

(19)



**Евразийское  
патентное  
ведомство**

(11) **044265**

(13) **B1**

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

(45) Дата публикации и выдачи патента  
**2023.08.09**

(51) Int. Cl. **G06F 21/30** (2013.01)  
**G06Q 10/10** (2012.01)

(21) Номер заявки  
**202090361**

(22) Дата подачи заявки  
**2018.07.23**

---

(54) **СПОСОБ УСТАНОВКИ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЯ В БЛОКЕ ОБМЕНА  
ИНФОРМАЦИЕЙ В СИСТЕМЕ**

---

(31) **201710608633.4**

(56) CN-A-106803138  
CN-A-102468971  
CN-A-107491668  
CN-A-107480512  
US-B1-8402514

(32) **2017.07.24**

(33) **CN**

(43) **2020.05.18**

(86) **PCT/CN2018/096713**

(87) **WO 2019/019981 2019.01.31**

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

(72) Изобретатель:  
**Чень Дачжи (CN)**

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

---

(57) В изобретении раскрыт способ установки полномочий пользователя в блоке обмена информацией в системе, включающий в себя: установку множества информационных разделов для блока обмена информацией; установку ролей участия для каждого информационного раздела, соответственно, причем роль участия включает в себя одну или несколько ролей в системе; и установку полномочий каждой из ролей участия в информационном разделе, при этом каждая роль представляет собой независимый субъект, а не группу/класс, причем одна роль может быть связана только с уникальным пользователем в течение того же периода, а один пользователь связан с одной или более ролями; и создание связи между пользователями и ролями в системе. Согласно изобретению, когда сотрудник изменяет содержание своей работы или переводится с должности, полномочия сотрудника в информационном разделе блока обмена информацией не должны устанавливаться отдельно.

---

**B1**

**044265**

**044265  
B1**

### Область техники

Изобретение относится к системам управляющего программного обеспечения, таким как ERP (Enterprise Resource Planning, Планирование ресурсов предприятия), и, в частности, к способу установки полномочий пользователя в блоке обмена информацией в системе.

#### Предшествующий уровень техники

Управление доступом на основе ролей (RBAC, Role-Based Access Control) является одним из наиболее изученных и развитых в последние годы механизмов управления полномочиями для баз данных. Он считается идеальным вариантом для замены общепринятого мандатного управления доступом (MAC, Mandatory Access Control) и избирательного управления доступом (DAC, Discretionary Access Control). Основная идея управления доступом на основе ролей (RBAC) состоит в том, чтобы разделять разные роли в соответствии с различными функциональными позициями в рамках организации предприятия, инкапсулировать разрешение доступа к ресурсам базы данных в ролях, и разрешать пользователям опосредованный доступ к ресурсам базы данных путем назначения разных ролей пользователям.

В крупномасштабные прикладные системы зачастую встроено большое количество таблиц и представлений, что значительно усложняет управление ресурсами базы данных и авторизацию. Пользователю очень сложно напрямую управлять доступом и полномочиями ресурсов базы данных. Это требует от пользователя глубокого понимания структуры базы данных и знания языка SQL. С изменением структуры прикладной системы или требований к безопасности требуется большое количество сложных и объемных изменений полномочий, что весьма вероятно приводит к возникновению уязвимостей информационной безопасности, вызванных непредвиденными ошибками авторизации. Поэтому разработка простого и эффективного способа управления полномочиями для крупномасштабных прикладных систем стала общим требованием для систем и пользователей систем.

Механизм управления полномочиями на основе ролей позволяет легко и эффективно управлять полномочиями системы, что значительно снижает нагрузку и затраты на управление системными правами, а также делает управление системными правами более совместимым с техническими требованиями к управлению бизнесом прикладной системы.

Однако традиционный способ управления полномочиями пользователей на основе ролей использует механизм связи "роль к пользователю один-ко-многим", где "роль" представляет собой группу/класс. Это означает, что одна роль может одновременно соответствовать нескольким пользователям или может быть связана с ними, и роль аналогична положению/должности/виду работы или другим понятиям. В соответствии с этим механизмом связи авторизация полномочий для пользователя в основном выполняется следующими тремя способами: 1. Как показано на фиг. 1, прямая авторизация полномочий пользователя, имеет недостаток, заключающийся в высокой рабочей нагрузке и частоте, и объемности операций. 2. Как показано на фиг. 2, роль (представляющая собой класс/группу/положение/вид работы) авторизована (одна роль может быть связана с несколькими пользователями), и пользователь получает полномочия посредством своей роли. 3. Как показано на фиг. 3, вышеуказанные два способа сочетаются.

В вышеприведенных описаниях 2 и 3 необходимо проводить авторизацию роли типа класса/группы. Способ авторизации посредством роли типа класса/группы/ должности/вида работы, имеет следующие недостатки:

1. Возникновение сложностей с выполнением операций в случае изменения полномочий пользователя. В процессе реального использования системы полномочия пользователя подвергаются частым изменениям. Например, в процессе обработки изменений полномочий сотрудника, при изменении полномочий сотрудника, связанных с ролью, является нецелесообразным изменение полномочий всей роли из-за изменения полномочий отдельного сотрудника, поскольку эта роль также связана с другими сотрудниками, чьи полномочия остались неизменными. В результате, либо создается новая роль, соответствующая сотруднику, чьи полномочия были изменены, либо полномочия непосредственно предоставляются сотруднику (не связаны с ролью) на основе требований к полномочиям. Два вышеупомянутых способа обработки не только трудоемкие, но и легко приводят к ошибкам при авторизации роли в случае, если роль обладает большими полномочиями. Пользователю приходится выполнять объемную работу, в результате чего происходят ошибки, приводящие к потерям для пользователя системы.

2. Сложно удержать в памяти конкретные полномочия, содержащиеся в роли, в течение длительного времени. Если у роли имеется много функциональных полномочий, с течением времени сложно вспомнить конкретные полномочия роли, а еще труднее вспомнить различия в полномочиях между ролями с аналогичными полномочиями. Если нужно связать нового пользователя, невозможно точно определить, как выбрать связь.

3. Поскольку полномочия пользователей изменяются, будет создано больше ролей (если новые роли не будут созданы, непосредственная авторизация для пользователя существенно увеличится), и будет сложнее находить конкретные отличия между полномочиями ролей.

4. При переводе пользователя на другую должность и необходимости назначать другим пользователям большое количество полномочий переведенного пользователя, необходимо разделять полномочия переведенного пользователя и создавать роли в связи с другими пользователями, соответственно, необходимые при обработке. Такие операции не только сложны и трудоемки, но и предрасположены к

ошибкам.

В блоке обмена информацией (таком как база знаний) существующего программного обеспечения управления установлено множество разделов. Каждый раздел содержит информацию о другой области или другом отделе. Если полномочия пользователя в информационном разделе блока обмена информацией в системе не могут быть эффективно управляемыми со временем, информационный раздел блока обмена информацией в системе легко перестает работать нормально и эффективно. Установка полномочий выполняется следующими существующими способами. Первый способ заключается в том, чтобы напрямую устанавливать полномочия для пользователя. В случае использования способа для прямой установки полномочий для пользователя, когда содержание работы, должность или другая информация пользователя изменилась, произойдет утечка информации, если полномочия пользователя в информационном разделе блока обмена информацией не будут своевременно изменены. Например, раздел данных исследований и разработок, раздел данных о продажах, раздел финансовых данных и т. п. устанавливаются в блоке базы знаний. Если сотрудник А в финансовом отделе может загружать данные из раздела финансовых данных, а полномочия сотрудника А в блоке базы знаний не изменяются во времени после перевода сотрудника А из финансового отдела в отдел продаж, сотрудник А по-прежнему сможет загружать данные из раздела финансовых данных после перевода в отдел продаж, а также может выполнять операции с данными, которые впоследствии добавляются в раздел финансовых данных, что приводит к утечке финансовых данных. Кроме того, сотруднику А также запрещено загружать данные из раздела данных о продажах, что влияет на его нормальную работу.

Однако при практическом применении в одной системе может существовать много пользователей, и содержание работы и должности пользователей часто изменяются. Таким образом, сложно гарантировать, что все полномочия этих пользователей в информационном разделе блока обмена информацией изменяются во времени, что приводит к скрытым рискам утечки информации. Кроме того, всякий раз, когда изменяется содержание работы, должность и т. п. пользователя, полномочия пользователя в информационном разделе блока обмена информацией должны устанавливаться снова, что приводит к огромной рабочей нагрузке для установки полномочий.

Второй способ состоит в том, чтобы устанавливать полномочия на основе типа работы. Такой способ установки полномочий в зависимости от типа работы также может вызвать утечку информации. Например, когда блок обмена информацией содержит раздел продаж авиационного подразделения и раздел продаж мебельного подразделения. Если полномочия установлены в зависимости от типа работ по продажам (вышеупомянутые два раздела устанавливаются как доступные для сотрудников, относящихся к типу работ по продажам), продавец в отделе мебельной подразделения может просматривать информацию раздела продаж авиационного подразделения, что приводит к утечке информации.

Третий способ состоит в том, чтобы устанавливать полномочия на основе отдела. Такой способ установки полномочий на основе отдела также может вызвать утечку информации. Например, в каждом отделе может существовать несколько видов работ. Например, отдел продаж включает следующие виды работ, такие как инженер по продажам и служащий, который помогает инженеру по продажам в подготовке данных; а производственный отдел включает в себя следующие виды работ, такие как сборщики и испытатели. Если разрешения установлены на основе отдела, сотрудники, относящиеся к различным видам работ, могут иметь одинаковые полномочия в блоке обмена информацией, что упрощает утечку информации. В другом примере, когда отдел включает следующие виды работы, такие как сотрудники и руководитель, невозможно разрешить руководителю участвовать только в одном разделе в блоке обмена информацией.

Кроме того, некоторые существующие блоки обмена информацией дополнительно не делятся на разделы. Следовательно, любое лицо, которому разрешено входить в блок обмена информацией, может выполнять операции с информацией в блоке обмена информацией, такие как просмотр информации, что повышает вероятность ее утечки. Например, продавец может просматривать информацию об исследованиях и разработках и т. п., которая не связана с содержанием его работы, в блоке обмена информацией, что приводит к утечке информации об исследованиях и разработках.

Установка управленческого персонала: В случае если субъект назначен непосредственно в качестве управленческого персонала, предполагая, что Чжан Сань в настоящее время относится к типу работы по управлению продажами и отвечает за управление отделом продаж, после перевода Чжан Саня на производственную должность, другой сотрудник должен занять место Чжан Саня для управления отделом продаж. Если полномочия не установлены своевременно, Чжан Сань может не только просматривать последующие данные о продажах или рыночную информацию компании, но также загружать/изменять/удалять данные, что приведет к утечке информации и другим потерям для компании. С другой стороны, если модератору этого отдела необходимо проверить загруженные данные, поскольку Чжан Сань был переведен с этой должности, и прекратил свою ответственность за эту должность, то Чжан Сань не должен проверять подлежащие проверке данные, и, следовательно, данные, представленные на проверку, не могут быть проверены вовремя. Даже если новый модератор возьмет на себя работу этого отдела в будущем, новый модератор лишен возможности проверять данные, ранее загруженные для проверки, поскольку задача проверки остается за Чжан Санем.

### Раскрытие сущности изобретения

Технические задачи.

Настоящее изобретение направлено на преодоление недостатков предшествующего уровня техники и обеспечение способ установки полномочий пользователя в блоке обмена информацией в системе. При изменении содержания работы или должности сотрудника нет необходимости отдельно устанавливать полномочия сотрудника в информационном разделе блока обмена информацией.

Решение задач. Технические решения.

Цель настоящего изобретения реализуется с помощью следующих технических решений.

Способ установки полномочий пользователя в блоке обмена информацией в системе включает в себя:

- (1) установку одного или более информационных разделов для блока обмена информацией;
- (2) установку ролей участников соответственно для каждого информационного раздела, причем упомянутая роль участника включает в себя одну или более ролей в системе; и установку полномочий каждой из ролей участия в информационном разделе, при этом каждая роль представляет собой независимый субъект, а не группу/класс, одна роль может быть связана только с уникальным пользователем в течение одного периода, а один пользователь связан с одной или более ролей; и
- (3) создание связей между пользователями и ролями в системе.

Этап (1) и этап (2) выполняют последовательно, и этап (3) может выполняться перед этапом (1), после этапа (1), перед этапом (2) или после этапа (2).

Предпочтительно, полномочия указанной роли в информационном разделе включают в себя полномочия на участие и/или полномочия на управление.

Предпочтительно указанные полномочия на участие включают в себя один или несколько типов проверяемых данных (содержание/информация), загружаемых данных (содержание/информация), выгружаемых данных (содержание/ информация) и оцениваемых данных (содержание/информация).

Предпочтительно упомянутые полномочия на управление включают в себя один или несколько типов оценки просматриваемых данных (содержания/ информации), загружаемых данных (содержания/информации), изменяемых данных (содержания/информации), выгружаемых данных (содержания/информации), оцениваемых данных (содержания/информации), архивируемых данных (содержания/ информации), разархивируемых данных (содержания/информации), проверяемых данных (содержания/информации) и удаляемых данных (содержания/информации).

Предпочтительно, указанные полномочия на управление включают в себя по меньшей мере один уровень.

Предпочтительно, если отдел выбран для роли, при создании роли или после ее создания, роль принадлежит отделу, роль авторизована в соответствии с содержанием работы роли, название роли уникально в отделе, а номер роли уникален в системе.

Предпочтительно, когда указанного пользователя переводят с должности, связь пользователя с ролью, соответствующей исходной должности, отменяется, а пользователя связывают с ролью, соответствующей новой должности.

Предпочтительно, один сотрудник совпадает с одним пользователем, один пользователь совпадает с одним сотрудником, и сотрудник определяет (получает) свои полномочия в блоке обмена информацией на основе роли, связанной с пользователем, совпадающим с сотрудником; после ухода сотрудника с должности пользователь, совпадающий с сотрудником, замораживается; а когда сотрудника снова принимают на работу, пользователь, ранее совпадающий с этим сотрудником, размораживается и служит в качестве текущего пользователя, совпадающего с этим сотрудником. В течение периода замораживания пользователь не может служить в качестве пользователя, совпадающего с сотрудником.

Предпочтительно, когда сотрудник, совпадающий с пользователем, связанным с ролью, которой назначены полномочия на управление, проверяет данные, скорость передачи данных в течение заданного времени получают путем деления числа лиц, представивших результаты проверки и сдавших проверку, на общее количество лиц, представивших результаты проверки. Описанный выше способ проверки также может быть способом проверки и утверждения.

Способ установки полномочий пользователя в блоке обмена информацией в системе, включает в себя: настройку одного или более информационных разделов для блока обмена информацией; установку полномочий роли в каждом информационном разделе в системе, при этом каждая роль представляет собой независимый субъект, а не группу/класс, причем одна роль может быть связана только с уникальным пользователем в течение одного периода, а один пользователь связан с одной или более ролей; и создание связей между пользователями и ролями в системе.

Положительные эффекты изобретения. Положительные эффекты.

Настоящее изобретение имеет следующие положительные эффекты.

- (1) В настоящем изобретении полномочия пользователя в информационном разделе блока обмена информацией устанавливаются на основе роли. Когда пользователя переводят с должности, связь пользователя с ролью, соответствующей исходной должности, отменяется, а пользователя связывают с ролью, соответствующей новой должности. Полномочия пользователя в информационном разделе блока

обмена информацией изменяются при изменении рабочих полномочий пользователя, и полномочия в информационном разделе блока обмена информацией не требуют отдельного изменения для пользователя. Это не только гарантирует, что полномочия пользователя в информационном разделе блока обмена информацией обновляются вовремя, но также значительно снижает нагрузку для установки полномочий пользователя в информационном разделе блока обмена информацией.

Например, содержание работы сотрудника А включает разработку продукта и продажу продукта. Содержание работы для роли 1 представляет собой разработку продукта, и роль 1 имеет полномочия на просмотр данных, загрузку данных и выгрузку данных в разделе данных исследований и разработок. Содержание работы для роли 2 представляет собой продажу продукта, и роль 2 имеет полномочия на просмотр данных, загрузку данных и выгрузку данных в разделе данных о продажах. Содержание работы для роли 3 представляет собой производство продукта, и роль 3 имеет полномочия на просмотр данных, загрузку данных и выгрузку данных в разделе данных производства продукта. При связывании роли 1 и роли 2 только с пользователем, совпадающим с сотрудником А, санкционирован не только доступ к содержанию работы сотрудника А, но сотруднику А также разрешено просматривать данные, загружать данные и выгружать данные в разделе данных исследований и разработок и разделе данных о продажах. Чтобы настроить содержание работы сотрудника А только для разработки продукта, необходимо только отменить связь пользователя 2 с пользователем, совпадающим с сотрудником А, а вместе с тем, настраивается содержание работы сотрудника А и его полномочия в информационном разделе блока обмена информацией. Чтобы настроить содержание работы сотрудника А для производства продукта, необходимо только отменить связь роли 1 и роли 2 с пользователем, совпадающим с сотрудником А, и связать пользователя, совпадающего с сотрудником А, с ролью 3, а вместе с тем настраивается содержание работы сотрудника А и его полномочия в информационном разделе блока обмена информацией.

(2) Блок обмена информацией в настоящем изобретении включает в себя множество информационных разделов. Полномочия для роли в каждом информационном разделе устанавливаются соответственно, чтобы ограничить роли участия в каждом информационном разделе и дополнительно ограничить полномочия на участие пользователя в каждом информационном разделе, и предотвратить утечку информации в каждом информационном разделе к не имеющим отношения лицам.

(3) Традиционный механизм управления полномочиями определяет роль как характер группы, вила работы, класса или т. п. Роль находится в связи "один ко многим" с пользователем. В процессе реального использования системы полномочия пользователя подвергаются частым изменениям. Например, в процессе обработки изменения полномочий сотрудника, при изменении полномочий сотрудника, связанных с ролью, является нецелесообразным изменение полномочий всей роли из-за изменения полномочий отдельного сотрудника, поскольку эта роль также связана с другими сотрудниками, чьи полномочия остались неизменными. В результате, либо создается новая роль, соответствующая сотруднику, чьи полномочия были изменены, либо полномочия непосредственно предоставляются сотруднику (не связаны с ролью) на основе требований к полномочиям. Два вышеупомянутых способа обработки не только трудоемкие, но и легко приводят к ошибкам при авторизации роли в случае, если роль обладает большими полномочиями. Пользователю приходится выполнять объемную работу, в результате чего происходят ошибки, приводящие к потерям для пользователя системы.

Однако в соответствии со способом, предложенным в настоящей заявке, поскольку роль представляет собой независимый субъект, цель может быть достигнута путем изменения полномочий роли. Хотя способ согласно настоящей заявке, по-видимому, увеличивает рабочую нагрузку во время инициализации системы, посредством копирования или т. п., роль может быть создана или авторизована более эффективно, чем обычные роли, имеющие характер группы. Поскольку нет необходимости учитывать общность ролей, имеющих характер группы, при удовлетворении связанных пользователей, решения, предложенные в настоящей заявке, делают настройку полномочий ясной и однозначной. В особенности, после использования системы в течение определенного периода времени (после динамического изменения полномочий пользователя/роли), решения согласно настоящей заявке могут значительно повысить эффективность управления полномочиями для пользователя системы при использовании системы, сделать динамическую авторизацию проще, удобнее, яснее и понятнее, а также повысить эффективность и надежность установки полномочий.

(4) Обычный способ авторизации роли с характером группы предрасположен к ошибкам. Способ, обеспечиваемый настоящей заявкой, значительно снижает вероятность ошибок авторизации, поскольку способ, описанный в настоящей заявке, должен рассматривать роль только как независимый субъект, без учета общности нескольких пользователей, связанных с ролью, имеющей характер группы, по общепринятому способу. Даже если возникают ошибки авторизации, затрагивается только пользователь, связанный с ролью. Хотя в случае общепринятой роли, имеющей характер группы, затрагиваются все пользователи, связанные с этой ролью. Даже если возникают ошибки авторизации, способ исправления согласно настоящей заявке прост и занимает немного времени, в то время как в случае обычной роли, имеющей характер группы, при исправлении ошибок должна учитываться общность полномочий всех пользователей, связанных с потребностями роли. При наличии большого количества функциональных точек модификация является громоздкой, сложной и предрасположенной к ошибкам, и во многих случаях проблема

не может быть решена без создания новой роли.

(5) В традиционном способе авторизации роли на основе группы, если роль имеет много функциональных полномочий, с течением времени сложно вспомнить конкретные полномочия роли, а еще труднее вспомнить различия в полномочиях между ролями с аналогичными полномочиями. Если нужно связать нового пользователя, невозможно точно определить, как выбрать связь. В способе согласно настоящей заявке сама роль имеет характер номера положения/номера станции, так что выбор может быть сделан легко.

(6) При переводе пользователя на другую должность и необходимости назначить другим пользователям большого количества полномочий переведенного пользователя, при обработке необходимо разделить полномочия переводимого пользователя и создать роли для связи с другими пользователями, соответственно. Такие операции сложные, трудоемкие, а также предрасположены к ошибкам.

Способ согласно настоящей заявке состоит в следующем: переведенный пользователь связан с несколькими ролями. Когда пользователя переводят с должности, связь пользователя с ролями в исходном отделе сначала отменяется (отмененные роли могут быть связаны с другими пользователями), а затем пользователь связывается с ролью в новом отделе. Операция проста и не предрасположена к ошибкам.

(7) При создании роли или после него необходимо выбрать отдел, и тогда отдел, которому принадлежит роль, не может быть заменен. Причины, по которым отдел, которому принадлежит роль, не может быть заменен, заключаются в следующем. Причина 1: Поскольку роль согласно данной заявке, по сути, эквивалентна номеру рабочей станции или номеру должности, различные номера станций или номера должностей имеют разное содержание работы или полномочия. Например, роль продавца 1 в отделе продаж и роль разработчика 1 в техническом отделе имеют два совершенно разных номера станций или номера должности, и имеют разные полномочия. Причина 2: Если отдел (отдел продаж), которому принадлежит роль продавца 1, заменяется техническим отделом без изменения полномочий роли продавца 1, то в техническом отделе существует роль, которой принадлежат полномочия отдела продаж. Это приводит к беспорядку в управлении и уязвимостям безопасности.

#### **Краткое описание графических материалов**

Описание графических материалов.

На фиг. 1 представлено схематическое изображение непосредственной авторизации пользователя системой в предшествующем уровне техники.

На фиг. 2 представлено схематическое изображение авторизации в системе роли группового или классового характера в предшествующем уровне техники.

На фиг. 3 представлено схематическое изображение непосредственной авторизации в системе и пользователя, и роли группового или классового характера в предшествующем уровне техники.

На фиг. 4 приведена последовательность операций согласно настоящему изобретению.

На фиг. 5 приведена принципиальная схема, авторизации пользователя в системе на основе роли, имеющей характер независимого субъекта, согласно настоящему изобретению.

На фиг. 6 приведена последовательность операций другого варианта осуществления согласно настоящему изобретению.

#### **Осуществление изобретения**

Описание вариантов реализации изобретения.

Технические решения данного изобретения будут описаны ниже более подробно со ссылкой на прилагаемые фигуры, но объем защиты настоящего изобретения не ограничивается нижеследующим описанием.

[Вариант осуществления 1]

Как показано на фиг. 4, способ установки полномочий пользователя в блоке обмена информацией в системе включает в себя: установку множества информационных разделов (или информационных категорий) для блока обмена информацией, например, установку электрического раздела, механического раздела, раздела химической промышленности, финансового раздела, раздела управления и т. п. в базе знаний; и установку ролей участия для каждого информационного раздела, соответственно, причем роль участия включает в себя одну или более ролей в системе; и установку полномочий каждой из ролей участия в информационном разделе, при этом каждая роль представляет собой независимый субъект, а не группу/класс, одна роль может быть связана только с уникальным пользователем в течение одного периода, а один пользователь связан с одной или более ролей; то есть для каждого информационного раздела выбирают одну или более ролей из ролей в системе в качестве ролей участия информационного раздела и устанавливают полномочия для каждой из ролей участия в информационном разделе.

Как показано на фиг. 5, роль представляет собой независимый субъект, а не группу/класс. Одна роль может быть связана только с уникальным пользователем в течение одного периода, а один пользователь связан с одной или более ролей. При создании роли или после него для роли выбирают отдел, так что роль принадлежит отделу. Авторизация роли выполняется в соответствии с ее рабочим содержанием, имя роли уникально в отделе, а номер роли уникален в системе.

Определение роли: роль по своей сути не является группой/классом/категорией/должностью/положением/типом работы или тому подобным, но носит не коллективный характер. Роль уникальна и

представляет собой независимый субъект. Применяемая на предприятии или в учреждении, роль эквивалентна номеру должности (при этом номер должности не является должностью, и одна должность может одновременно иметь несколько сотрудников, но один номер должности может соответствовать только одному сотруднику в течение одного периода).

Например, в системе компании могут быть созданы следующие роли: генеральный менеджер, заместитель генерального менеджера 1, заместитель генерального менеджера 2, менеджер Пекинского отдела продаж I, менеджер Пекинского отдела продаж II, менеджер Пекинского отдела продаж III, Шанхайский инженер по продажам 1, Шанхайский инженер по продажам 2, Шанхайский инженер по продажам 3, Шанхайский инженер по продажам 4, Шанхайский инженер по продажам 5 и так далее. Связь между пользователями и ролями выглядит следующим образом: если Чжан Сань, сотрудник компании, выступает в качестве заместителя генерального менеджера 2 и в то же время выступает в качестве менеджера Пекинского отдела продаж I, то Чжан Сань должен быть связан с ролью заместителя генерального менеджера 2 и ролью менеджера Пекинского отдела продаж I, то есть Чжан Сань обладает полномочиями двух ролей.

Концепция традиционных ролей, по сути, представляет собой группу/ класс/ должность/ положение/ вид работы, и одна роль может соответствовать нескольким пользователям. Однако в настоящей заявке понятие "роль" эквивалентно номеру должности/номеру рабочего места, а также аналогично роли в кино и телевизионной драме: одна роль (в детстве, юности, среднем возрасте...) может одновременно исполняться только одним актером или актрисой, но один актер или актриса могут играть несколько ролей.

Когда пользователя переводят с должности, связь пользователя с ролью в исходном отделе отменяется, а пользователя связывают с ролью в новом отделе. После создания роли, пользователь может быть связан с ролью в процессе создания пользователя, или может быть связан с ролью в любое время после создания пользователя. После того как пользователь связан с ролью, пользователь может быть освобожден от связи с ролью в любое время, и связь между пользователем и другой ролью может быть создана в любое время.

Полномочия роли в информационном разделе включают в себя полномочия на участие и/или полномочия на управление, так что пользователи в информационном разделе могут быть разделены на участников и менеджеров в информационном разделе блока обмена информацией. Разные полномочия назначаются участникам и менеджерам соответственно (полномочия на участие назначаются участнику, а полномочия на управление назначаются менеджеру), что помогает поддерживать нормальную работу информационного раздела блока обмена информацией.

Указанные полномочия на участие включают в себя один или более типов просмотра данных, загрузки данных, выгрузки данных, оценки данных и т. п. Кроме того, полномочия на участие включают в себя по меньшей мере полномочия на просмотр данных.

Указанные полномочия на управление включают в себя один или более типов просмотра данных, загрузки, разгрузки данных, изменения данных, выгрузки данных, оценки данных, архивирования данных, разархивирования данных, проверки данных, удаления оценки данных и т. п.

Один сотрудник совпадает с одним пользователем, один пользователь совпадает с одним сотрудником, и сотрудник определяет (получает) полномочия на основе роли, связанной с пользователем, совпадающим с сотрудником.

Указанные полномочия на управление включают в себя по меньшей мере один уровень. Например, полномочия на управление включают два уровня, один из которых - обычные полномочия на управление, а другой - специальные полномочия на управление. Сотрудник, соответствующий обычным полномочиям на управление, управляет соответствующим информационным разделом (например, проверяет данные), а сотрудник, соответствующий специальным полномочиям на управление, контролирует качество управления, выполняемого сотрудником, соответствующим обычным полномочиям на управление в соответствующем информационном разделе.

Когда сотрудник, соответствующий роли, которой назначены полномочия на управление, проверяет данные (например, загруженные данные), скорость передачи данных в течение заданного времени (заданное время определяется пользователем) получают путем деления числа лиц, представивших результаты проверки и сдавших проверку, на общее количество лиц, представивших результаты проверки. Когда скорость передачи данных больше заданного значения или равна ему, проверка считается пройденной. В противном случае проверка не удалась. Это значительно сокращает период проверки данных.

Кроме того, содержание обычных полномочий на управление включает в себя один или более типов просмотра данных, проверки данных, удаления данных и удаления оценки данных, а также один или более типов загрузки данных, выгрузки данных и оценки данных. Содержимое специальных полномочий на управление включает в себя один или более типов просмотра данных, архивирования данных, разархивирования данных, загрузки данных, выгрузки данных, оценки данных, проверки данных, удаления данных и удаления оценки данных. Архивирование данных предназначено для сокрытия данных (включая соответствующую информацию об оценке данных и т. п.). После того как данные заархивированы, только сотрудники, соответствующие специальным полномочиям на управление, могут выполнять такие

операции, как просмотр данных, а сотрудники, соответствующие обычным полномочиям на управление и участие, не могут просматривать заархивированные данные. Разархивирование данных служит для возобновления отображения архивных данных, и разархивированные данные восстанавливаются до последнего состояния перед архивированием.

Способ дополнительно включает в себя этап создания связей между пользователями и ролями в системе.

[Вариант осуществления 2]

Как показано на фиг. 6, способ установки полномочий пользователя в блоке обмена информацией в системе включает в себя: установку множества информационных разделов (или информационных категорий) для блока обмена информацией, например, установку электрического раздела, механического раздела, раздела химической промышленности, финансового раздела, раздела управления и т. п. в базе знаний; и установку полномочий роли в системе в каждом информационном разделе, причем каждая роль представляет собой независимый субъект, а не группу/класс, при этом одна роль может быть связана только с уникальным пользователем в течение одного периода, и один пользователь связан с одной или более ролей.

Роль представляет собой независимый субъект, а не группу/класс. Одна роль может быть связана только с уникальным пользователем в течение одного периода, а один пользователь связан с одной или более ролей. При создании роли или после него для роли выбирают отдел, так что роль принадлежит отделу. Авторизация роли выполняется в соответствии с содержанием ее работы, имя роли уникально в отделе, а номер роли уникален в системе.

Когда пользователя переводят с должности, связь пользователя с ролью в исходном отделе отменяется, а пользователя связывают с ролью в новом отделе. После создания роли пользователь может быть связан с ролью в процессе создания пользователя, или может быть связан с ролью в любое время после создания пользователя. После того как пользователь связан с ролью, пользователь может быть освобожден от связи с ролью в любое время, и связь между пользователем и другой ролью может быть создана в любое время.

Полномочия роли в информационном разделе включают в себя полномочия на участие и/или полномочия на управление, так что пользователи в информационном разделе могут быть разделены на участников и менеджеров в информационном разделе блока обмена информацией. Разные/соответствующие полномочия назначаются участникам и менеджерам соответственно (полномочия на участие назначаются участнику, а полномочия на управление назначаются менеджеру), что помогает поддерживать нормальную работу информационного раздела блока обмена информацией.

Указанные полномочия на участие включают в себя один или более типов просмотра данных, загрузки данных, выгрузки данных и оценки данных. Кроме того, полномочия на участие включают в себя по меньшей мере полномочия на просмотр данных.

Указанные полномочия на управление включают в себя один или более типов просмотра данных, загрузки, загрузки данных, изменения данных, выгрузки данных, оценки данных, архивирования данных, разархивирования данных, проверки данных и удаления оценки данных.

Один сотрудник совпадает с одним пользователем, один пользователь совпадает с одним сотрудником, и сотрудник определяет (получает) полномочия на основе роли, связанной с пользователем, совпадающим с сотрудником.

Указанные полномочия на управление включают в себя по меньшей мере один уровень. Например, полномочия на управление включают два уровня, один из которых - обычные полномочия на управление, а другой - специальные полномочия на управление. Сотрудник, соответствующий обычным полномочиям на управление, управляет соответствующим информационным разделом, а сотрудник, соответствующий специальным полномочиям на управление, контролирует качество управления, выполняемого сотрудником, соответствующим обычным полномочиям на управление в соответствующем информационном разделе.

Содержимое обычных полномочий на управление включает в себя один или более типов просмотра данных, загрузки данных, выгрузки данных, оценки данных, проверки данных, удаления данных и удаления оценки данных. Содержимое специальных полномочий на управление включает в себя один или более типов просмотра данных, загрузки данных, выгрузки данных, оценки данных, архивирования данных, разархивирования данных, проверки данных, удаления данных и удаления оценки данных. Заархивированные данные служат для сокрытия данных. После того как данные заархивированы, только сотрудники, соответствующие специальным полномочиям на управление, могут выполнять такие операции, как просмотр данных, а сотрудники, соответствующие обычным полномочиям на управление и участие, не могут просматривать заархивированные данные. Разархивирование данных служат для возобновления отображения архивных данных, и разархивированные данные восстанавливаются до последнего состояния перед архивированием.

Способ дополнительно включает в себя этап создания связей между пользователями и ролями в системе.

Вышеизложенное представляет собой только предпочтительные варианты осуществления данного

изобретения. Следует понимать, что данное изобретение не ограничено вариантами, раскрытыми в настоящем документе, и не должно толковаться как исключающее другие варианты осуществления, но может использоваться в различных других комбинациях, модификациях и средах. А также может быть модифицировано посредством вышеизложенных принципов либо технологий и знаний в смежных сферах. Предполагается, что все изменения и модификации, сделанные специалистами в данной области техники без отклонения от сущности и объема настоящего изобретения, находятся в пределах объема защиты прилагаемой формулы изобретения.

#### ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ установки полномочий пользователя в блоке обмена информацией в системе, включающий в себя:

установку одного или более информационных разделов для блока обмена информацией;

установку ролей участников соответственно для каждого информационного раздела, причем упомянутая роль участника включает в себя одну или более ролей в системе; и

установку полномочий каждой из ролей участия в информационном разделе, при этом каждая роль представляет собой независимый субъект, а не группу/класс, одна роль может быть связана только с уникальным пользователем в течение одного периода, а один пользователь связан с одной или более ролями; и

создание связей между пользователями и ролями в системе;

при этом, когда указанного пользователя переводят с должности, связь пользователя с ролью, соответствующей исходной должности, аннулируется, и пользователь связывается с ролью, соответствующей новой должности.

2. Способ установки полномочий пользователя в блоке обмена информацией в системе по п.1, в котором полномочия указанной роли в информационном разделе включают полномочия на участие и/или полномочия на управление.

3. Способ установки полномочий пользователя в блоке обмена информацией в системе по п.2, в котором указанные полномочия на участие включают в себя один или более типов просмотра данных, загрузки данных, выгрузки данных и оценки данных.

4. Способ установки полномочий пользователя в блоке обмена информацией в системе по п.2, в котором указанные полномочия на участие включают в себя один или более типов просмотра данных, загрузки данных, изменения данных, выгрузки данных, оценки данных, архивирования данных, разархивирования данных, проверки данных и удаления оценки данных.

5. Способ установки полномочий пользователя в блоке обмена информацией в системе по п.2, в котором указанные полномочия на управление содержат по меньшей мере один уровень.

6. Способ установки полномочий пользователя в блоке обмена информацией в системе по п.1, в котором, если для роли выбран отдел при создании роли или после него, роль принадлежит отделу, роль авторизуется в соответствии с содержанием работы роли, имя роли уникально в отделе, а номер роли уникален в системе.

7. Способ установки полномочий пользователя в блоке обмена информацией в системе по п.1, в котором один сотрудник совпадает с одним пользователем, один пользователь совпадает с одним сотрудником, при этом сотрудник определяет полномочия на основе роли, связанной с пользователем, совпадающим с сотрудником.

8. Способ установки полномочий пользователя в блоке обмена информацией в системе по п.4, в котором, когда сотрудник, совпадающий с пользователем, связанным с ролью, которой назначены полномочия на управление, проверяет данные, скорость передачи данных в течение заданного времени получают путем деления числа лиц, представивших результаты проверки и сдавших проверку, на общее количество лиц, представивших результаты проверки.

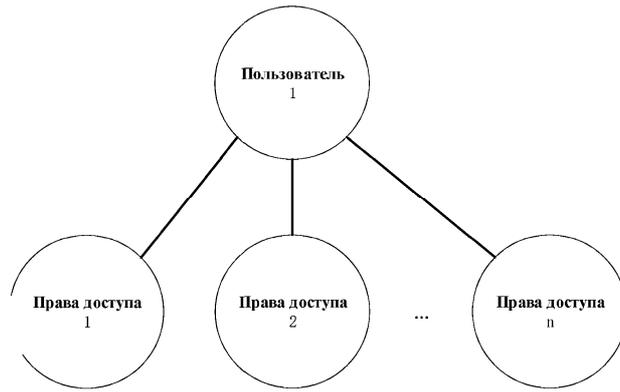
9. Способ установки полномочий пользователя в блоке обмена информацией в системе, включающий в себя:

установку одного или более информационных разделов для блока обмена информацией;

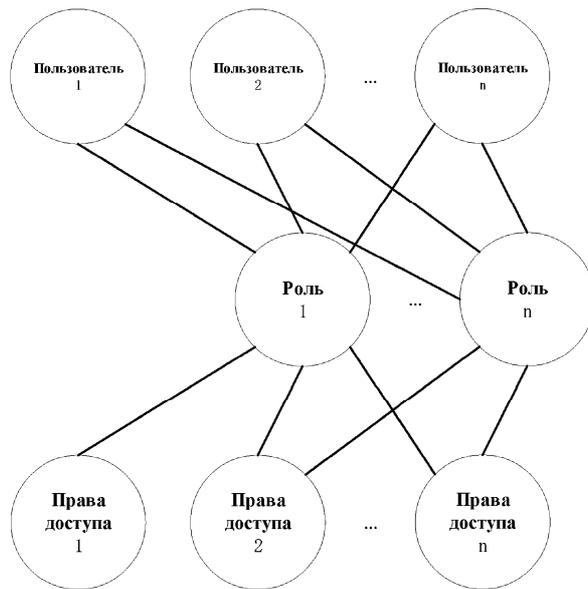
установку полномочий роли в системе в каждом информационном разделе, причем каждая роль представляет собой независимый субъект, а не группу/класс, при этом одна роль может быть связана только с уникальным пользователем в течение одного периода, и один пользователь связан с одной или более ролями, и

создание связей между пользователями и ролями в системе;

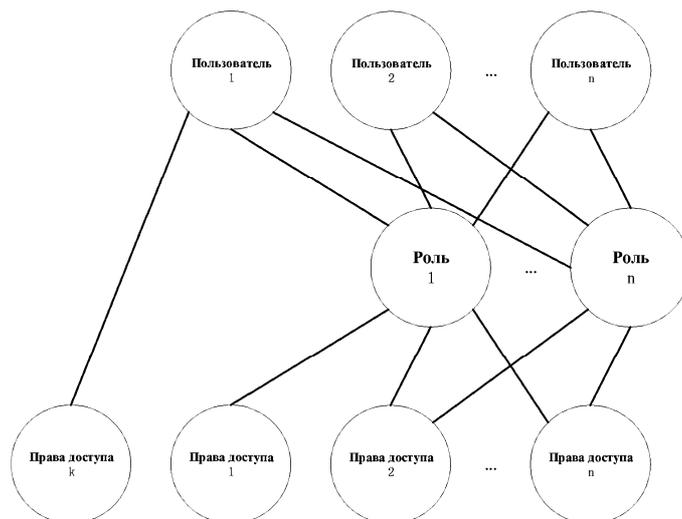
при этом, когда указанного пользователя переводят с должности, связь пользователя с ролью, соответствующей исходной должности, аннулируется, и пользователь связывается с ролью, соответствующей новой должности.



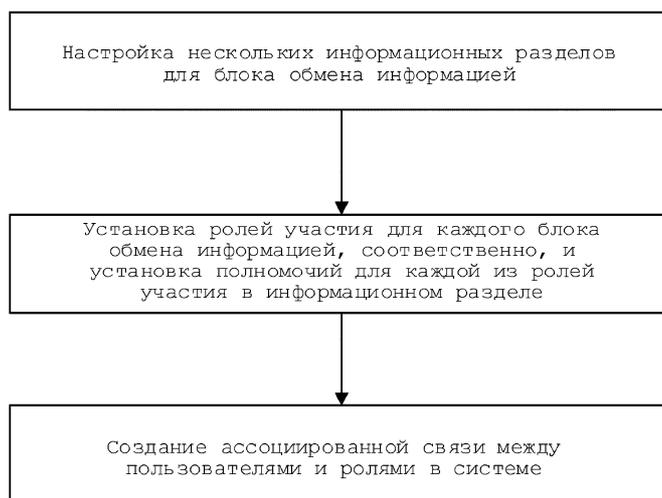
Фиг. 1



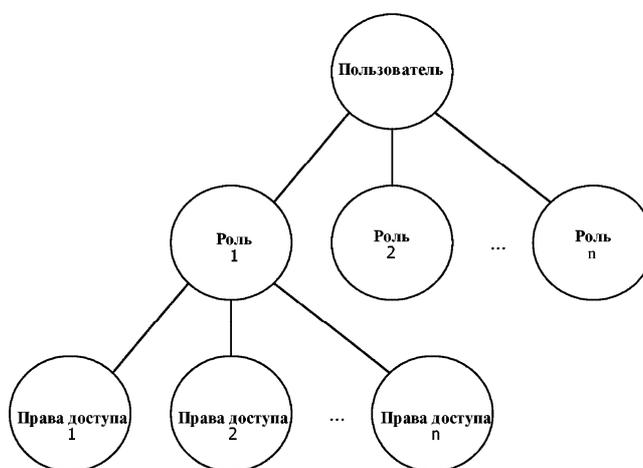
Фиг. 2



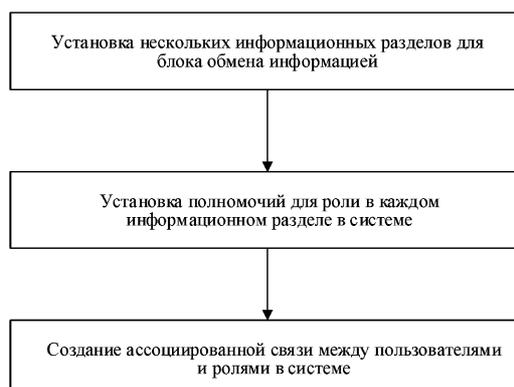
Фиг. 3



Фиг. 4



Фиг. 5



Фиг. 6

