3. Служба пользователей и групп

3.1 Информация о службе

Имя службы	Служба пользователей и групп
Версия службы	1
Идентификатор службы (см. M14.4.42)	cd532472-85b0-4c1c-82b4-5c8370b7d0e6

3.2 Основные понятия

3.2.1 Подход к управлению группами и пользователями в MoReq2010

Грамотное управление группами и пользователями очень важно для успешного функционирования системы управления записями. Это необходимо для всех корпоративных информационных систем. Существует много инструментов для управления группами и пользователями; очень часто такая функциональность включена в операционные системы. Имеются распространенные стандарты управления группами и пользователями, а также связанными с ними службами каталогов, в частности X.500, а для идентификации пользователя — OpenID.

Именно поэтому в MoReq2010 не описываются конкретные протоколы, используемые для авторизации пользователей, а также для управления пользователями и группами. Служба групп и пользователей в MoReq2010 представляет собой набор требований, допускающих как использование внешней службы каталогов, так и службы каталогов, интегрированной в систему управления записями. MoReq2010 дает разъяснения по поводу значения основных понятий, но не содержит никаких предписаний относительно того, каким именно образом должно осуществляться управление пользователями и группами.

3.2.2 Требования к управлению записями

Традиционные службы каталогов не содержат функций, необходимых в системах управления записями. Данные, хранимые в службах каталогов, зачастую отличаются неустойчивостью. Возможность отслеживать действия предыдущих пользователей ограничена или отсутствует вообще. Системные идентификаторы для пользователей и групп могут не иметь универсального характера, а также допускают возможность изменения — например, в случае дублирования или изменения службы каталогов. Важно отметить также, что в проприетарных службах каталогов данные могут сохраняться в особых форматах, которые не

могут быть прочитаны при перемещении записей в другую систему.

В силу этих факторов бывает очень трудно определить, какие пользователи осуществляли конкретные действия и к каким группам они принадлежат.

MoReq2010 требует, чтобы в системе управления записями хранилась как основная, так и дополнительная информация о пользователях и группах, включая информацию о прошлых операциях. Информация о прошлых операциях включает сведения о создании объектов для представления пользователей и групп внутри системы; об использовании универсальных системных идентификаторов; об изменениях метаданных объектов. При удалении пользователей или групп создаются остаточные (резидуальные)объекты, но полного удаления из системы не происходит.

Если система управления записями использует внешнюю службу каталогов для управления группами и пользователями, необходимо, чтобы она была синхронизирована с системой для захвата, регулярного обновления и сохранения после удаления из внешней системы. MoReq2010 не содержит никаких указаний относительно того, каким образом все это должно осуществляться.

3.2.3 Как работают пользователи и группы

На рисунке 3а показана система отношений между пользователями и группами внутри системы управления записями.

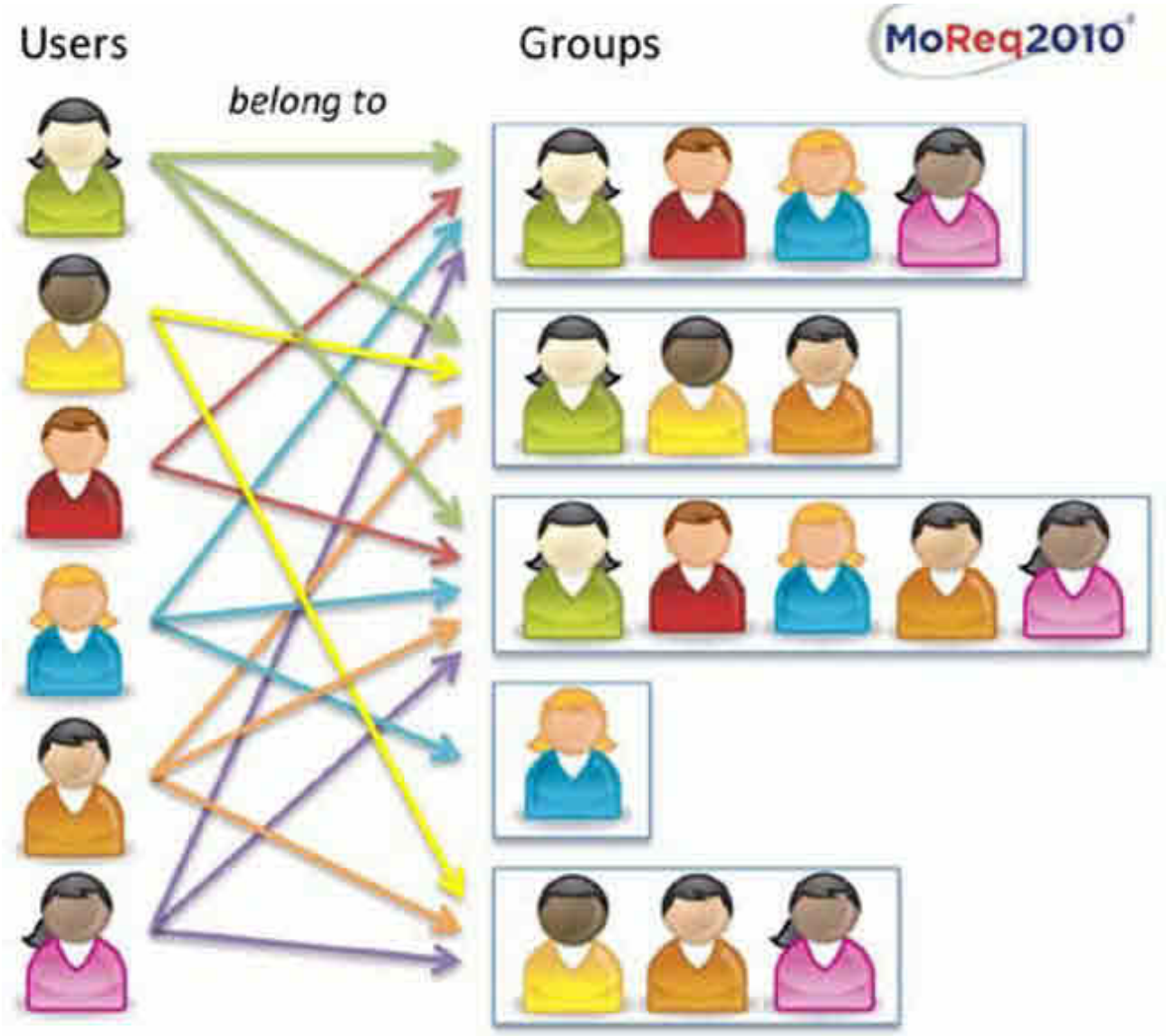

Рисунок 3а. - В системе управления записями отношения между пользователями и группами организованы по модели «многие ко многим».

Эта упрощенная структура показывает, какими должными отношения между пользователями и группами в соответствии с требованиями MoReq2010. Отслеживать отношения между пользователями и группами не требуется. На рисунке 3а видно, что некоторые группы являются по сути подгруппами других групп.

3.2.4 Удаление пользователей и групп

В службе пользователей и групп следует применять подход к удалению объектов, принятый в MoReq2010. Таким образом, после того, как удаленные объекты прекращают функционировать, о них остается запись в системе. MoReq2010 требует, чтобы пользователи и группы не удалялись полностью из системы, но сохранялись с целью воссоздания контекста для записей, хранимых в системе (см. предыдущее обсуждение в 2**.2.10 Жизненный цикл объекта**).

Функциональность остаточного (резидуального) объекта не совпадает с функциональностью

активного объекта. Если объект «Пользователь» удален, остаточный (резидуальный) пользователь не должен получать доступа к системе. В случае с остаточными (резидуальными) группами роли, назначенные членам этой группы, должны быть отменены. Следовательно, если активный пользователь включен в остаточную (резидуальную) группу, он не будет наследовать ролей, назначенных этой группе (подробнее об этом см. в **3. Типовая служба ролей**).

3.4 Функциональные требования

R3.4.1 Доступ к системе управления записями должны получать только авторизованные пользователи, для которых создан активный объект типа «Пользователь» (E14.2.16), обладающий по меньшей мере следующие метаданные:

- системный идентификатор (M14.4.100);
- метка времени создания (M14.4.9);
- дата и время создания (M14.4.61);
- метку времени начала использования (M14.4. 32);
- идентификатор группы (M14.4.36);
- название (M14.4.61);
- описание (M14.4.16);
- метка времени удаления (M14.4.17).

Для каждого объекта также имеются:

- история событий (см. **2. Системные службы**);
- список доступа (или его эквивалент, см. **4. Типовая служба ролей**) и могут также присутствовать:
- контекстуальные метаданные (или их эквивалент, см. **7. Типовая служба метаданных**).

Аутентификация пользователя представляет собой процесс установления его идентичности, на основе которого система предоставляет ему определенный уровень доступа для выполнения функций, ассоциируя каждую функцию с определенным объектом типа «Пользователь». MoReq2010 не содержит каких-либо указаний относительно того, как должен быть организован этот процесс. Простая форма аутентификации требует от пользователя ввода имени и пароля; она вполне пригодна для многих систем управления записями, но есть и другие, более сложные методы могут включать, например, двухфакторную аутентификацию, для которой требуется вводить несколько параметров.

*В зависимости от подхода, используемого в системе управления записями при внедрении 4. **Типовой службы ролей**, списки доступа MoReq2010 могут не использоваться при осуществлении системных операций и быть добавлены к объекту типа «Пользователь»*

только при экспорте.

*В зависимости от подхода, используемого в системе при внедрении 7**. Типовой службы метаданных**, способы добавления контекстуальных метаданных могут различаться для разных объектов.*

R3.4.2 Система должна поддерживать процесс создания пользователей, обладающих метаданными и другими свойствами, перечисленными в R3.4.1.

MoReq2010 не определяет, каким именно образом должен осуществляться этот процесс; при некоторых вариантах внедрения новые пользователи не могут создаваться пользователями системы управления записями. Организации должны оценить, соответствует ли решение, предлагаемое поставщиком, их производственным потребностям и требованиям к безопасности.

R3.4.3 Система должна поддерживать процесс обновления названия и описания активного пользователя и любых контекстуальных метаданных для отражения всех изменений в профиле пользователя.

*MoReq2010 не содержит никаких указаний по поводу того, каким именно образом должен осуществляться этот процесс; он может осуществляться в системе управления записями отдельно и позже синхронизироваться со службой каталогов. Однако изменение пользовательских метаданных должно быть отражено в истории событий пользователя как отдельное событие в соответствии с **R2.4.15**, **R2.4.13**.*

R3.4.4 Система должна поддерживать процессы добавления активных пользователей в активные группы и удаления активных пользователей из активных групп. При кажлдом случае добавления или удаления должно создаваться новое событие.

MoReq2010 не содержит никаких указаний по поводу того, каким именно образом должен осуществляться этот процесс; он может осуществляться в системе управления записями отдельно и позже синхронизироваться со службой каталогов. Только активные пользователи могут управлять своим членством в активных группах. Они могут быть либо добавлены в активные группы, либо удалены из них. Информация о членстве остаточного пользователя в группах на момент удаления будет сохранена. Для остаточной группы также будет сохранен список членов на момент удаления.

*Обратите внимание, что при выполнении этой функции **всегда** должно создаваться новое событие; требование R2.4.13 в данном случае не имеет силы. Создание событий осуществляется с целью обеспечения точности отчетов в соответствии с **R3.4.7** и **R3.4.13**.*

R3.4.5 Система должна поддерживать процесс полного удаления пользователя, ни разу не воспользовавшегося ей для выполнения какой-либо функции.

MoReq2010 не содержит никаких указаний по поводу того, каким именно образом должен осуществляться этот процесс; он может осуществляться в системе управления записями

отдельно и позже синхронизироваться со службой каталогов. Когда пользователь впервые использует систему для выполнения какой-либо функции, должна создаваться метка времени для первого использования.

R3.4.6 Система должна поддерживать процесс удаления пользователя, который использовал ее для выполнения той или иной функции.

MoReq2010 не содержит никаких указаний по поводу того, каким именно образом должен осуществляться этот процесс; он может осуществляться в системе управления записями отдельно и позже синхронизироваться со службой каталогов. После выполнения какой-либо функции пользователь не может быть удален из системы полностью. После удаления должна создаваться следующая метка времени, а также сохраняться остаточный объект.

R3.4.7 В системе должна присутствовать возможность создания по запросу авторизованного пользователя отчета, в котором будет указано, в каких группах состоял конкретный пользователь системы в конкретный момент времени.

В отчет не должны содержаться группы, просмотр которых закрыт для запросившего отчет пользователя.

В отчете должны быть отражены дата и время создания и удаления объекта.

R3.4.8 Система должна обеспечивать поддержку групп, обладающих по меньшей мере следующими метаданными:

- системный идентификатор (M14.4.100);
- метка времени создания (M14.4.9);
- дата и время создания (M14.4.61);
- метку времени начала использования (M14.4. 32);
- идентификатор группы (M14.4.36);
- название (M14.4.61);
- описание (M14.4.16);
- метка времени удаления (M14.4.17).

Каждая группа включает также:

- список пользователей, являющихся ее членами;
- историю событий (см. **2. Системные службы**);
- список доступа (или его эквивалент, см. **4. Типовая служба ролей**) и могут также присутствовать:
- контекстуальные метаданные (или их эквивалент, см. **7. Типовая служба**

метаданных).

В зависимости от подхода, используемого в системе управления записями при внедрении 4. ***Типовой службы ролей****, списки доступа MoReq2010 могут не использоваться при осуществлении системных операций и быть добавлены к объекту типа «Пользователь» только при экспорте.*

В зависимости от подхода, используемого в системе при внедрении 7. ***Типовой службы метаданных****, способы добавления контекстуальных метаданных могут различаться для разных объектов.*

R3.4.9 Система должна поддерживать процесс создания пользователей, обладающих метаданными и другими свойствами, перечисленными в R3.4.1.

MoReq2010 не определяет, каким именно образом должен осуществляться этот процесс; при некоторых вариантах внедрения новые группы не могут создаваться пользователями системы управления записями.

R3.4.10 Система должна поддерживать процесс обновления названия и описания активной группы и любых контекстуальных метаданных для отражения всех изменений в профиле пользователя.

MoReq2010 не содержит никаких указаний по поводу того, каким именно образом должен осуществляться этот процесс; он может осуществляться в системе управления записями отдельно и позже синхронизироваться со службой каталогов. Однако изменение пользовательских метаданных должно быть отражено в истории событий пользователя как отдельное событие в соответствии с ***R2.4.15****,* ***R2.4.13****.*

R3.4.11 Система должна поддерживать процесс полного удаления группы, в которую не было добавлено ни одного пользователя.

MoReq2010 не содержит никаких указаний по поводу того, каким именно образом должен осуществляться этот процесс; он может осуществляться в системе управления записями отдельно и позже синхронизироваться со службой каталогов. Пользователи добавляются в группы в соответствии с R3.4.4

R3.4.12 Система должна поддерживать процесс удаления группы, членами которой являются некоторые пользователи.

MoReq2010 не содержит никаких указаний по поводу того, каким именно образом должен осуществляться этот процесс; он может осуществляться в системе управления записями отдельно и позже синхронизироваться со службой каталогов. После выполнения какой-либо функции группа, в состав которой входят или входили пользователи, не может быть удален из системы полностью. После удаления должна создаваться следующая метка времени, а также сохраняться остаточный объект.

R3.4.13 По запросу авторизованного пользователя система должна создавать отчет,

содержащий информацию о том, какие активные пользователи принадлежали к определенной группе на указанные дату и время.

В отчет не должны быть включены объекты типа «Пользователь», для просмотра которых у запросившего отчет пользователя нет прав. Пользователи должны быть активными в указанные дату и время, но могут быть неактивными на момент запроса отчета.

В отчете должна также присутствовать информация о том, соответствуют ли введенные даты и время периоду до создания группы или же до ее уничтожения.

R3.4.14 В соответствии с требованием R2.4.22, система должна позволять авторизованному пользователю просматривать пользователей и группы по крайней мере следующими способами:

- просматривать пользователей в службе пользователей и групп, а также осуществлять просмотр их метаданных;
- просматривать группы в службе пользователей и групп, а также осуществлять просмотр их метаданных;
- переходить от пользователя к группам, членом которых он является, и просматривать их метаданные;
- переходить от группы к пользователям, которые являются ее членами, и просматривать их метаданные.

*Значение термина «просматривать» разъяснено в главе **13. Глоссарий**.*