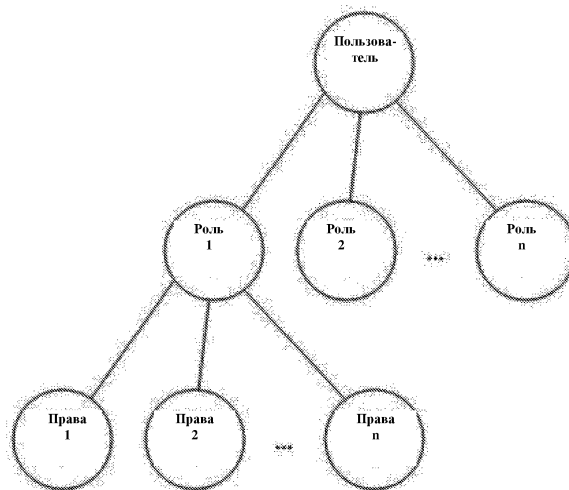
Фиг. 1



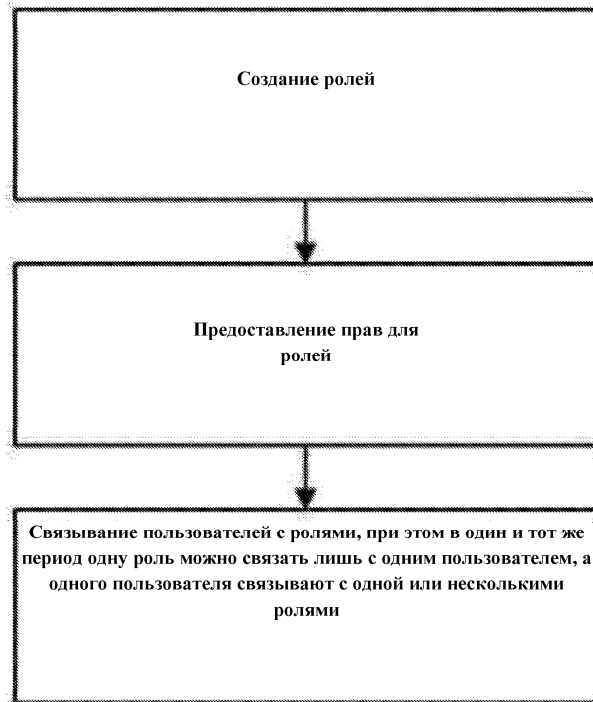
Фиг. 2



Фиг. 3



Фиг. 4



Фиг. 5