Информационно-аналитическая система «E5 Управление активами корпорации»

Руководство администратора системы

Раздел: Разграничение доступа

Версия: 2.0
Дата: 02.10.2015

г. Москва

Содержание

Глоссарий

№	Термин	Сокращение	Описание
1.	Доступ		Возможность пользователя работать с данными в базе данных
2.	Карточка		Объединенный набор полей одного или нескольких объектов системы, относящихся к заданной теме. Набор полей карточки может изменяться в зависимости от состояния объектов, роли текущего работника, глобальных настроек системы
3.	Объект		Самостоятельная выделяемая сущность, о которой хранится информация в системе. Например, организация, физическое лицо, документ
4.	Система	Е5 УАК	Информационно-аналитическая система по структуре владения и управления активами корпорации, разрабатываемая на программной платформе Е5 Управление Активами Корпорации (Е5 УАК), представленная в объективной форме Контента, систематизированная с помощью ПО таким образом, чтобы материалы Контента могли быть найдены, обработаны, проставлены логические связи по контуру управления и владения с помощью электронной вычислительной машины (ЭВМ), включающая интеграцию с централизованными корпоративными системами и отчётность
5.	Уведомление		Текстовое сообщение, направляемое работнику Системой в результате события, предусматривающего уведомление
6.		ФЛ	Физическое лицо
7.	Функция системы		Совокупность действий системы, направленная на достижение определенной цели
8.	Организация		Субъект хозяйствования любой формы юридической организации
9.	Работник		Работник организации
10.	Роль		Совокупность технических полномочий, определяющих доступ работника, обладающей данной ролью к объектам и разделам системы

№	Термин	Сокращение	Описание
11.	Поиск		Пользовательское приложение, состоящее из полей и позволяющее с их помощью формировать перечень, удовлетворяющий определенному набору критериев
12.	Экранная форма (экран)		Совокупность элементов интерфейса работника, выводимых на экран одновременно с возможностью просмотра содержимого без дополнительной навигации
13.	Справочник		Набор всех возможных значений поля, хранящийся в системе
14.		ФАС	Федеральная антимонопольная служба
15.	Раздел системы		Искусственно выделенная группа карточек системы, объединенная по признаку принадлежности к бизнес-направлению

Общие сведения

Цель документа

Целью настоящего документа является описание состава и порядка действий администратора Системы при предоставлении пользователям прав доступа к объектам и функциям Системы.

Задачи документа

Для достижения цели, в документе описываются:

- Объекты и функции Системы, являющиеся предметом разграничения доступа;
- Роли пользователей в Системе;
- Порядок разграничения доступа в Системе;
- Порядок действий администратора Системы при предоставлении пользователям прав доступа.

Защищаемые объекты системы

Перечень объектов

Перечень объектов системы, на которые распространяются процедуры разграничения доступа (защищаемые объекты), приведен в таблице 1.

Раздел	Объекты		Доступ
Организации	Карточки	Отчеты	
Физические лица	Карточки		
Заявки			
Справочники	Справочники		
Отчеты	Отчеты		
Журнал изменений			
Уведомления			
Файловое хранилище			Администратор Системы
Пользователи			Администратор Системы
Роли и права			Разработчик Системы

Таблица 1. Защищаемые объекты системы

- Заполненные столбцы «Объекты» означают, что разграничение доступа возможно как целиком, для всех объектов Раздела, так и для отдельных объектов внутри Раздела.
- Если столбцы «Объекты» не заполнены, доступ, или запрет доступа устанавливается только для Раздела в целом.
- Не заполненный столбец «Доступ» означает, что доступ к соответствующим группам объектов, настраиваемый.

Экранная реализация

Разделы и отдельные объекты отражаются в меню Системы (см. рис.1.)

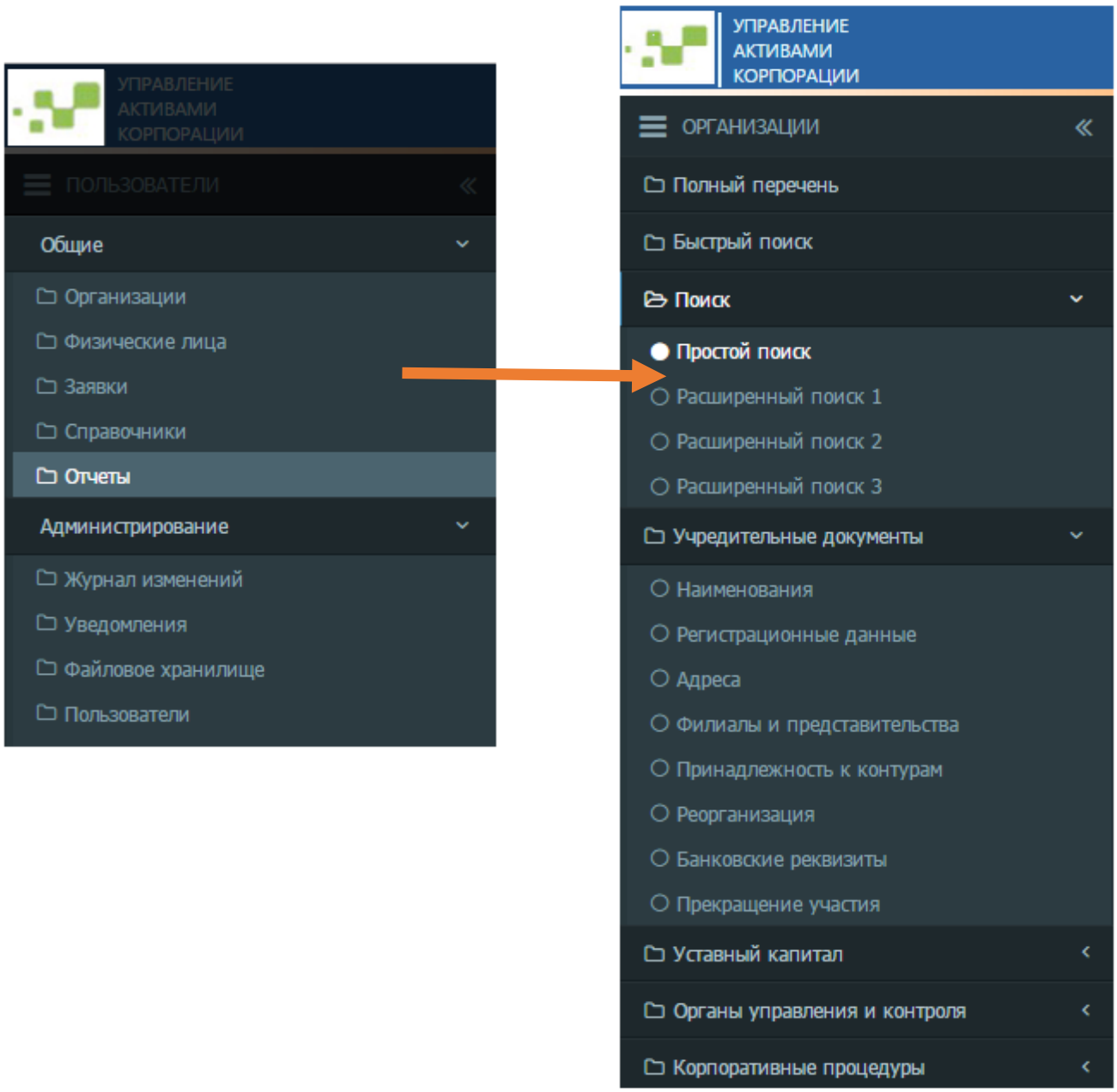

Рис. 1. Меню системы

- Если установлен запрет доступа для всех объектов Раздела, то последний не отображается в меню.
- Если хотя бы один объект Раздела доступен, то в меню отображаются: заголовок Раздела, поисковые разделы, необходимые для корректной работы с объектами, и доступные объекты.
- Объекты, доступ к которым запрещен, в меню не отображаются.

Функции системы

К объектам каждого класса (раздела) защищаемых объектов в Системе применим свой, уникальный набор функций. Матрица функций в разрезе объектов представлена в таблице 2.

Раздел	Объекты	Функции		
		1	**2**	**3**
Организации	Карточки	Просмотр (ПР)	Редактирование (РД)	Администри-рование (АДМ)
Физические лица	Карточки	Просмотр	Редактирование	Администри-рование
Заявки		Просмотр	Утверждение (УТВ)	
Справочники	Справочники	Просмотр	Редактирование	Администри-рование
Отчеты	Отчеты	Просмотр	Формирование	
Журнал изменений		Просмотр		
Уведомления		Просмотр		
Файловое хранилище	Документы	Загрузка (ЗГР)	Выгрузка (ВГР)	Удаление (УДЛ)
Пользователи		Администри-рование пользователей	Администри-рование доступа	

Таблица 2. Матрица функций системы

Подробно функционал технических ролей описан в Приложении 1.

Технические роли Системы

Настройка защиты объектов Системы производится с помощью технических ролей.

Техническая роль состоит из двух сущностей: перечня объектов (см. табл.1), доступ к которым разрешен [1], и функций Системы определенных для каждого объекта представленного в роли (см. Табл.2).

Набор технических ролей формируется разработчиками Системы, является фиксированным и размещается в корпоративной Active Directory. Средства редактирования набора ролей Заказчику не передаются.

Каждая техническая роль уникальным образом именуется в системе. Наименование обычно отражает семантику разграничения – для каких пользователей она предназначена, какие объекты доступны для этой роли и т.д.

Пример перечня технических ролей представлен на рис.2.

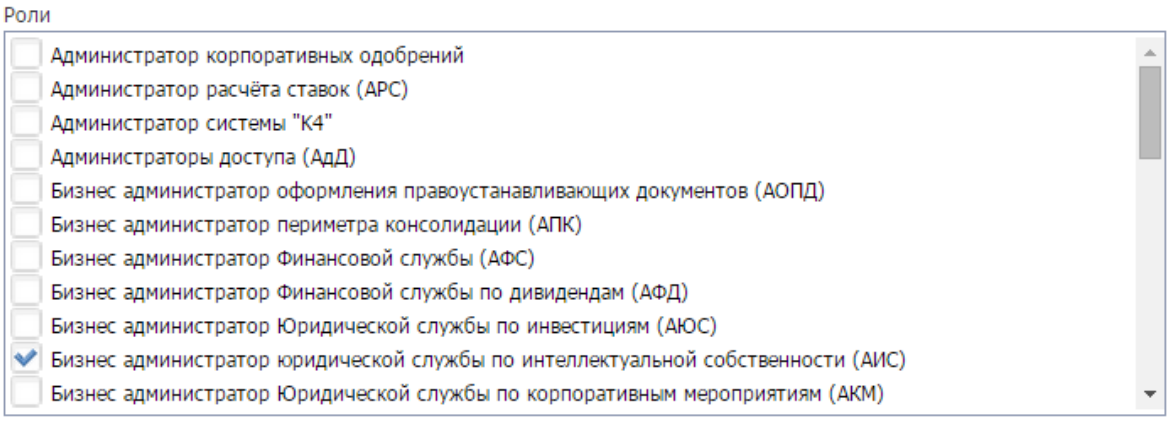

Рис.2. Перечень технических ролей (пример)

В рамках одной роли возможны различные действия с объектами: с одним объектом, только просмотр информации, с другим редактирование данных и т.д. Однако для простоты администрирования рекомендуется устанавливать для одной роли единый функционал.

[1] методом исключения - при создании роли все объекты доступны

Механизм разграничения доступа

Настройка разграничения доступа производится администратором Система в два этапа.

Сначала пользователям присваиваются технические роли, затем определяется перечень организаций, с которыми пользователь имеет право работать.

Определение технических ролей пользователей

При настройке доступа, каждому пользователю (выполняющему на предприятии определенные функциональные обязанности (функциональную роль: бухгалтер, юрист департамента эмиссий, инспектор по кадрам) ставится в соответствие одна или несколько технических ролей. Таким образом пользователь получает доступ к перечисленным в них объектам и определяются возможные действия с ними.

После первоначального добавления пользователя в систему ему не назначена ни одна техническая роль. Также при первоначальном добавлении новой технической роли, она не назначена ни одному пользователю.

Типовая конфигурация технических ролей отражена на рис.3.

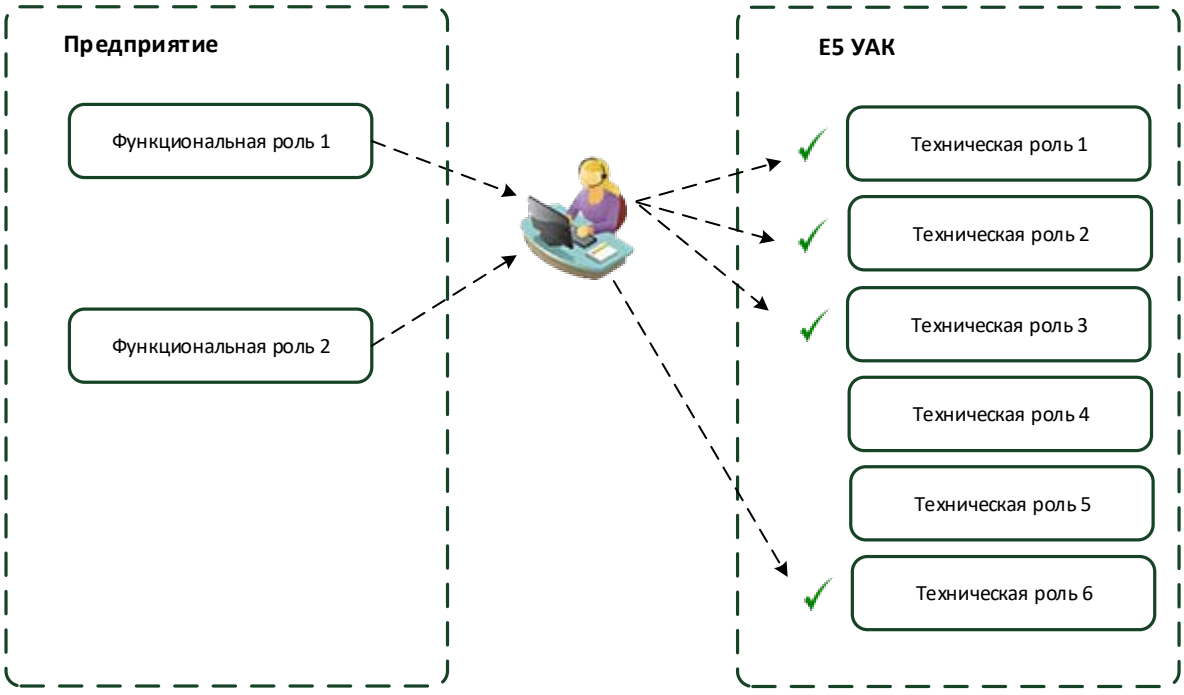

Рис.3.Типовая конфигурация технических ролей

Настройка организационного фильтра

На втором этапе определяется перечень организаций, с которыми имеет право работать пользователь в рамках полномочий, определенных в технических ролях.

Организации предварительно должны быть определены в Системе.

Имеется возможность фильтровать организации по определенным признакам (в частности по принадлежности группам контура управления) и массово снимать или устанавливать работнику доступ ко всем отфильтрованным организациям.

После первоначального добавления работника в систему ему не назначена ни одна организация. Также при первоначальном добавлении новой организации в систему она не назначена ни одному пользователю, но работники, имеющие доступ к системе, видят его в списках организаций.

Итоговая принципиальная схема разграничения доступа для конкретного пользователя отражена на рис.4.

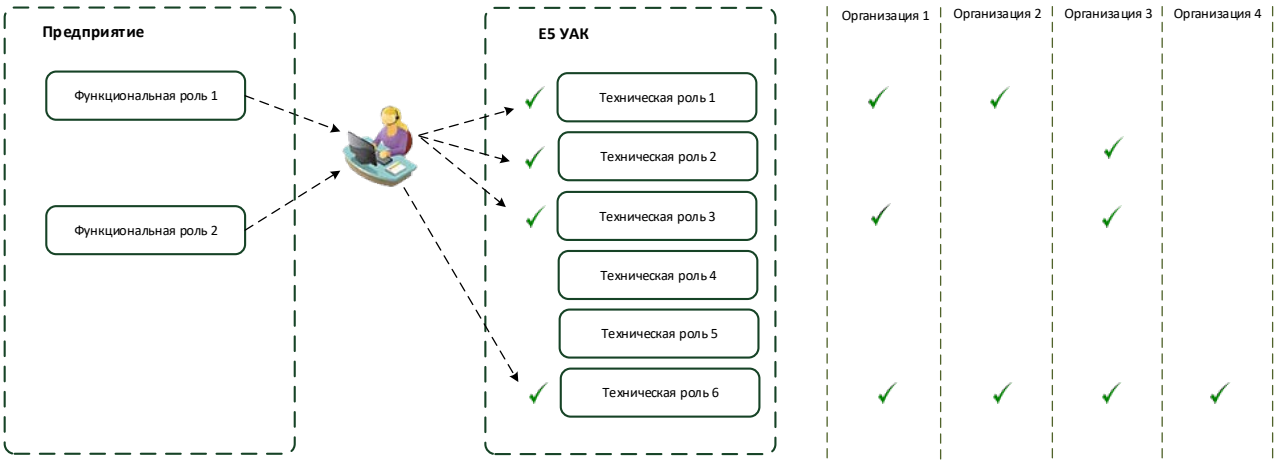

Рис 4. Принципиальная схема разграничения доступа для конкретного пользователя

Управление ролями пользователей в системе

Поиск работников

Работа с правами доступа к различным разделам в системе начинается с поиска работников, в отношении которых будет производится настройка доступа.

Правами на просмотр списков пользователей и на редактирование уровней доступа обладают работники с правами «Администратор системы».

На странице поиска работников находится форма поиска, в которой содержатся:

- поле для ввода ФИО работников;
- список ролей пользователей из ActiveDirectory;
- список доступных групп организаций контура управления.

Работник с ролью Администратор системы может задать условия поиска, используя комбинацию параметров на этой странице.

Если в поле выбран, хотя бы один параметр, то происходит фильтрация по этому полю.

Если параметры поиска не заданы, система выводит список всех работников в системе.

После того, как будут указаны необходимые параметры поиска, работник нажимает на кнопку «Найти». Система выполняет поиск пользователей в папках Active Directory относящихся к системе (см. Рис. 5).

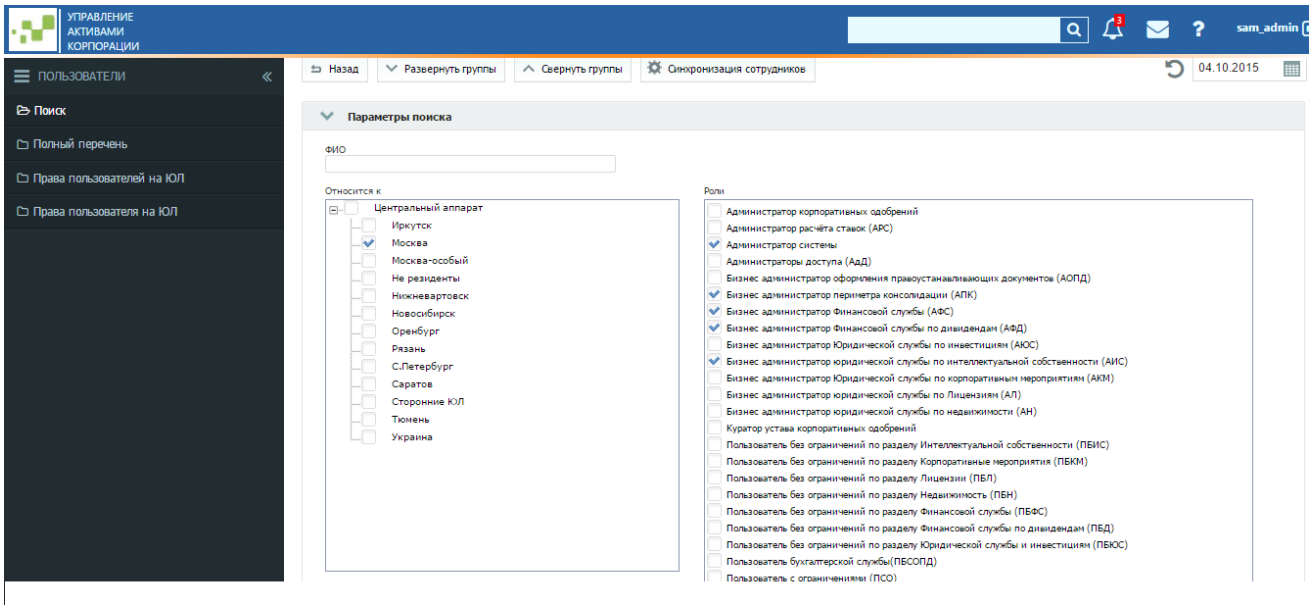

Рис 5. Экран поиска работников

Просмотр списка пользователей системы

На странице просмотра списка пользователей системы указаны условия поиска, который производился, количество пользователей, соответствующих этому запросу (Рис. 6).

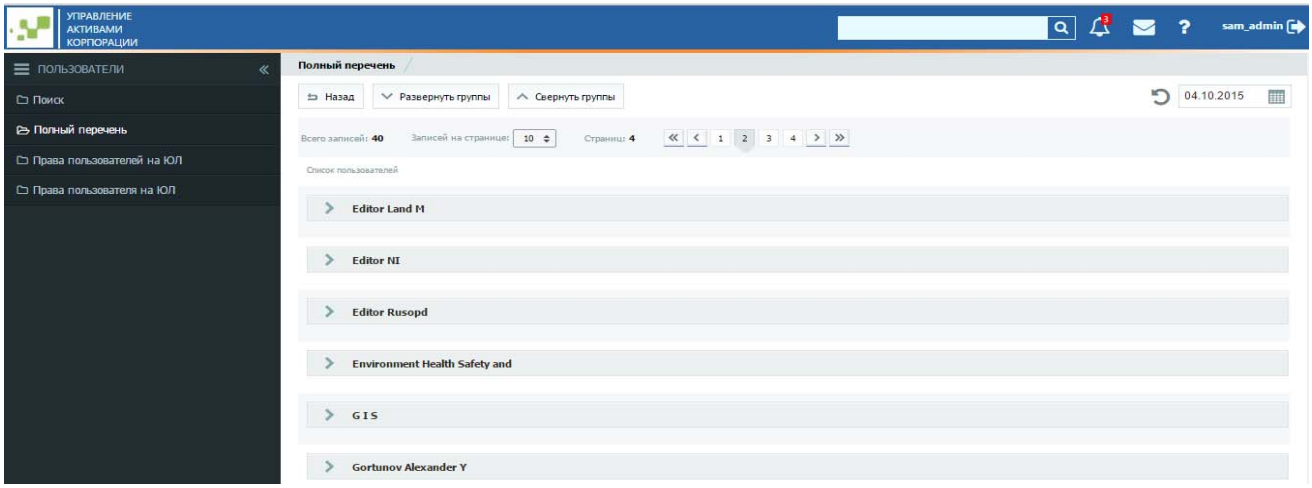

Рис. 6. Просмотр списка пользователей системы

По умолчанию список работников отсортирован по алфавиту.

Существует возможность свернуть все группы на странице, в таком случае на странице останется только список пользователей.

Редактирование прав доступа отдельного пользователя к группе организаций

Для редактирования прав доступа пользователей Администратор системы должен нажать на кнопку «Права пользователя на Организацию». Система откроет страницу, на которой можно отредактировать права доступа одного пользователя к нескольким организациям (Рис. 7).

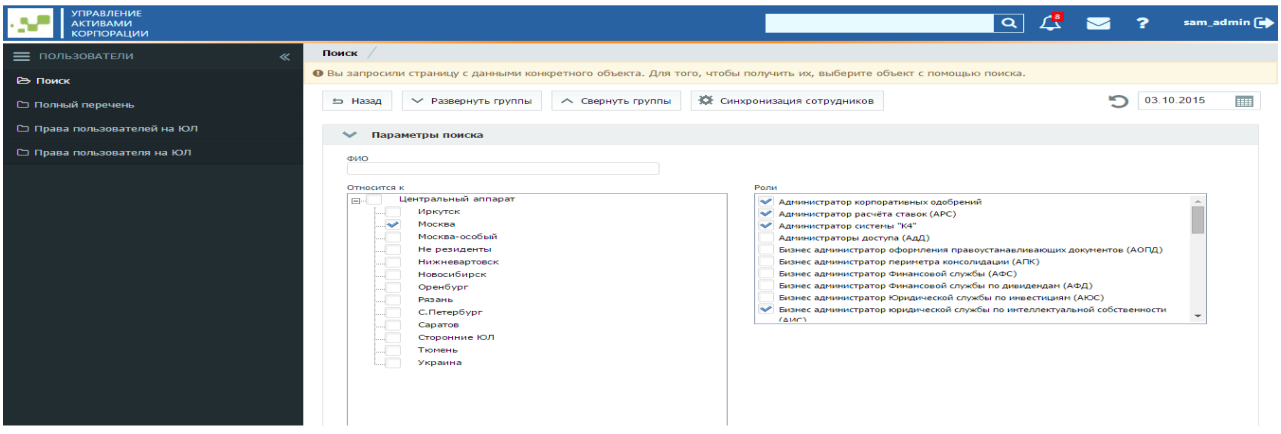

Рис. 7. Экран выбора пользователя.

Редактирование прав доступа происходит следующим образом:

1. Если пользователь известен, в поле <ФИО> указываются его реквизиты и по кнопке <Найти> происходит переход на страницу настройки доступа.

2. Если пользователь не известен, имеется возможность задать контур управления, например, <Москва>, и выбрать технические роли, по которым требуется найти пользователей. После этого система выдаст список пользователей, отвечающих заданным условиям. Выбор конкретного пользователя инициирует страницу настройки доступа (Рис 8).

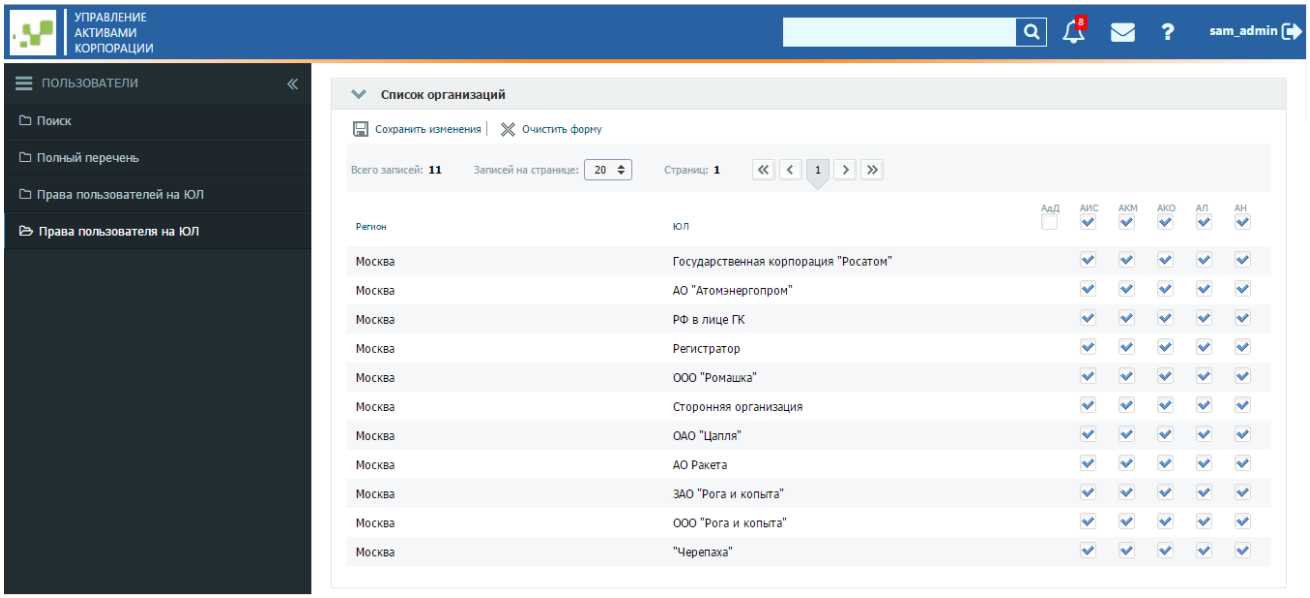

Рис. 8. Изменение организационной привязки.

3. Система отображает таблицу строками, в которой являются выбранные группы контура управления и организации, а в столбцах указаны роли, прописанные работнику в Active Directory, в ячейках таблицы находятся кнопки выбора.

4. Если для некоторых организаций уже были прописаны роли, соответствующая кнопка выбора будет отмечена галочкой.

5. Администратор системы может выбрать организацию, указывая их по одному, либо с помощью заглавной галочки выбора, которая ставит галочки во всех кнопках выбора в столбце на текущей странице.

6. Для того, чтобы удалить доступ к организации, Администратор системы указывает их либо по одному, либо с помощью отмены заглавной галочки выбора, которая убирает галочки во всех кнопках выбора в столбце на текущей странице.

7. Для сохранения изменений Администратор системы должен нажать кнопку «Сохранить изменения».

8. Для отмены действий Администратор системы должен нажать кнопку «Очистить форму». Эта кнопка не удаляет права доступа к организации, которые были назначены до последнего сохранения изменений.

9. Так как в столбцах содержатся аббревиатуры ролей, то для удобства Администратора системы при наведении на заголовок столбца должна выводиться подсказка с расшифровкой сокращения.

Редактирование прав доступа группы пользователей к отдельной организации

Для назначения прав доступа группы пользователей к отдельной организации Администратор системы может воспользоваться формой (Рис. 9).

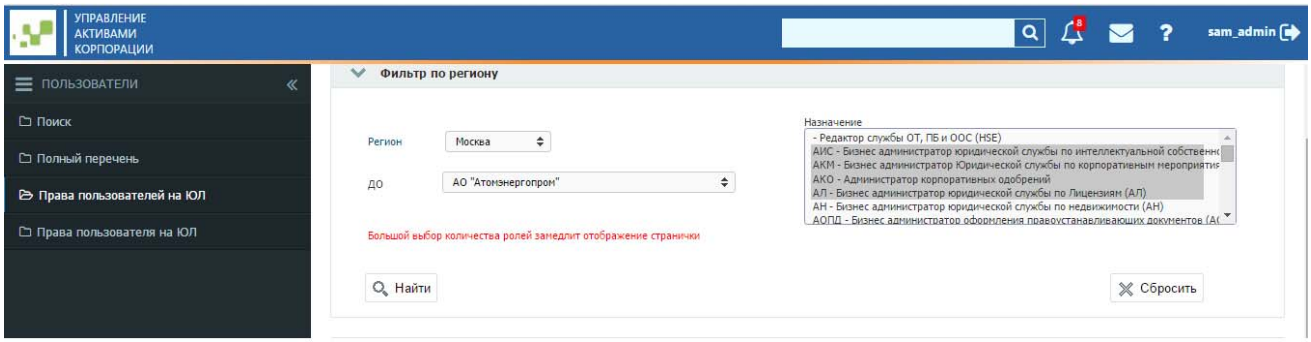

Рис. 9. Добавление прав доступа к обществу

Редактирование прав доступа происходит следующим образом:

1. Выбирается группирующая сущность (например, регион или субхолдинг, проект и т.п.) и организация. В списке технических ролей производится выбор одной или нескольких ролей, по которым будет производится поиск сотрудников. Нажимается кнопка <Найти>.

2. Система отображает таблицу, строками в которой являются Пользователи, в столбцах указаны роли, прописанные пользователям в Active Directory, а в ячейках таблицы находятся кнопки выбора (Рис 10).

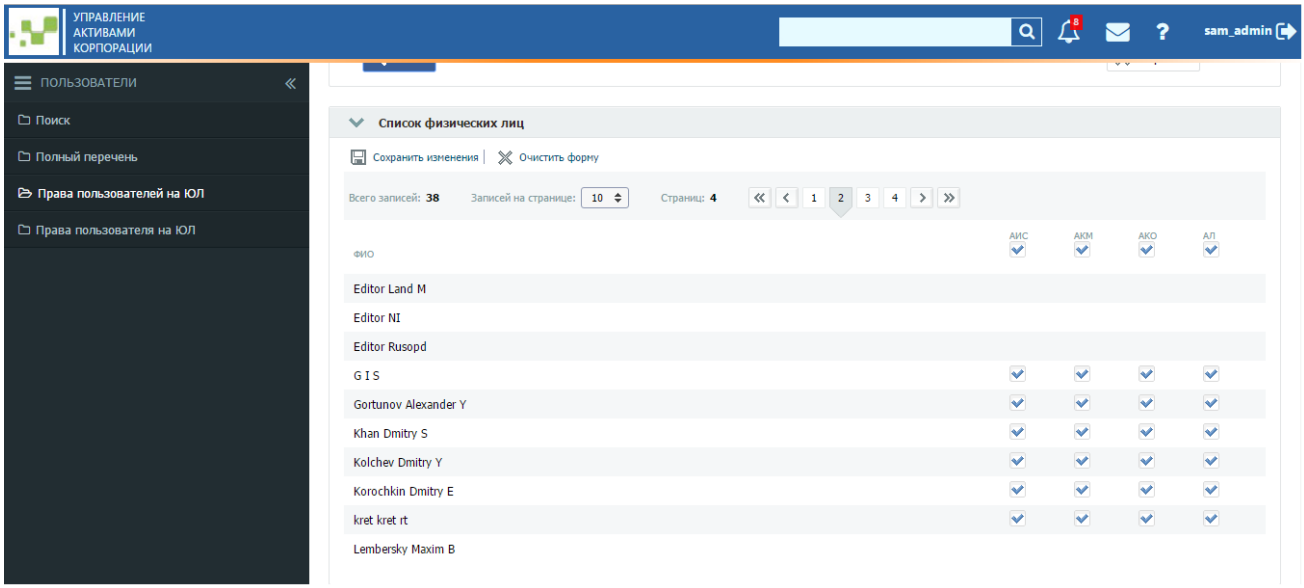

Рис. 10. Экран редактирования ролей группы пользователей

3. Если в выбранной организации пользователю не прописаны роли, кнопка выбора на пересечении строки, соответствующей пользователю и столбца с указанием роли будет неактивной.

4. Если для выбранной организации пользователю уже была прописана роль, соответствующая кнопка выбора будет отмечена галочкой.

5. Администратор доступа может дать пользователю права, указывая роли по одной.

6. Для сохранения изменений Администратор системы должен нажать кнопку «Сохранить изменения».

7. Для отмены действий Администратор системы должен нажать кнопку «Очистить форму». Эта кнопка не удаляет права доступа к организации, которые были назначены до последнего сохранения изменений.

   Так как в столбцах содержатся аббревиатуры ролей, то для удобства Администратора системы при наведении на заголовок столбца должна выводиться подсказка с расшифровкой сокращения.

Приложение 1: Функционал технических ролей

Пользователи с возможностью просмотра данных («Просмотр»)

Технические роли с данным функционалом[2] позволяют просматривать Полный перечень организаций, данных в карточках организаций, Полный перечень физических лиц и данных в карточках физических лиц.

Работнику доступна возможность просмотра и формирования списка отчётов, определенного в технической роли.

Данные, попадающие в отчёт, отображаются пользователю без ограничений. Работнику доступна возможность индивидуальной настройки состава колонок в Полных перечнях и сохранения данных из списков во внешние файлы Microsoft Excel.

Работник имеет возможность скачать прикреплённые файлы документов по доступным ему разделам.

Пользователи с возможностью редактирования данных («Редактор»)

Технические роли с данным функционалом имеют те же права, что и «Просмотр». Кроме того, редактору доступна возможность создания заявок на изменение данных карточек организаций и физических лиц, в рамках ролей, назначенных ему Администратором системы.

Разделы и карточки организаций, а также физических лиц, по которым редактор может создать заявку на изменение, ограничены его технической ролью. Редактор может создавать заявки на внесение либо изменение данных по доступным ему разделам. Редактор может просматривать текущее состояние созданных им заявок в разделе системы «Заявки».

Список организаций доступных редактору для редактирования ограничен назначенным ему перечнем организаций, которые указываются Администратором системы в рамках ролей пользователя.

Доступна возможность создания заявок на изменение данных общих справочников системы. Заявки направляются на утверждение работнику с ролью «Бизнес администратор».

[2] Далее по тексту допускаются такие конструкции как <роль “Редактор»>, <Редактор>, <Бизнес администратор> и т.п.. Это означает - техническая роль с функционалом «Редактор», «Бизнес администратор» и т.д..

Пользователи с возможностью редактирования и утверждения данных («Бизнес администраторы»)

Бизнес администратор имеет все права функционала «Просмотр».

Бизнес администратор может редактировать данные разделов доступных для функционала «Редактор» по схеме одношагового согласования. Такие заявки утверждаются сразу и вступают в силу после нажатия работником соответствующей кнопки.

Работник с данной ролью получает уведомления о заявках, созданных редакторами тех же разделов. Уведомления отображаются в интерфейсе системы и присылаются работнику посредством электронной почты (в случае указания соответствующей настройки в правиле уведомления).

Работнику с данной ролью, которому назначены организации, отправляются уведомления о создании заявки на изменение по этим организациям.

Работник с данной ролью может утвердить либо отклонить заявку, созданную по его разделу в рамках, относящихся к назначенным ему организациям.

Бизнес администратор может просматривать статус, утверждать либо отклонять заявки, созданные Редакторами тех же разделов системы.

Ему также доступен инструмент конструирования форм отчётов (Microsoft Reporting Service). Созданные работником формы отчётов, могут использоваться для формирования отчётов пользователями системы с соответствующими полномочиями.

Пользователи с возможностью изменения привязки к организационной структуре («Администратор системы(АС)»)

Администратор системы имеет возможность управлять доступом работников с группами технических ролей «редактор», «пользователь с правами на просмотр», и «бизнес администратор» к редактированию определённых организаций. Администратор системы может управлять доступом всех работников всех разделов с ролью «редактор», «пользователь с правами на просмотр» и «бизнес администратор» ко всем организациям.

Работник с данной ролью имеет возможность настраивать правила генерации уведомлений.

Работник с ролью Администратор системы имеет доступ к справочникам системы, в которые он может добавлять или удалять значения.

Также Администратор системы может читать служебные уведомления системы и журналы системных событий.

Никаких других функций в системе Администратору системы не предоставляется.

Управление доступом работников к организациям осуществляется посредством указания в интерфейсе системы списка организаций для выбранного работника либо указания в интерфейсе системы списка работников для выбранной организации. Одновременно для работника из списка можно выбрать несколько ролей (из назначенных ему) к каждой организации. Предусматриваются возможности фильтрации и массового проставления пометок для отфильтрованных работников.