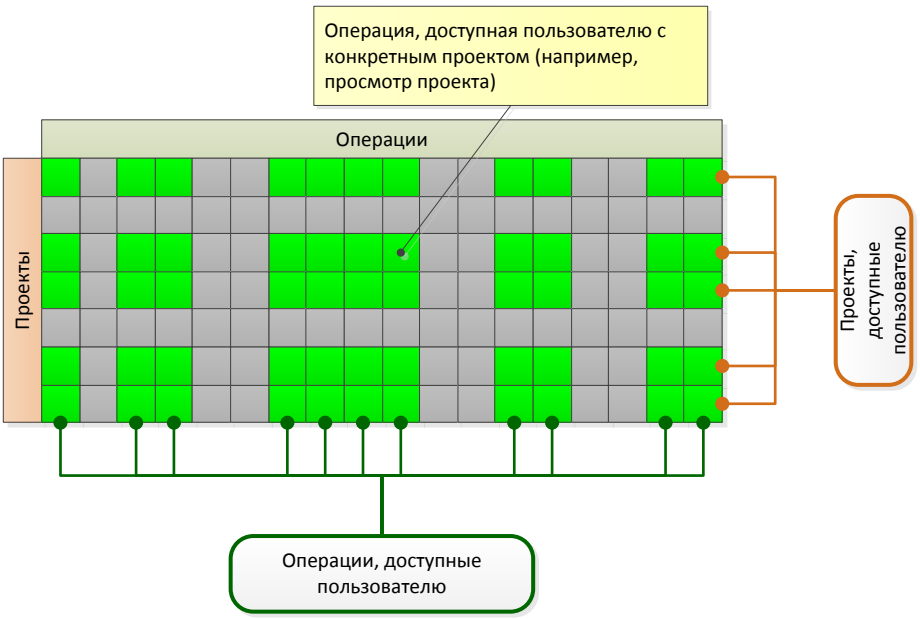
Разграничение доступа при работе с системой

Оглавление

Доступ к операциям и доступ к информации

Одна и особенностей системы – обеспечение ролевого доступа пользователей к функциям системы (например, разрешение на работу с клиентской базой) и к различным видам информации (доступ к конкретным клиентам, проектам и т.п.).

Пользователь с одной стороны имеет право на выполнение некоторых операций в системе с одной стороны (например, создание проекта, управление проектом и т.п.), а с другой стороны, имеет право на работу с конкретными проектами.

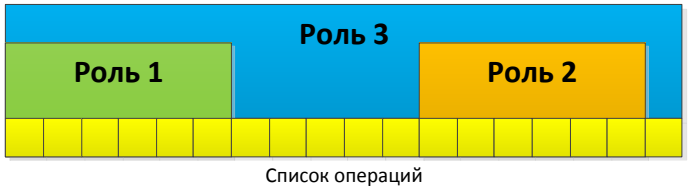


Это означает, что пользователь имеет возможность выполнять только определенные операции с определенными проектами.

Также существует ряд операций в системе, не связанных непосредственно с проектами (например, заведение нового пользователя, настройки системы и т.п.). Для этих операций также определяется возможность их выполнения конкретным пользователем.

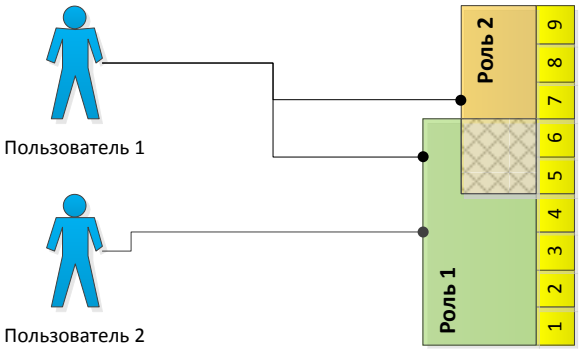
Понятие роли

Под ролью в системе понимается список операций, сгруппированных по какому-либо признаку. Роль создается ля того, чтобы нескольким пользователям, имеющим одинаковые функциональные обязанности (например, менеджерам из отдела продаж), выделять одинаковые права на выполнение операций. Единожды собрав операции в группу (роль) можно присваивать данную роль нескольким пользователям.



Одна операция может входить одновременно в несколько ролей.

Каждому пользователю может быть присвоена одна или несколько ролей. При присвоении пользователю роли пользователь получает доступ ко всем операциям, входящим в данную роль.



Рассмотрим пример на рисунке. Мы создали две роли: «Роль 1» обеспечивает права на операции с 1 по 6, а «Роль 2» – с 5 по 9. Пользователю 1 присвоено 2 роли – «Роль 1» и «Роль 2». Это означает, что «Пользователь 1» может выполнять все операции, входящие в обе роли (т.е. с 1 по 9). «Пользователю 2» присвоена только «Роль 1» и он может выполнять только операции с 1 по 6.

Заштрихованный участок на рисунке означает, что операции 5 и 6 могут выполнять пользователи, которым присвоена или «Роль 1», или «Роль 2», или обе роли сразу.

Подходы к настройке ролей

На практике существуют два подхода к разделению операций по ролям – функциональный и административный.

Функциональный подход

При функциональном походе все операции группируются в роли без пересечений. При этом каждая операция попадает в конкретную роль. Фактически в данном случае роль представляет собой группу прав. Например, создадим роль с именем «Настройка пользователей»:

Название роли	Список операций, доступных для роли
Настройка пользователей	Создание роли
	Удаление роли
	Просмотр списка ролей
	Изменение свойств роли
	Создание пользователя
	Удаление пользователя
	Просмотр списка пользователей
	Изменение данных пользователя

Данная роль может быть присвоена тем пользователям, которые будут иметь право создавать новых пользователей, изменят права пользователей и т.п. Как правило, людей в компании, имеющих право выполнять данные операции – 1-2 в системе. Эти людям присваивается настроенная нами роль.

Таким же способом все остальные операции разбиваются по ролям и пользователям выдаются права на операции путем присвоения списка нужных ролей.

Административный подход

При административном подходе пользователи системы ассоциируются с административными должностями и в роли собираются операции, которые необходимо выполнять тому или иному административному пользователю.

Например, можно завести две роли:

- Менеджер отдела продаж
- Руководитель отдела продаж

Роль Менеджера отдела продаж будет включать все необходимые операции, которые позволят пользователю заниматься продажами, такие как работа с клиентами (добавление, изменение, создание контактов и т.п.), работа с проектами (создание проектов, управление проектами и т.п.). Роль Руководителя отдела продаж будет включать в себя все операции, входящие в роль Менеджера отдела продаж (Руководитель также совершает самостоятельные продажи), а также ряд дополнительных операций, которые рядовым Менеджерам по продажам недоступны (например, Удаление пользователя, Удаление проекта, редактирование некоторых справочников, получение отчета по менеджерам и т.п.), т.е. те операции, которые требуют более высокого уровня административной ответственности.

При таком подходе каждая административная должность будет иметь соответствующую ей роль с соответствующим набором прав.

Смешанный подход

На практике встречаются оба описанных подхода распределения прав. Функциональный удобен, если административные функции пользователей в реальной жизни четко не описаны (тогда применение административного подхода вызывает необходимость постоянного изменения ролей с изменением административных функций должности).

Административный подход удобен, если в компании «устоялись» функциональные обязанности каждой должности и можно четко определить список операций, выполняемых каждой должностью.

Разграничение доступа к информации

Помимо разделения доступа к функциям системы существует разделение доступа к информации. Под информацией, хранящейся в системе, понимаются:

- Карточки клиентов и информация, находящаяся в них
- Проекты
- Документы в проектах
- Финансовая информация по проектам

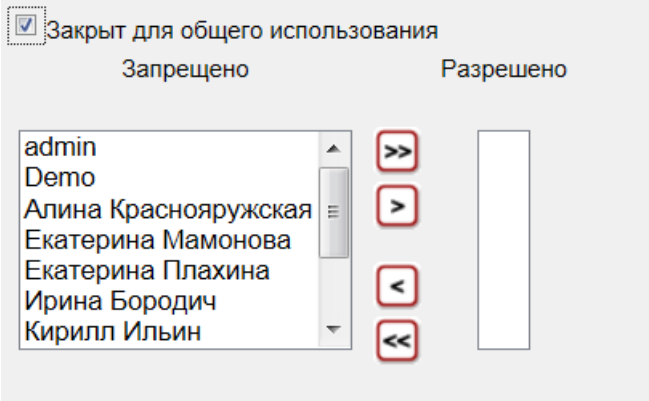
и т.д.

Разграничение доступа информации делается для того, чтобы все пользователи не имели возможности просматривать и изменять информацию по всем клиентам и всем проектам.

Доступ к клиентской базе

В системе каждый клиент закрепляется за конкретным пользователем. Данный пользователь имеет право на безусловное изменение всех данных по клиенту. Он может изменять имя клиента, другие данные по клиенту, добавлять контактных лиц, контакты, файлы и т.п.

При этом у каждого клиента существует свойство «Закрыт от общего использования».



Пока данное свойство не установлено, то данные по клиенту могут видеть все пользователи, имеющие право на соответствующие операции (просмотр карточки клиента, изменение карточки клиента и т.п.). Однако, если установить указанное свойство, то все пользователи, кроме Менеджера клиента, не имеют больше права на работу с данным клиентом.

Менеджер клиента может явно указать, кто кроме него имеет право доступа к карточке клиента, выбрав необходимых пользователей из списка и явно «разрешив» им работать с карточкой клиента. Все остальные пользователи, которым не разрешен явно доступ к карточке клиента, не будут иметь доступа к информации по клиенту.

Но, в некоторых случаях пользователи, которые не имеют доступа к карточке клиента должны иметь какую-то (пусть не всю) информацию о клиенте. Например, один менеджер должен знать, что такой-то клиент у компании есть и за него отвечает конкретный менеджер.

Задача решается определением политики доступа к информации при использовании «закрытого доступа».

Политика доступа к «закрытым» карточкам клиентов

В настройках системы (Главное меню -> Настройки -> Отображение -> Доступ к информации о клиентах) есть возможность настроить политику доступа к закрытым клиентам. Существуют две политики доступа:

- Информация о закрытых клиентах видна только тем пользователям, для которых настроен доступ
- Доступ к информации о закрытых клиентах для пользователей, которым запрещён доступ, определяется правилами доступа

В первом случае (когда доступ полностью закрыт), никакая информация по «закрытым» клиентам не отображается никому, кроме явно разрешенных пользователей. Т.е. клиент становится «прозрачным» и виден только определенному кругу лиц.

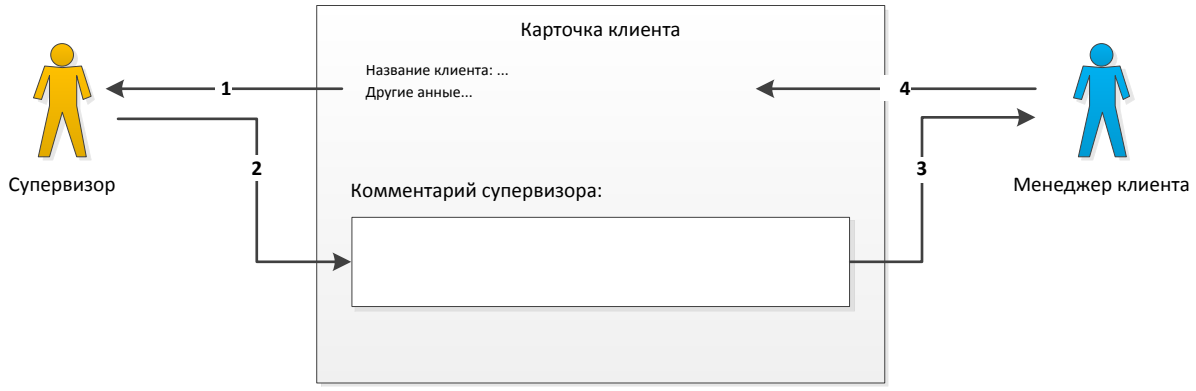
Во втором случае система позволяет явно определить, какие поля карточки клиента будут доступны для просмотра «остальным» пользователям, а какие поля будут доступны даже для редактирования.

Например, если мы хотим, чтобы по закрытым клиентам показывалась только информация о названии клиента и о менеджере, за которым данный клиент закреплен, то мы можем настроить систему соответствующим образом в настройках системы. Для каждого поля карточки клиента (включая пользовательские поля) может быть определено правило, может ли данное поле быть доступным для просмотра и/или редактирования пользователями, у которых нет явного доступа к карточке клиента.

Супервизор клиентов

При разграничении доступа к клиентам бывают ситуации, когда менеджер, за которым закреплен клиент, недоступен (заболел, в отъезде и т.п.). При этом, если клиент «Закрыт от общего использования», то изменить информацию по клиенту никто другой не может. Для решения данной проблемы в системе была введена специальная операция – «Супервизор клиента».

Пользователи, имеющие права на операцию «Супервизор клиента», могут видеть все карточки клиента вне зависимости от того, закрыты клиенты от общего использования или нет. Супервизор не имеет права редактировать свойства клиента, однако в карточке присутствует поле «Комментарий супервизора», в которое супервизор может вписать любую информацию. Впоследствии, когда менеджер увидит комментарии и сможет самостоятельно внести в карточку клиента необходимые изменения.



Последовательность работы с карточкой клиента:

1. Супервизор получает необходимую информацию по клиенту
2. Супервизор вносит изменения и комментарии в соответствующее поле
3. Менеджер клиента прочитывает комментарии
4. Менеджер клиента вносит необходимые изменения в поля карточки клиента и удаляет комментарии

Указанный подход позволяет с одной стороны обеспечить информацией о клиенте заинтересованных лиц в случае отсутствия менеджера клиента (через супервизора), с другой стороны, позволяет защитить карточку клиента от изменений, которые могут выполнены кем-то кроме менеджера клиента в отсутствие последнего, однако донести информацию о нужных изменениях до менеджера клиента.

Доступ к информации по проектам

Каждый проект содержит:

- общую информацию по проектам (название клиента, свойства проекта, пользовательские поля проекта)
- информацию по этапам проекта
- документы внутри этапов проекта

Доступ к каждому виду информации внутри проекта может быть ограничен.

Доступ к информации по проекту

Чтобы ограничить доступ к информации по проекту необходимо в свойствах проекта указать свойство «Закрыт для общего использования». Принцип работы ограничения от общего использования аналогичен закрытию доступа к общему использованию карточки клиента за исключением того, что для карточки клиента мы можем определить, какая информация остается открытой, а для проекта нет. Если доступ к проекту закрыт, то он закрыт для всех, кроме тех пользователей, которые непосредственно участвуют в проекте.

К таким пользователям относятся:

- менеджер проекта
- ответственные за этапы проекта
- авторы документов в этапах проекта
- получатели документов в этапах проекта

У каждого из вышеуказанных пользователей своя роль в проекте.

Менеджер проекта может просматривать и изменять информацию по проекту, видеть отчеты по проекту. Ответственный за этап имеет право просматривать информацию по своему этапу, загружать и получать документы по своему этапу. Авторы документов имеют право подгружать документы в те этапы, где они указаны как Авторы. Получатели документов имеют право скачивать документы в этапах, где они указаны как Получатели.

Таким образом, менеджер проекта является главным лицом в проекте и может все? Нет, это не так. Чтобы разобраться в возможностях менеджера проекта рассмотрим два типа «менеджеров», встречающихся на практике.

Управляющие и Администраторы

В различных компаниях менеджеры проектов выполняют различные функции. Два основных типа менеджера проектов – это Управляющий и Администратор. Эти два типа различаются по уровню возложенной на них ответственности в проекте.

Управляющий проектом как правило имеет возможность не только следить за выполнением проекта, но и активно влиять на ход проекта, принимать решения о сдвиге сроков проекта, изменять ответственных за этапы проекта и т.п. Основная функция Управляющего – именно управлять проектом, то есть вносить изменения в проект в зависимости от текущей или ожидаемой ситуации. Управляющему должно быт разрешено изменение сроков отдельных этапов, смена ответственных за этапы, работа с документами проекта и т.д. Главное, что отличает Управляющего – наличие ответственности за выполнение проекта и наличие возможностей это ответственность реализовать.

Администратор проекта напротив выполняет функции «слежения» за ходом проекта и, в случае отклонения хода проекта от намеченного, должен эскалировать возникшую проблему «вверх» до лица, принимающего решение о внесении изменений в проект.

Для поддержания обеих моделей «менеджеров» в системе предусмотрено разделение операций по изменению проекта на две:

- Изменение данных проекта
- Изменение свойств этапов проекта

Первая операция позволяет вносить изменения в общую информацию о проекте (создавать проект, подключать клиента, изменять пользовательские свойства проекта и т.п.), но не разрешает изменять свойства этапов. Вторая операция напротив позволяет изменять свойства этапа (менять ответственного, изменять даты предупреждения и паники, менять списки Авторов и Получателей этапов).

Таким образом, менеджеры проектов, выполняющие функции Управляющего, должны иметь права на обе вышеперечисленные операции, а Администраторы – только на изменение свойств проекта.

В зависимости от логической роли менеджера проекта в компании возможности каждого конкретного пользователя, который будет выступать в качестве менеджера проектов, должны быть определены заранее установкой прав на соответствующие операции в настройке роли.

Доступ к информации по этапу

К информации по этапу имеют доступ:

- Менеджер проекта (если не установлено специальное запрещение, о котором будет сказано ниже)
- Ответственный за этап
- Авторы документов этапа
- Получатели документов этапа

Ответственный за этап следит за сроками завершения этапа, проверяет документы, загруженные авторами, и визирует этап после того, как все документы загружены и проверены. Ответственный за этап имеет право самостоятельной загрузки документов в этап.

Авторы этапа имеют право загружать документы в этап, а также скачивать документы этапа.

Получатели документов имеют право только скачивать документы этапа и ничего больше.

Специальные ограничения при работе с этапами

Менеджер проекта по умолчанию имеет право выступать в качестве Автора и Получателя документов любом этапе. Однако если менеджер выступает в качестве Администратора, а не Управляющего, то можно запретить менеджеру проекта доступ к документам этапов.

В настройках системы (Главное меню -> Настройки -> Дополнения -> Параметры системы) можно установить свойство:

«Разрешить менеджеру проектов загружать и получать документы этапов»

Данное свойство установлено по умолчанию. Для запрета доступа менеджера проекта к документам этапа необходимо снять «галку» у данного параметра.

По умолчанию если пользователь является Ответственным за один из этапов проекта, Автором или Получателем в одном из этапов, то такой пользователь может просматривать информацию по другим этапам проекта. Если требуется, чтобы этапы были «автономны» и к информации по этапу имели доступ только пользователи, являющиеся Ответственным за этот этап, Автором в этом этапе или Получателем в этом этапе, то необходимо снять общее разрешение в настройке параметров системы.

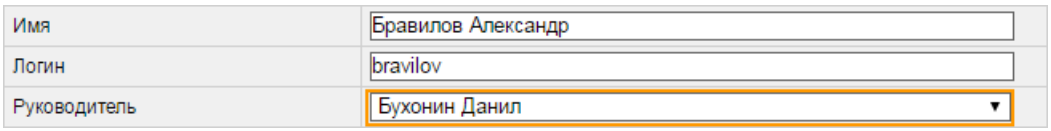
В настройках системы (Главное меню -> Настройки -> Дополнения -> Параметры системы) можно снять свойство:

«Разрешить просмотр данных этапа пользователям, не являющимся авторами, получателями, ответственными за этап или менеджерами проекта»

После этого доступ к каждому этапу проекта будет иметь доступ только Ответственный за этап, Авторы этого этапа и Получатели этого этапа. Остальные пользователи не смогут смотреть информацию по данному этапу и будут получать сообщение «Доступ к этапу запрещен» при попытке перейти в этап.

Иерархия и наследование прав доступа

У каждого пользователя можно определить «руководителя». Руководитель – это другой пользователь, обладающий всеми правами своих подчинённых. Настроить руководителя для пользователя можно в свойствах пользователя (Главное меню -> Настройки -> Пользователи -> Пользователи -> Редактировать пользователя):



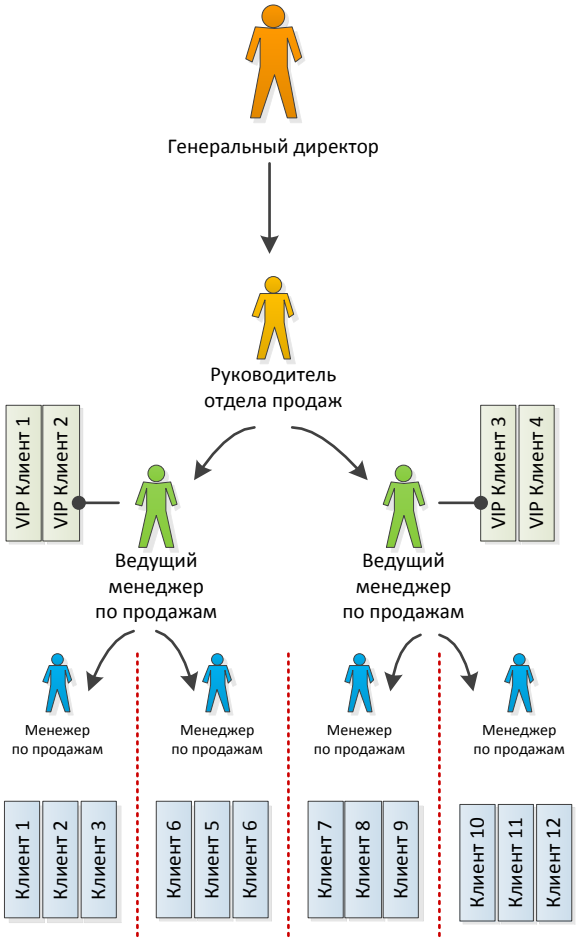
Все операции, доступные пользователю также доступны его руководителю. Все права на информацию (например, доступ к клиентам, к проектам, к этапам) доступны руководителю.

Например, если пользователь является менеджером клиента, то его руководитель также может просматривать и изменять информацию по этому клиенту.

Однако, если в карточку клиента были внесены изменения (например, создан новый контакт), то данные изменения будут созданы от имени руководителя, а не от имени подчиненного. Т.е. если при создании нового контакта с клиентом руководитель зашел в карточку клиента с правами подчиненного, то контакт будет создан от имени руководителя, а не от имени подчиненного, и ответственность за выполненное действие будет лежать на руководителе, а не на подчиненном.

У каждого пользователя может быть руководитель. Это означает, что если пользователь является руководителем для одного или нескольких пользователей, то он, в свою очередь, может быть подчиненным для руководителя более высокого уровня. При этом принцип наследования прав подчиненных сохраняется по всей иерархии подчинения, е если на вершине иерархии стоит, к примеру, генеральный директор, а внизу иерархии расположились рядовые менеджеры, до генеральный директор будет обладать всеми правами всех рядовых менеджеров.

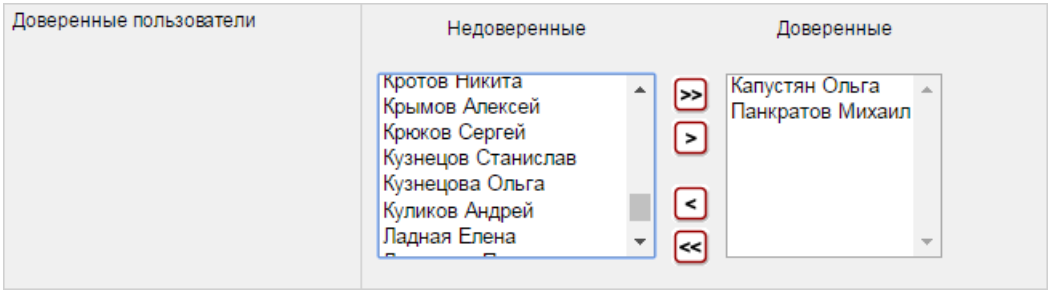
Такая модель позволяет строить древовидные иерархии с любым количеством уровней. Ниже представлен пример разделения доступа к клиентам на основе иерархии, построенной на указании руководителей.



Каждый менеджер по продажам работает только со своими клиентами, не видя при этом клиентов других менеджеров по продажам. Ведущие менеджеры по продажам работают со своими VIP клиентами, не видя VIP клиентов друг друга, и могут также иметь доступ к информации по клиентам своих подчиненных. Руководитель отдела продаж не имеет своих клиентов (хотя и может), но при этом контролирует всех клиентов компании в целом. Генеральный директор также видит всех клиентов компании, являясь руководителем Руководителя отдела продаж.

Доверенные пользователи

Пользователь может иметь одного или нескольких доверенных пользователей. Доверенный пользователь имеет права доступа к объектам такие же, как и у доверителя, но выполняет действия от своего имени. Например, если доверитель является менеджером проекта, то доверенный пользователь тоже может выполнять функции менеджера для данного проекта.



Права предоставляются доверителем только доверенному пользователю, но не его руководителю. Таким образом, руководители доверенных пользователей не получают автоматически прав, доверенных их подчиненным.

Команда проекта

Команда проекта – это список «должностей», участвующих в каждом проекте. Например, в каждом проекте может быть «Менеджер проекта», «Архитектор», «Дизайнер», «Технолог», «Прораб», «Бухгалтер» и т.д.

Команда проекта настраивается в одноименном словаре:
Главное меню -> Настройки -> Словари -> Команда проекта.

При создании проекта (или после создания проекта при его редактировании), можно указать какой конкретно пользователь выступает в той или иной «должности» в данном конкретном проекте.

Каждый член проекта имеет свой набор прав на операции в проекте (список прав указывается при настройке команды проекта). Например, «Бухгалтер» имеет право только вносить платежи и смотреть финансовый отчет, «Технолог» имеет возможность делать заявки по проекту и т.д.

Также члена команды проекта можно настроить в шаблоне этапа в качестве Ответственного за этап, Автора или Получателя документов этапа.

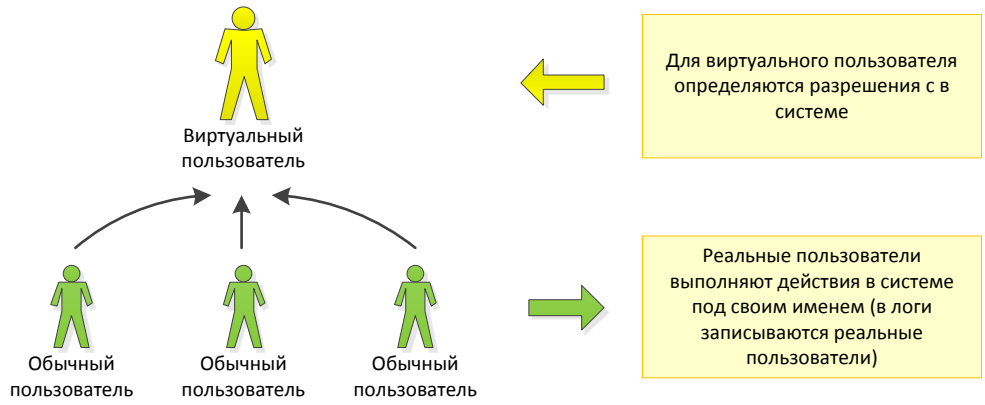
Например, «Дизайнер» может являться ответственным за этап «Дизайн» (т.е. можно определить при настройке шаблона этапа, что не конкретный пользователь Петров будет ответственным за этап, а член команды проекта с должностью «Дизайнер»),

Таким образом, можно определить ВСЕ роли в проекте заранее на стадии настройки шаблона проекта и шаблона этапов, а при создании проекта указывать, какие конкретные пользователи будут выступать в той или иной «должности» в проекте (будут в команде проекта).

Виртуальные пользователи

Виртуальные пользователи представляют собой несуществующих пользователей, от имени которых могут работать в системе другие пользователи. Можно ассоциировать «виртуального» пользователя с группой пользователей, однако это не совсем правильная ассоциация. Группа пользователей объединяет в себе нескольких совершенно разных пользователей, а виртуальный пользователь воспринимается как один пользователь, аналогичный обычным пользователям.

Виртуальные пользователи содержат одного или более обычных пользователей.



Виртуальный пользователь создается в том же окне, что и реальный пользователь:

Главное меню -> Настройки -> Пользователи -> Пользователи -> Создать виртуального пользователя

В данном примере создается виртуальный пользователь с именем «Виртуальный» и определяется, что под этим пользователем могут работать «Менеджер 1» и «Менеджер 2».

Виртуальный пользователь может быть (как и обычный пользователь») менеджером проекта, ответственным за этап, Автором, Получателем и т.п. Везде, где можно настроить ответственным обычного пользователя, можно настроить ответственным и виртуального пользователя.

Например, если виртуального пользователя сделать ответственным за этап, то любой из входящих в него реальных пользователей может поставить визу на этап. При постановке визы на этап система будет показывать, что визу поставил конкретный обычный пользователь.

Виртуальных пользователей удобно использовать в нескольких случаях. Посмотрим на примерах.

Пример 1

В компании есть два менеджера, которые одновременно работают с одним и тем же VIP клиентом. В этом случае можно создать виртуального пользователя, сделать его менеджером клиента. Тогда оба входящих в него обычных пользователя будут иметь одинаковый доступ к данному клиенту.

Пример 2

В компании есть три курьера, которые работают параллельно. В проекте предусмотрен этап «Доставка документов клиенту». Заранее непонятно, кто из курьеров будет свободен, поэтому визу на этапе должен поставить тот, кто реально отвезет документы клиенту.

Создается виртуальный пользователь «Курьеры», который в шаблоне этапа указывается как ответственный за этап «Доставка документов клиенту». Кто-то из реальных курьеров доставляет документы и ставит визу на этап (поскольку виртуальный пользователь является ответственным за этап, то от его имени визу может поставить любой из курьеров). Свободный курьер отвозит документы и ставит визу на этап. Система показывает, что визу поставил конкретный пользователь. При этом снять визу может также любой из курьеров.

Пример 3

В компании выделен один менеджер для работы с VIP клиентами. В текущий момент менеджер Иванов выполняет роль менеджера по работе с VIP клиентами, но предполагается, что менеджер по VIP клиентам может поменяться. В этом случае необходимо автоматически переключить всех VIP клиентов на нового менеджера.

Эта задача решается путем заведения виртуального менеджера «Менеджер VIP», у которого есть только один реальный пользователь Иванов. Для всех VIP клиентов менеджером клиента устанавливается виртуальный пользователь «Менеджер VIP» и только Иванов имеет доступ к данным клиентам.

В какой-то момент времени Иванов увольняется и в должность менеджера по VIP вступает Панов. В этом случае достаточно пользователя Панова добавить в виртуального пользователя «Менеджер VIP» и убрать Иванова. Все VIP клиенты автоматически будут управляться теперь менеджером Пановым.

Когда удобно использовать виртуальных пользователей? Несколько случаев:

1) Если в компании существует должность, на которой часто меняются занимающие её лица
2) Когда в какой-то должности в разный момент времени выступают разные лица
3) Когда необходимо установить равноправный доступ к какой-то сущности (клиент, проект, ответственный) нескольким пользователям, а система подразумевает установку ответственным только одного пользователя

Также надо понимать, что везде, где система предполагает использование в качестве ответственного лица одного пользователя, то предполагается строгая ответственность конкретного пользователя за выполняемые действия. Использование виртуальных пользователей «размывает» ответственность (поскольку действие может быть выполнено несколькими

пользователями), хотя и позволяет зафиксировать, каким конкретно пользователем было выполнено данное действие.