Ролевое управление доступом. Иерархия ролей. Отношения наследования

Рассмотрим более подробно систему ролевого доступа (Role-Based Access Control, RBAC). Здесь имеются удобные механизмы для соблюдения принципа минимальных привилегий. И хотя теоретически дискреционный метод доступа DAC позволяет проводить еще более тонкую настройку прав пользователя, практически невозможно проконтролировать этот процесс так, чтобы добиться реализации этого принципа. В системе, где механизм назначения прав распределен между всеми пользователями, очень сложно отследить ситуацию, когда набор прав пользователя становится неадекватным решаемым им задачам.

Согласно природе производственных отношений должностные обязанности сотрудников, занимающих разные позиции, могут частично перекрываться. Некоторые самые общие функции, такие, например, как ознакомление с инструкциями по соблюдения режима работы предприятия, резервирование отпусков, фиксирование на внутреннем сайте компании индивидуального рабочего графика и др., могут быть обязательными для всех сотрудников. Применительно к ролям это означает, что администратор должен выполнять много рутинной работы по приписыванию одних и тех же прав доступа разным ролям, в том числе вновь создаваемым. Решением этой проблемы является иерархическая организация ролей, когда одна роль может включать другую роль, тем самым расширяя свой набор прав за счет добавления прав, ассоциированных с инкапсулированной ролью.

Иерархия ролей создается определением для них отношений, называемых наследованием: в соответствии с этим определением, если роль R2 является наследницей R1, то все права роли R1 приписываются к правам роли R2, а все пользователи роли R2 приписываются к пользователям роли R1 (рис. 1). Таким образом, установление отношений наследования является еще одним способом наделения пользователя правами наряду с явным назначением пользователю некоторой роли.

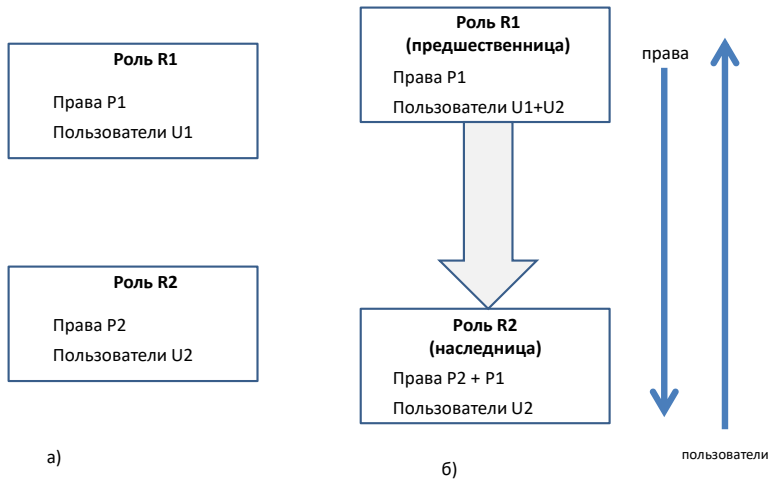

Рис. 1. Отношение наследования ролей; *а* — независимые роли; *б* — роль R2 является наследницей роли R1

Отношения наследования относятся к типу «многие ко многим», то есть у одной роли может быть несколько наследниц, и одна роль может быть наследницей нескольких ролей.

Иерархия ролей обычно в той или иной степени отражает структуру реального предприятия. На рис. 2 показан фрагмент организационной структуры предприятия.

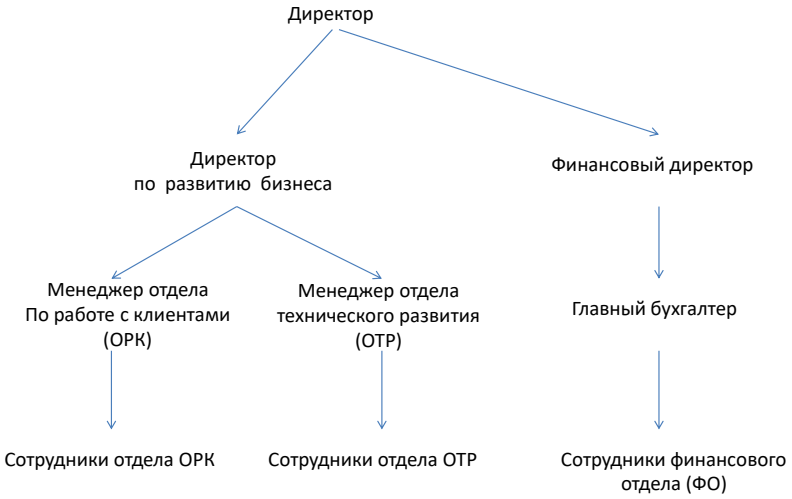

Рис. 2. Фрагмент организационной структуры предприятия

Такой *организационной структуре* может быть поставлена в соответствие *ролевая структура*, полученная в результате установления между ролями отношений наследования (рис. 3). Роль «сотрудник» представляет собой те общие, наличествующие у всех сотрудников организации права. Должность менеджера по работе с клиентами добавляет к должностным обязанностям рядового сотрудника отдела ОРК еще ряд функций. Например, менеджер обязан разрабатывать план увеличения клиентской базы, что требует доступа к некоторым финансовым документам. Находящийся с ним на одном уровне менеджер отдела развития (ОР) также нуждается в расширении прав доступа к информационным ресурсам по отношению к рядовым сотрудникам отдела ОР. После установления отношений наследования с ролями «сотрудник ОРК», «сотрудник ОТР», «сотрудник ФО» и «директор» все общие права сотрудников оказались неявным образом добавлены к этим ролям-наследницам, а их пользователи соответственно переместились наверх. Наследники следующей ступени — роли «менеджер ОРК» и «менеджер ОТР» — сами являются предшественниками для роли «директор по развитию», которая таким образом, аккумулировала права этих двух ролей.

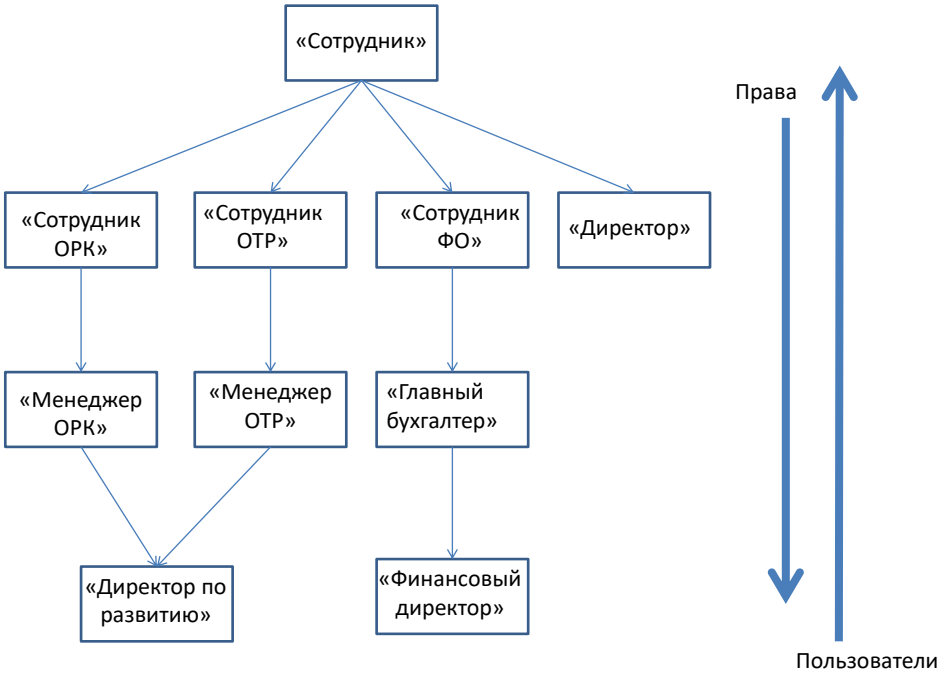

Рис. 3. Структура ролей, образованная отношениями наследования

Важным положением безопасности является *принцип разделения обязанностей*, в соответствии с которым некоторые должностные функции не должны поручаться одному и тому же человеку. К примеру, сотрудник, которому назначена роль «инженер», побывав в командировке, должен после возвращения составить финансовый отчет о своих тратах. Затем этот отчет должен быть проверен и представлен к оплате, эти действия возлагаются на сотрудника, отнесенного к роли «сотрудник финансового отдела». Понятно, что такое совмещение функций, то есть одновременная принадлежность одного пользователя к ролям «инженер» и «сотрудник финансового отдела», является нежелательным. Чтобы избежать подобных ситуаций, в методе RBAC предусмотрен специальный механизм, накладывающий ограничения на приписывание ролей пользователям. Этот механизм действует следующим образом. Совокупность ролей, относительно совмещения которых нужно устанавливать ограничения, объединяется в устойчивую группу и к ней приписывается число-ограничитель. В нашем случае это группа ролей {«инженер», «сотрудник финансового отдела»}, которой должен быть приписан ограничитель 1. Если теперь администратором будет сделана попытка приписать пользователю обе эти роли, то система заблокирует его действия.