Подсистема настройки прав доступа

Содержание

Концепция подсистемы настройки прав доступа 1
Общая характеристика подсистемы 2
Работа по шагам 3
Шаг 1. Определение функции пользователя 3
Шаг 1.1. Создание функции пользователя 3
Шаг 1.2. Задание запретов 3
Шаг 2. Определение рабочего место пользователя 6
Шаг 2.1 Добавление рабочего места пользователя системы 6
Шаг 3. Определение пользователя 7
Шаг 3.1 Добавление нового пользователя 7
Шаг 4. Сохранение информации в подсистеме настройки прав доступа 8
Место хранения информации подсистемы настройки прав доступа 8

Концепция подсистемы настройки прав доступа

В описываемой подсистеме можно настроить права доступа (разрешить или запретить доступ) как к каждому отдельному системному ресурсу, так и к его отдельным частям (полям или группам характеристик). При этом можно как разрешить доступ к системному ресурсу с правом изменения его отдельных атрибутов, так и только с правом просмотра (но без права изменения). Можно также полностью запретить доступ ко всему системному ресурсу или его отдельному свойству или характеристике (полю или группе характеристик).

Рассмотрим основные понятия подсистемы настройки прав доступа (рисунок 1).

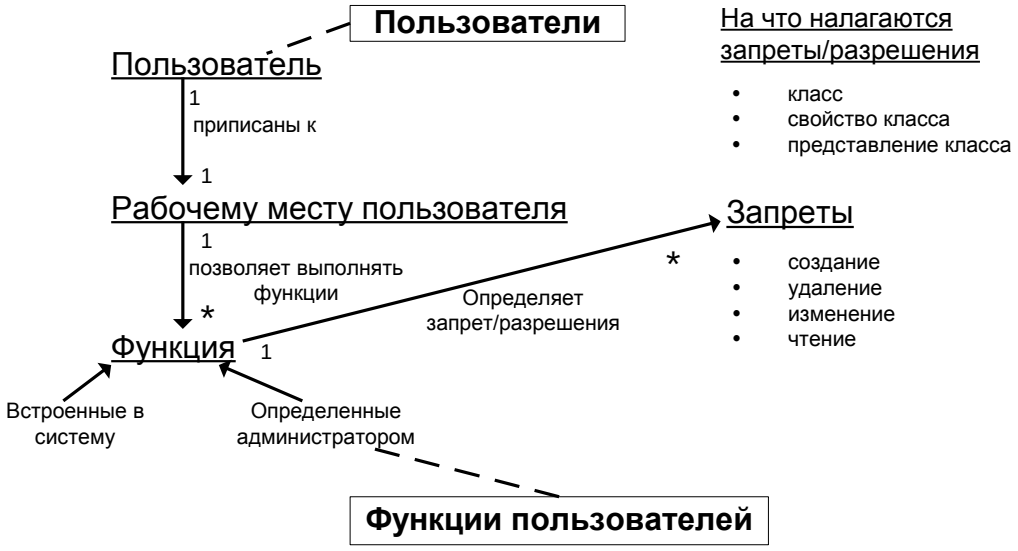


Рисунок 1 – Структура понятий подсистемы

Пользователь реестровой системы связан с учетной записью Windows. Аутентификация клиентов осуществляется средствами Internet Information Server (IIS). При подключении клиента к серверу система находит соответствующего пользователя реестровой системы по названию учетной записи Windows. К работе с системой допускаются только те клиенты, учетные записи которых присутствуют в списке пользователей. Каждый *пользователь* реестровой системы приписан к одному *Рабочему месту пользователя.*

Каждому *Рабочему месту пользователя* разрешено выполнять набор *Функций (Настраиваемые* и *Предопределенные).*

Набор *Предопределенных функций* фиксирован системой, администратор не может добавить или изменить эти функции. В систему встроены следующие предопределенные функции:

- настройка прав доступа;
- просмотр журнала изменений;
- экспорт данных.

Настраиваемые функции определяются администратором безопасности как набор ограничений (*запреты для .../запреты для всех, кроме...*) на выполнение элементарных операций над классами и элементами класса. Системой контролируется следующие элементарные операции над классом объектов:

- создание объекта данного класса;
- чтение всего объекта вместе со всеми подобъектами;
- удаление объекта данного класса;
- чтение определенного свойства класса;
- изменение определенного свойства класса;
- получение представления класса (выходные документы);
- операции над подобъектами (вложенными классами).

Если в *функции пользователя* определить набор ограничений как «*запрет для всех, кроме..*», то эти ограничения будут применяться для всех *рабочих мест*, у которых эта функция не включена. Таким образом, элементарные операции, определенные в «***запретах для всех кроме…***», будут **разрешены** только тем *рабочим местам*, в которых эта *функция* **включена**.

Если в *функции пользователя* определить набор ограничений (элементарных операций) как «***запрет для...***», то эти элементарные операции будут **запрещены** только для тех *рабочих мест*, в которых эта *функция* **включена**.

По умолчанию все операции над объектами всех классов разрешены всем пользователям, пока администратор безопасности не установит ограничения на выбранные реестровые классы.

Общая характеристика подсистемы

Система настройки прав доступа оформлена в виде отдельного рабочего места системного администратора, и недоступна для обычных пользователей. При загрузке по электронному адресу: **http://<имя сервера>/<название приложения>/inmeta/security** появляется главная страница подсистемы представленная на рисунке 2.

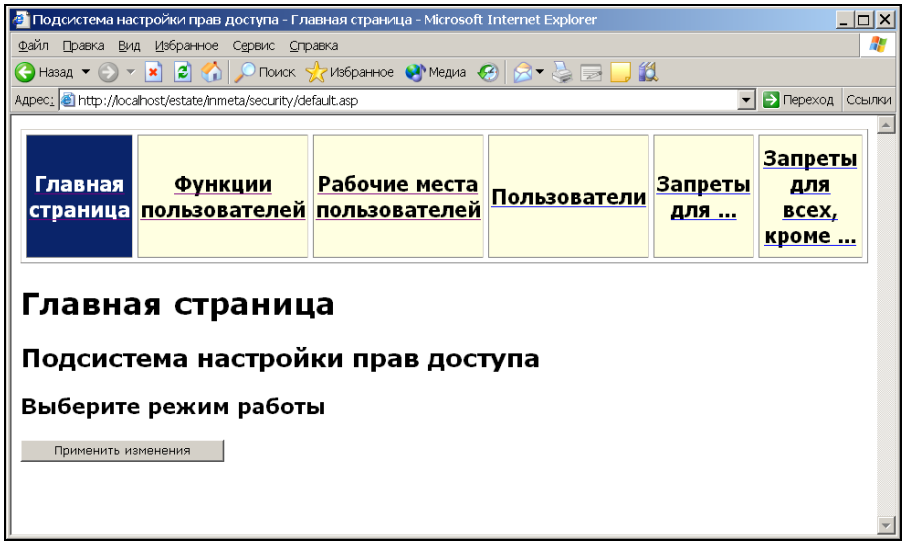


Рисунок 2 - Главная страница подсистемы

На этой странице администратором определяются все функции по настройке прав доступа. Здесь можно перейти на любую из секций, с помощью которой администратор по настройке прав доступа может разрешить или запретить доступ ко всему системному ресурсу или к его части. После настройки подсистемы необходимо сохранить данные изменения. Для этого нужно вернуться с текущей страницы на главную и нажать кнопку «Применить изменения».

Работа по шагам

Шаг 1. Определение функции пользователя

Функция пользователя – это набор ограничений доступа к различным операциям над реестровыми ресурсами (создание, удаление объектов, изменение характеристик объектов и т.п.). Если на определенную функцию настроить **«запреты для всех, кроме…»** (например, на изменение свойства класса), то данный запрет будет применяться ко всем пользователям, не обладающим этой функцией. Перечисленные операции смогут выполнять только пользователи, обладающие этой функцией. На данном шаге мы определим ограничения доступа.

Шаг 1.1. Создание функции пользователя

Допустим Вам необходимо, в рамках политики ограничений прав доступа, ограничить всех пользователей системы, кроме некоторых в **изменении, создании и удалении почтового адреса здания**. Для этого добавим новую функцию, которая ограничит всех пользователей системы, кроме тех, кому назначит ее администратор. Чтобы добавить функцию, необходимо выполнить операцию "Добавить", которая находится в последней строке таблицы со списком «Заголовок функции».

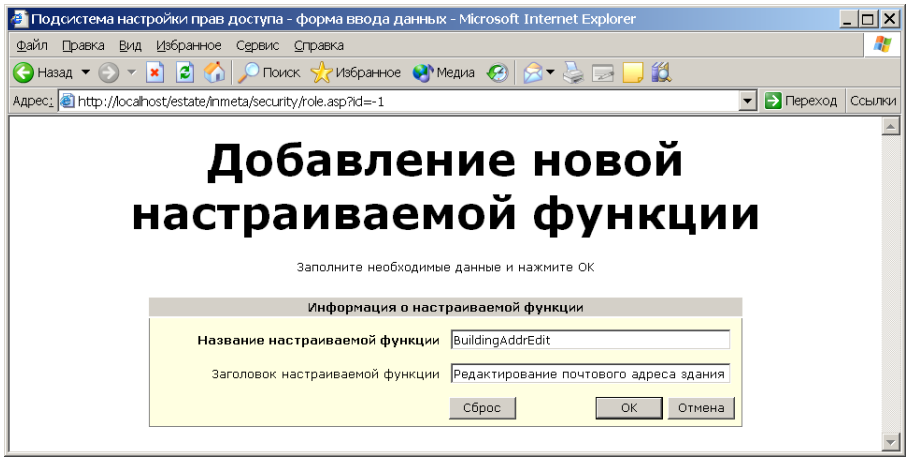


Рисунок 3 - Страница для добавления новой функции

На рисунке 3 изображен процесс добавление функции «Редактирование почтового адреса». Чтобы сохранить изменение нажмите кнопку «OK». Кнопка "Сброс" позволяет вернуться к исходному состоянию, т.е. если осуществлялся ввод новой функции, то поля для ввода очистятся, а если осуществлялась корректировка, то в полях для ввода появится исходная информация. Кнопка "Отмена" позволяет отменить выполняемую операцию и вновь вернуться в предыдущее окно. Естественно, если в данном случае какая-то информация была введена в поля формы, то она будет потеряна.

Шаг 1.2. Задание запретов

Итак, после того, как добавили функцию необходимо ограничить ее использование среди пользователей системы. Для этого напротив введенной Вами функции в столбце

«Запреты для всех, кроме…» нужно перейти по ссылке «Добавить», после чего откроется страница представленная на рисунке 4.

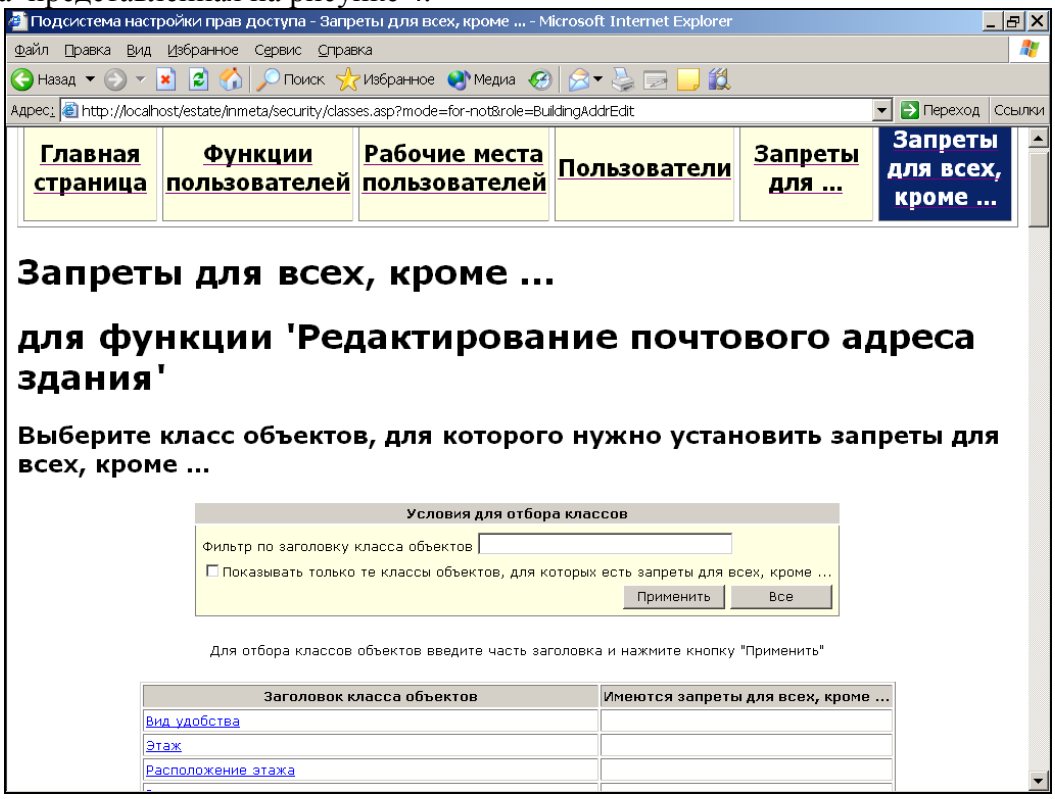


Рисунок 4 - Страница для выбора реестровых данных

На странице «Запреты для всех, кроме…» осуществляется настройка ограничений прав доступа, то есть пользователям запрещается работать с конкретными ресурсами.

В нашем примере пользователь, обладающий функцией «Редактирование почтового адреса здания» будет иметь право доступа с действиями – **создать и удалить класс «Адрес» с изменениями всех свойств данного класса**, а пользователям, у которых не отмечены данные функции, будут запрещены изменения в данном классе, кроме чтения. Для этого в списке класса объектов выбрать, нажатием мыши по заголовку, объект «**Здание**», откуда перейти во вложенный класс «**Адрес**» (рисунок 5). Далее необходимо сохранить эти изменения, нажав на кнопку «ОК». Следует отметить, что если пометить галочкой «все свойства класса», то это значит, что нет необходимости помечать свойства дальше по списку, на изменении всех свойств стоит ограничение прав доступа. После сохранения изменений мы вернемся на страницу родительского класса «**Здание**», где можно убедиться в том, что теперь во вложенном (дочернем) классе «**Адрес**» стоят запреты (рисунок 6).

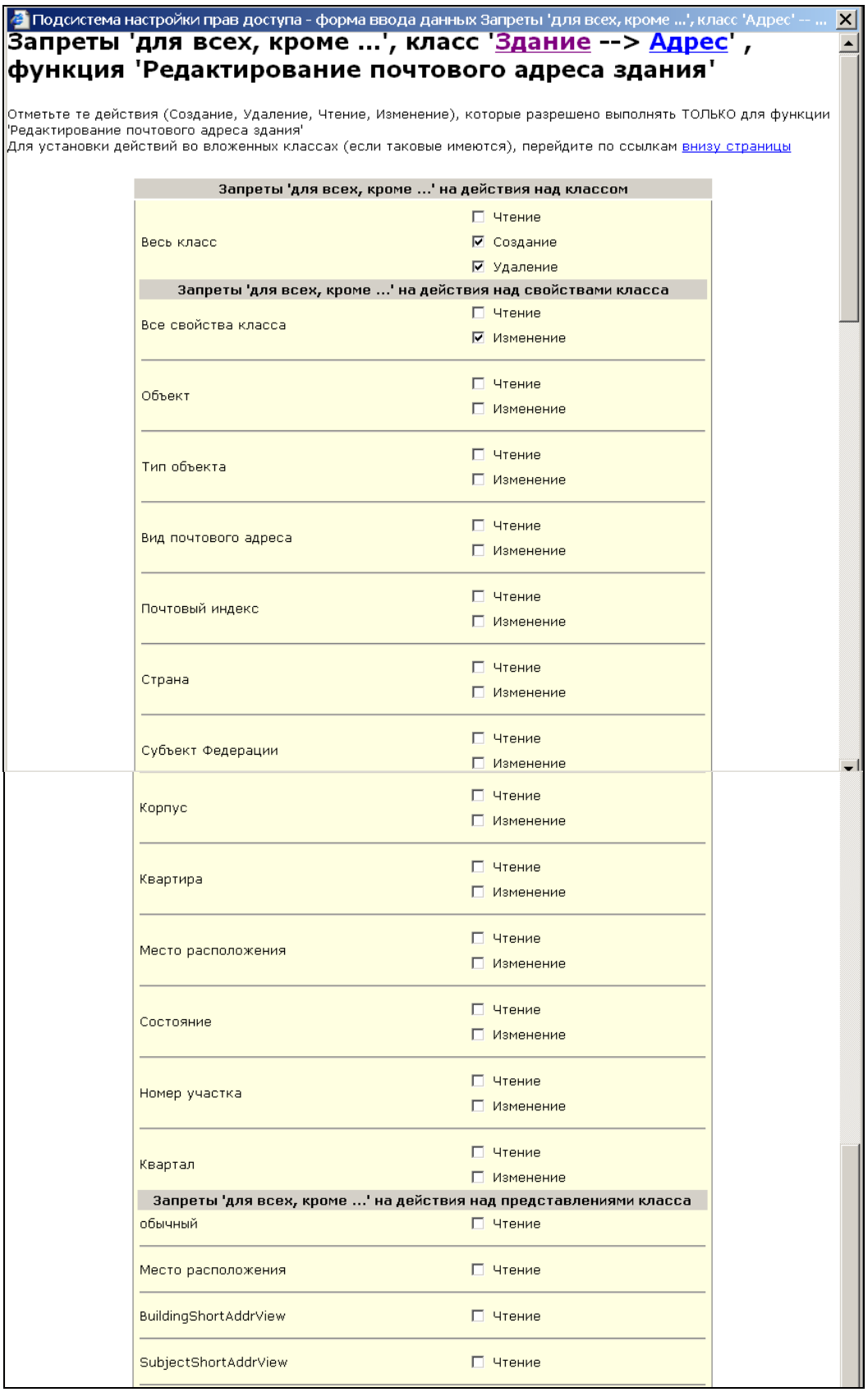


Рисунок 5 - Настройка ограничения прав пользователя

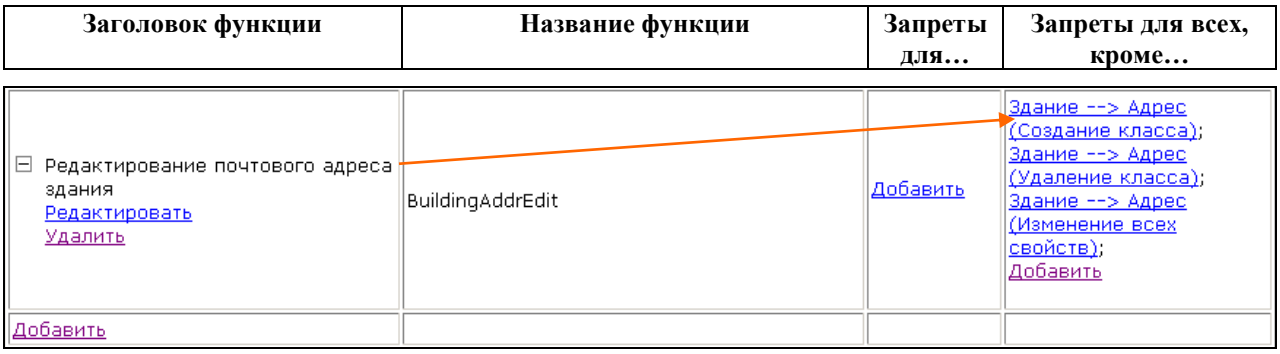


Рисунок 6 - Новая функция с ограничением прав доступа

Шаг 2. Определение рабочего место пользователя

Рабочее место пользователя – это определенная роль пользователя, обладающая какими-либо функциями по работе в системе.

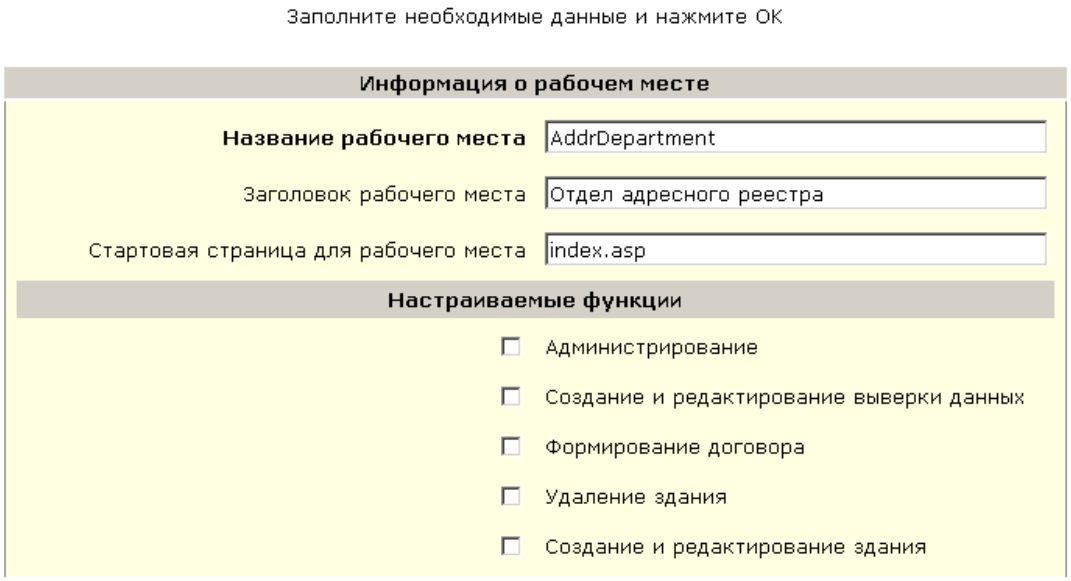
Шаг 2.1 Добавление рабочего места пользователя системы

Для того чтобы наша функция «**Редактирование почтового адреса здания**» выполнялась пользователем, нужно присвоить ее определенному рабочему месту. Поэтому перейдем в секцию «Рабочие места пользователей» и добавим новое рабочее место пользователя - «**Отдел адресного реестра**», как показано на рисунке 7. Здесь вся информация состоит из трех частей:

1) информация о рабочем месте, где присваивается название новому рабочему месту, а также начальная страница;

2) список настраиваемых функций, где Вы помечаете галочкой те функции, которые будет выполнять данное рабочее место;

3) предопределенные функции – функции, которые встроены в систему и их нельзя менять. Далее сохраним изменения, нажав на кнопку «OK».



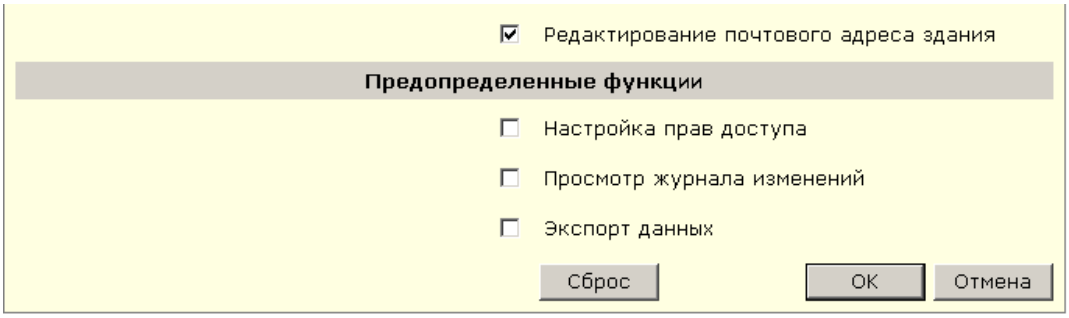


Рисунок 7 - Добавление рабочего места пользователя

В результате пользователи, отнесенные к рабочему месту «**Отдел адресного реестра**» смогут выполнять редактирование адреса. А другим пользователям, отнесенным к рабочим местам без включенной функции «**Редактирование почтового адреса здания**», выполнение этой операции будет запрещено.

Шаг 3. Определение пользователя

Итак, после задания рабочего места пользователя, которое наделено определенными функциями (действиями), необходимо прикрепить его к конкретному пользователю.

Шаг 3.1 Добавление нового пользователя

Добавим нового(ых) пользователя(ей) в систему, и укажем определенный тип рабочего места пользователя (рисунок 8), при этом не забывая сохранять изменения.

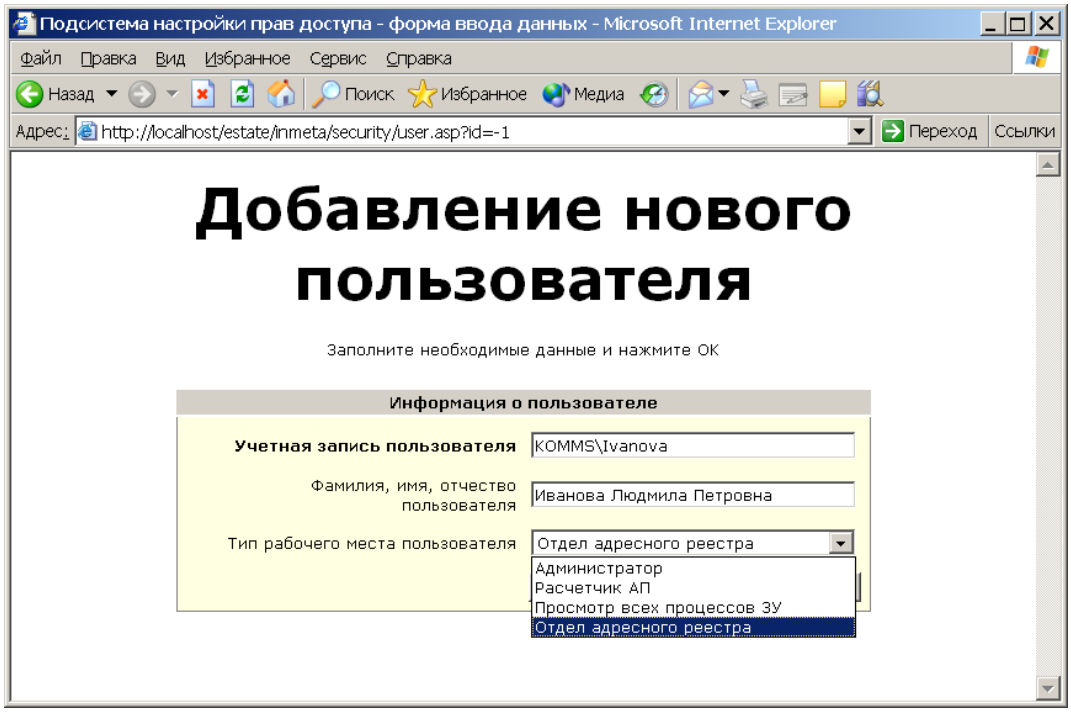


Рисунок 8 - Добавление нового пользователя в систему

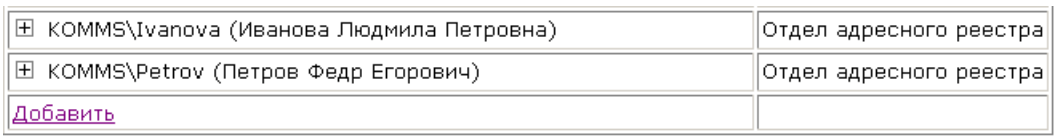


Рисунок 9 - Результат после добавления новых пользователей

Шаг 4. Сохранение информации в подсистеме настройки прав доступа

Все конечные изменения необходимо сохранить на главной странице, **нажав на кнопку «Применить изменения»**.

В результате, мы получили двух пользователей системы, работающих в отделе адресного реестра и обладающих правом на изменение, создание и удаление данных в адресном реестре.

Место хранения информации подсистемы настройки прав доступа

Все настройки прав доступа располагаются в следующих файлах каталога C:\Program Files\Integro\InMeta\<Название приложения>\Meta:

- _denies.xml (запреты для…/ запреты для всех, кроме…)
- _policies.xml (предопределенные функции)
- _roles.xml (настраиваемые функции)
- _ui.xml (рабочие места)
- _users.xml (пользователи)

Для работы подсистемы настройки прав доступа необходимо, чтобы с этих файлов был снят атрибут «Только для чтения» (Read Only).