УТВЕРЖДАЮ

_____

_____

_____

_____

«_____» _____ 2016

Информационная система дистанционного обучения «Тренинг-Сфера»

Руководство администратора

2016

Содержание

1. Цели документа 6

2. Общие положения 7

2.1. Назначение Системы 7

2.2. Принципы построения системы 7

3. Описание основных решений 9

3.1. Решения по архитектуре Системы 9

3.1.1. Серверные части Системы 9

3.1.2. Клиентские части Система 9

3.1.3. Выбор программного обеспечения 9

4. Описание решений по информационной безопасности 11

4.1. Общие положения 11

4.2. Обеспечение требований к подсистеме управления доступом 13

4.2.1. Аутентификация пользователей посредством протокола LDAP 13

4.2.2. Аутентификация пользователей посредством протокола SPNEGO 14

4.2.3. Авторизация доступа пользователей к объектам доступа 16

5. Условия выполнения программы 17

5.1. Требования к спецификации оборудования 17

5.2. Требования к каналам связи 17

6. Установка системы из дистрибутива 18

6.1. Установка серверной части Система 18

7. Проектное решение по формированию ролей и полномочий 20

7.1. Назначение проектного решения 20

7.2. Права доступа к объектам системы дистанционного обучения 20

7.3. Типовая структура ролей 20

7.3.1. Технические роли 20

7.3.2. Функциональные роли 21

7.4. Группы пользователей. 21

7.5. Разграничение прав доступа пользователей системы к объектам системы 22
7.6. Предоставление прав доступа пользователям. 22
8. Руководство администратора системы 23
8.1. Назначение раздела 23
8.2. Запуск системы и идентификация администратора в системе 23
8.3. Права и обязанности администратора в системе 23
8.3.1. Работа с ролями 23
8.3.2. Организация групп пользователей 31
8.3.3. Привязка ролей к группам пользователей 35
8.3.4. Определение состава пользователей в той или иной группе 36
8.3.5. Привязка ролей к отдельным пользователям 43
8.3.6. Особенности создания ролей для разграничения прав доступа к папкам, подпапкам документов или отдельным документам 46
8.3.7. Настройка уровней показа оргструктуры. 47
Приложение 1. Права доступа в разрезе объектов 48
Приложение 2. Структура функциональных ролей 56
Приложение 3. Группы исполнителей 66

Перечень используемых терминов

Термин	Значение термина
ECM (Enterprise Content Management)	Информационная система или компьютерная программа, предназначенная для организации совместного процесса создания, редактирования и управления контентом (содержимым).
Портал	Совокупность взаимосвязанных непосредственно аппаратных средств и веб - интерфейсов для доступа сотрудников к корпоративным данным и приложениям, выполненная с возможностью обработки указанной информации с последующим предоставлением ее результатов.
Электронная библиотека	Упорядоченная коллекция разнородного электронного контента (текстового, графического, звукового, видео и т. п.), снабженная средствами пополнения, навигации, поиска и предоставления информации.
Права доступа	Совокупность разрешений и запретов на какие-либо действия.
Роли	Определяют набор прав доступа к объектам портала

Перечень используемых сокращений

Сокращение	Расшифровка сокращения
АС	Автоматизированная система
КХД	Корпоративное хранилище данных
ИБ	Информационная безопасность
ИС	Информационная система
ПО	Программное обеспечение
ПС	Портальные сервисы
СУБД	Система управления базами данных

1. Цели документа

В данном документе приведена техническая информация об администрировании Информационной системы дистанционного обучения «Тренинг-Сфера», далее Система.

Данный документ предназначен для технического персонала, осуществляющего администрирование и сопровождение Системы.

Целью создания данного документа является предоставлении группе сопровождения документации по администрированию Системы.

2. Общие положения

2.1. Назначение Системы

Основными задачами Системы, являются автоматизация образовательных процессов внутри организации, в частности:

- формирование поэтапных процессов обучения в виде совокупности курсов и разделов;
- контроль результатов обучения, а также сроков сдачи заданий и тестов;
- формирование мультимедийной среды обучения (видеоконференции, вэбинары, чаты и т.д.);
- создание обратной связи между обучающимися и преподавателями;
- сокращение временных и материальных затрат на создание и контроль образовательных процессов

2.2. Принципы построения системы

Система построена на свободном программном обеспечении с открытым кодом с применением всех современных промышленных стандартов, что что дает следующие преимущества:

- **Кросс-платформенность**. Система может эксплуатироваться на различных ОС и СУБД;
- **Импортонезависимость.** Конфигурация Системы построена на базе проектов свободного программного обеспечения и собственных разработок;
- **Минимизация рисков**. Переход к использованию российских разработок и свободному программному обеспечению снижает риски от использования зарубежного лицензионного ПО и позволяет защититься от непредсказуемой технологической, лицензионной и ценовой политики западных поставщиков;
- **Сокращение расходов**. Применяемое свободное программное обеспечение поставляется по открытой лицензии, что позволяет сократить затраты на этапе внедрения и увеличивать количество рабочих мест, не неся лицензионных расходов.

Особое внимание при разработке Системы уделялось требованиям информационной безопасности.

Система прошла сертификационные испытания на соответствие требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999 год) по классу защищенности 1Г, более того, в данный момент идет работа по подготовке Системы для прохождения сертификации на соответствие требованиям защиты информации вплоть до класса защищенности 1Б, что позволяет ей обрабатывать секретную информацию, включая уровень «Совершенно секретно».

Архитектура Системы включает серверную часть, которая исполняется под управлением Unix-подобных операционных систем или операционной системы Microsoft Windows, а также клиентские части, которые представляют собой веб-браузеры, способные работать на различных операционных системах, а также на мобильных платформах.

3. Описание основных решений

3.1. Решения по архитектуре Системы

3.1.1. Серверные части Системы

В силу того, что Система разработана с помощью портальных веб–технологий, она, по сути, полностью является серверной системой. Вся ее функциональность реализована в модулях, являющихся теми или иными серверами. Система представляет собой взаимодействие таких серверных служб как СУБД PostgreSQL, сервер приложений Glassfish, система управления порталами Liferay.

СУБД PostgreSQL предназначена для хранения в своих БД данных всех подсистем, входящих в Система, оперативного снабжения данными этих подсистем и информационного взаимодействия между ними.

Сервер приложений Glassfish OSE является платформой для разворачивания на ней различных сервисов, подсистем и модулей Система. Glassfish, поддерживая модульную и расширяемую архитектуру, кластеризацию, а также имея отличные надежность и производительность, является гибким и удобным инструментом для обеспечения всех требований Система.

Система управления порталом Liferay Portal Community Edition, развернутая на платформе Glassfish, поддерживает такие промышленные стандарты как JSR 170, JSR 286, JSR 168. Этот продукт обеспечивает большую часть функциональности Системы.

3.1.2. Клиентские части Система

В качестве клиентских приложений Системы используются web-браузеры (Microsoft Internet Explorer версии не менее 9, Mozilla Firefox версии не менее 14.0, Google Chrome версии не менее 10.0.648).

3.1.3. Выбор программного обеспечения

Система разработана на основе программного обеспечения с открытым исходным кодом. В качестве базового ПО использовано:

- Сервер приложений Glassfish Server OSE 3.1.2.2.,
- Система управления порталом Liferay Portal Community Edition, версия 6.2 GA3,
- Система управления базами данных PostgreSQL версия 9,

Для реализации необходимой функциональности, которая отсутствует в вышеуказанных продуктах, собственными силами были разработаны отдельные части и модули подсистем на языке JAVA с помощью пакета OpenJDK версии 1.6.

Система поддерживает следующие требования:

- Система не имеет привязку к конкретному операционному окружению, напротив, поддерживаются многоплатформенность и гетерогенная сетевая среда.
- Система опирается на открытые индустриальные стандарты, поддерживаемые широким кругом производителей.
- Поддерживается сквозная аутентификация пользователей на базе информации о текущем сеансе.
- Поддерживается использование XML – представления объектных данных и XSL – технологии совместно с механизмом XSLT – преобразований.
- Поддерживается масштабируемость – обеспечение масштабируемости по количеству пользователей, объему хранимых данных, интенсивности обмена данными, скорости обработки запросов и данных, набору предоставляемых услуг, способам обеспечения доступа.
- Поддерживается возможность настройки – Система имеет возможность настройки без модификации кода модулей при изменении внешней среды и конкретных задач пользователя.

В качестве клиентских приложений Системы используются web-браузеры (Microsoft Internet Explorer версии не менее 9, Mozilla Firefox версии не менее 14.0, Google Chrome версии не менее 10.0.648).

4. Описание решений по информационной безопасности

4.1. Общие положения

Назначение любой подсистемы безопасности состоит в разграничении доступа к составляющим системы, подлежащих защите. Поставленную задачу можно разделить на две составляющие:

1. Проверка подлинности предоставленных пользователем системы учётных данных (процесс аутентификации).
2. Предоставление доступа к ресурсам системы в соответствии с назначенными пользователю полномочиями (процесс авторизации).

Решение указанных задач в части автоматизированных систем (АС) регламентируется РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации», Гостехкомиссия России, 1992 г.

Функциональной средой Системы является ЗОС «Astra Linux Special Edition 1.3» (ALSE). Для управления пользователями в рамках ОС Windows используется служба Active Directory (AD). Служба AD представляет собой надстройку над технологиями LDAP, Kerberos и NTLM и обеспечивает автоматическую настройку всех необходимых файлов конфигурации служб, реализующих перечисленные технологии, а также предоставляет интерфейс управления и администрирования.

Kerberos является протоколом, обеспечивающим централизованную идентификацию пользователей и применяющим техническое маскирование данных для противодействия различным видам атак.

Основным компонентом системы Kerberos является центр распределения ключей (KDC). KDC отвечает за аутентификацию в некоторой области Kerberos. В процессе своей работы система Kerberos выдаёт билеты (tickets, TGT) на использование различных служб.

Сервером Kerberos называется ЭВМ, на которой выполняется серверная программа Kerberos, или сама программа KDC. Клиент Kerberos – это ЭВМ или программа, которые получают билет от сервера Kerberos. Обычно действия системы Kerberos инициирует пользователь, отправляющий запрос на получение услуг от некоторого сервера приложений (например, сервера почты). Kerberos предоставляет билеты принципалам, в роли которых выступают пользователи или серверные программы.

Технология Kerberos предоставляет собой механизм аутентификации пользователей и сервисов, основным достоинством которой является повышенная защищённость при использовании в сети, достигаемая механизмом защищённого обмена билетами между пользователями, сервисами и сервером учётных записей Kerberos. При данном механизме пароли пользователей по сети не передаются, что обеспечивает повышенную защищённость от сетевых атак. С помощью механизма открытых и закрытых ключей, а также синхронизации часов клиентских ПЭВМ с сервером Kerberos, обеспечивается уникальность билетов и их защищённость от подделки.

LDAP – это протокол, используемый для доступа к информации, хранящейся на распределённых в сети серверах. Указанная информация представляет собой данные, хранящиеся в атрибутах. При этом предполагается, что такие данные чаще читаются, чем модифицируются. LDAP основан на модели взаимодействия «клиент-сервер». Общая модель данного протокола состоит в том, что клиент выполняет операции протокола на серверах. Клиент передаёт запрос, описывающий операцию, которая должна быть выполнена сервером. Сервер выполняет необходимые операции в каталоге. После завершения операции сервер возвращает клиенту ответ, содержащий результат выполнения операции или ошибку. Информация на сервере LDAP представляет собой совокупность записей, которые содержат набор атрибутов и сгруппированы в древовидную иерархическую структуру.

Записи идентифицируются глобально уникальным именем (DN) подобно имени домена в структуре DNS. Каталог является специализированной БД, которая может использоваться в современной жизни – телефонная книга, программа передач и тому подобное. Предполагается, что данные каталога в достаточной мере статичны. Классическим примером подобной специализированной БД является сервис DNS.

NTLM представляет собой протокол сетевой аутентификации, разработанный фирмой Microsoft для линейки своих операционных систем Windows NT.

В качестве защищённой СУБД в составе ЗОС «Astra Linux Special Edition 1.3» (ALSE) используется PostgreSQL, доработанная в соответствии с требованием интеграции с ALSE в части мандатного разграничения доступа к информации.

Для аутентификации пользователей Система использует подключение к LDAP-каталогу от имени настраиваемого технологического пользователя AD.

Работа в едином пространстве пользователя (ЕПП) основана на использовании механизма SPNEGO, применяемого для аутентификации клиентского приложения на удалённом сервере в том случае, если ни одна из сторон не знает, какой протокол аутентификации поддерживает другая сторона. В процессе согласования протокола аутентификации производится выбор конкретного

механизма GSSAPI, используемого в последующем при проведении процедуры подтверждения подлинности пользователя.

GSSAPI представляет собой программный интерфейс для доступа к сервисам безопасности. Виртуальная машина Java, входящая в состав ЗОС «Astra Linux Special Edition 1.3», включает в свой состав реализацию данного программного интерфейса, позволяющего произвести аутентификацию пользователя Системы при помощи протокола Kerberos.

4.2. Обеспечение требований к подсистеме управления доступом

4.2.1. Аутентификация пользователей посредством протокола LDAP

Доступ к сервисам и данным Системы осуществляется на основе учётных данных пользователей, содержащихся в AD.

Схема подтверждения подлинности пользователей Система, при протоколе LDAP, приведена на рисунке 2. При этом следует учесть, что обмен данными между клиентской и серверной частями Системы осуществляется с использованием протокола HTTPS. HTTPS представляет собой расширение протокола передачи данных HTTP, поддерживающее шифрование.

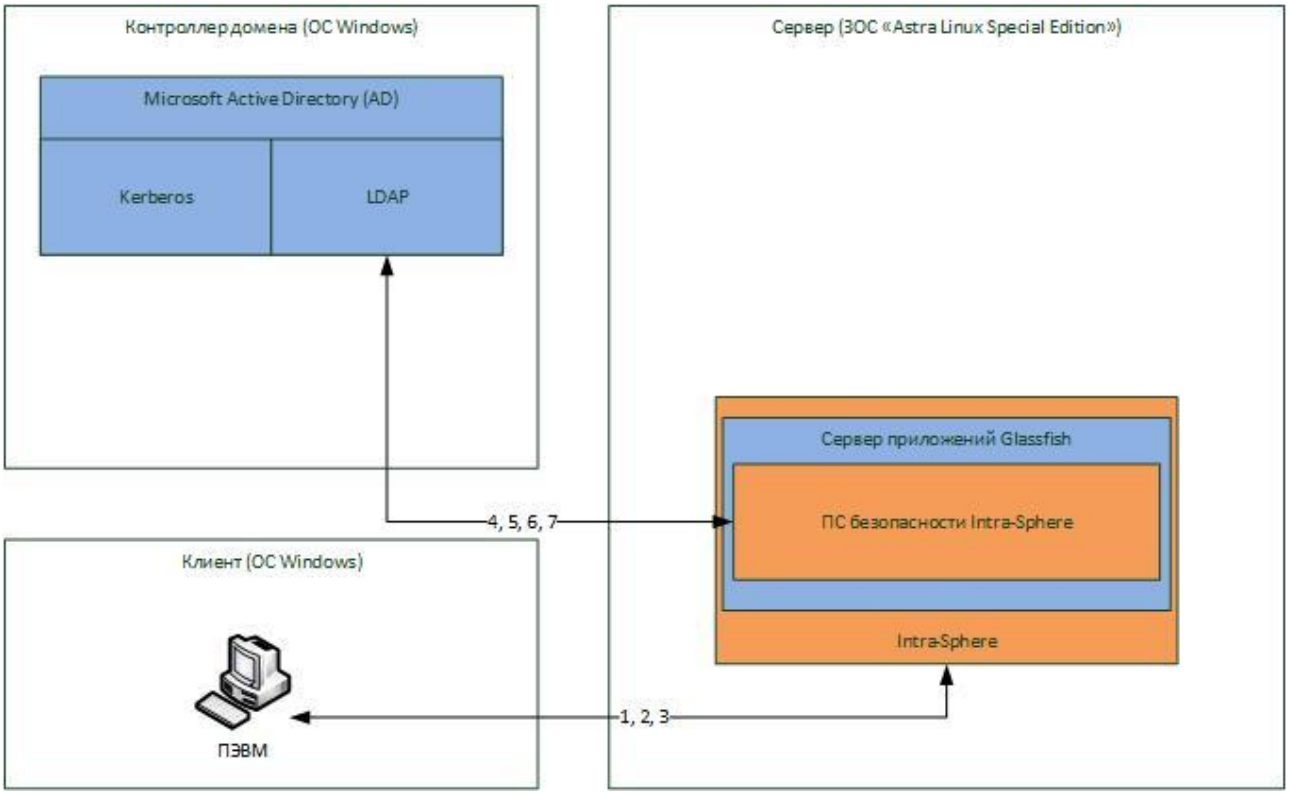

Рисунок 2. Схема аутентификации пользователя Системы посредством протокола LDAP (ввода учётных данных).

Полная последовательность действий в рассматриваемом случае подразделяется на следующие этапы:

1. интернет-навигатор ПЭВМ пользователя запрашивает обслуживание у Система;
2. в ответ Система предлагает ввести пользователю свои учётные данные;
3. по окончании ввода пользователем учётных данных, интернет-навигатор передаёт полученные данные Система;
4. Система передаёт от имени технологического пользователя серверу LDAP AD учётные данные пользователя для проведения процедуры идентификации;
5. в случае успешного завершения процедуры идентификации, Система осуществляет поиск уникального имени (DN) в дереве LDAP AD;
6. в случае успешного выполнения пункта 5, Система осуществляет попытку подключения от имени пользователя к серверу LDAP AD;
7. в случае успешного выполнения пункта 6, Система осуществляет выгрузку из дерева LDAP AD перечня групп, в которых состоит пользователь, используемый в дальнейшем для проверки прав доступа к объектам Система.

4.2.2. Аутентификация пользователей посредством протокола SPNEGO

Система позволяет организовать работу в ЕПП. Схема аутентификации пользователей, в рассматриваемом случае, представлена на рисунке 3. В этом случае, как и ранее, обмен данными между клиентской и серверной частями Системы осуществляется с использованием протокола HTTPS.

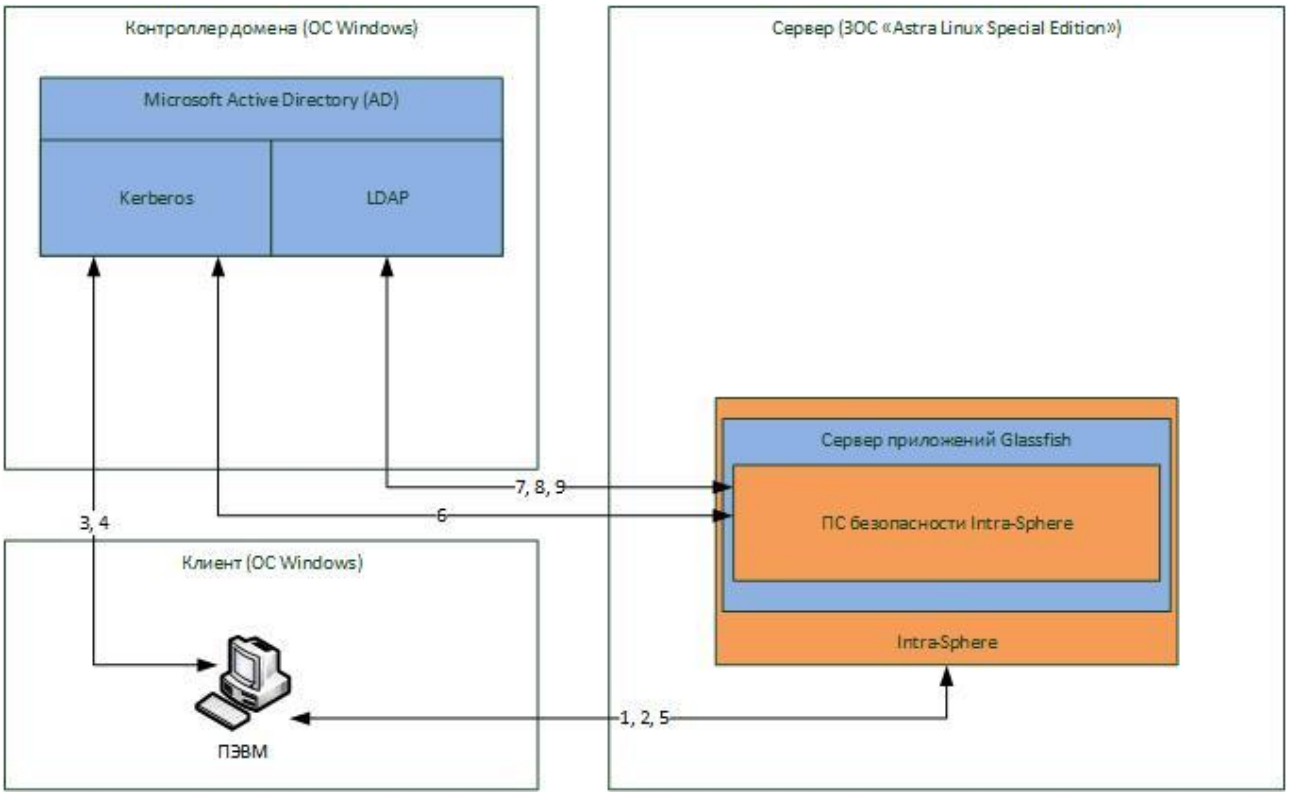

Рисунок 3. Схема аутентификации пользователя Системы посредством протокола SPNEGO.

Последовательность действий, выполняемых при аутентификации пользователя, примет следующий вид:

1. интернет-навигатор ПЭВМ пользователя Системы запрашивает обслуживание у Система;
2. в ответ Система, используя протокол SPNEGO, высылает требование провести идентификацию посредством механизма Kerberos;
3. интернет-навигатор ПЭВМ пользователя Системы передаёт серверу Kerberos AD учётные данные пользователя для проведения процедуры идентификации;
4. в случае успешного завершения процедуры идентификации сервер Kerberos AD возвращает билет (TGT) на использование служб, входящих в состав ОС Windows;
5. интернет-навигатор заново запрашивает обслуживание у Система, используя протокол SPNEGO и прикладывая к запросу полученный TGT;
6. Система, при помощи механизма GSSAPI для протокола Kerberos, проверяет корректность принятого билета;
7. в случае успешного завершения пункта 6, Система осуществляет поиск уникального имени (DN) в дереве LDAP AD;

8. в случае успешного выполнения пункта 7, Система осуществляет попытку подключения от имени пользователя к серверу LDAP AD;
9. в случае успешного выполнения пункта 8, Система осуществляет выгрузку из дерева LDAP AD перечня групп, в которых состоит пользователь, используемый в дальнейшем для проверки прав доступа к объектам Система;
10. обеспечивает доступ Система к внутренним сервисам Система и данным КХД.

4.2.3. Авторизация доступа пользователей к объектам доступа

Информация объектов доступа Системы хранится в БД под управлением СУБД PostgreSQL, входящей в состав ЗОС «Astra Linux Special Edition 1.3». Система осуществляет взаимодействие с указанной БД от имени технологического пользователя. Функции разграничение доступа субъектов Система к объектам системы возложены на подсистему безопасности Системы. Проектное решение по разграничению доступа на основе ролей и полномочий, приведено в пункте 7. «Права доступа к объектам Система» настоящего документа.

5. Условия выполнения программы

5.1. Требования к спецификации оборудования

Поскольку работа Пользователей с Системой предусматривается в режиме веб-доступа с использованием стандартных браузеров Internet Explorer, Mozilla Firefox и Google Chrome, ресурсы используемых ими компьютеров должны обеспечивать эффективную работу с данными приложениями.

5.2. Требования к каналам связи

Для обеспечения комфортной работы с Система, подсистемы, обеспечивающие связь серверов Системы с АРМ пользователей должны обладать скоростью передачи, достаточной для комфортной работы в веб-браузере с цветной графической информацией высокого качества, а также для связи с удаленными серверами интеграции (ориентировочно от 100 Мбит/с).

6. Установка системы из дистрибутива

6.1. Установка серверной части Система

Серверные части Системы устанавливается на компьютер, с предустановленной операционной системой Linux, также, на этот же компьютер, или на другой, доступный по сети, должна быть установлена СУБД PostgreSQL.

1. На компьютере, на который будет устанавливаться серверная часть Системы, должны быть установлены следующие необходимые для успешного функционирования Системы пакеты:

- openjdk-6-jdk
- zip
- imagemagick
- libpostgresql-jdbc-java

2. В СУБД PostgreSQL создать новую роль «portal» с привилегиями «SUPERUSER», «CREATEDB», «CREATEROLE» и новые базы данных «sdobase» и «khdbase» с владельцем «portal» с помощью следующих команд:

- CREATE USER portal PASSWORD SUPERUSER CREATEROLE CREATEDB;
- CREATE DATABASE sdobase WITH OWNER=portal;
- CREATE DATABASE khdbase WITH OWNER=portal;

3. С помощью команды adduser создать нового пользователя portal.
4. Создать директорию /home/portal/sdo и перейти в нее.
5. Переписать архив dstr-sdo.tar.gz в директорию /home/portal/sdo и распаковать его
6. Восстановить дампы баз данных Система, выполнив команды:

- psql -U portal -W -d sdobase -h ‘IP_адрес_машины_с_СУБД_PosthreSQL’ -p ‘Порт_PostgreSQL’ -q -f dstr-sdobase_dump
- psql -U portal -W -d khdbase -h ‘IP_адрес_машины_с_СУБД_PosthreSQL’ -p ‘Порт_PostgreSQL’ -q -f dstr-khdbase_dump

7. Оптимизация настроек памяти для JVM

   Для комфортной работы Системы количество оперативной памяти на компьютере не должно быть не меньше 8 ГБ. В этом случае, необходимо провести оптимизацию настроек выделения памяти для JVM.

правка файла /home/portal/sdo/ps/glassfish3/glassfish/domains/pserp/config/domain.xml :
XX:PermSize=512m – минимальный размер области памяти Permanent Generation
XX:MaxPermSize=1024m – максимальный размер области памяти Permanent Generation
Xmx4096m – максимальный размер области памяти HEAP

8. В каталоге /home/portal/sdo/ps/glassfish3/glassfish/domains/pserp/config в файле portal-ext.properties, откорректировать строку с домашним каталогом домена:

   liferay.home=/home/portal/sdo/ps/glassfish3/glassfish/domains/pserp

   а также строки, указывающие на параметры коннекта к БД:

   jdbc.default.password=troP4444

   jdbc.default.username=portal

   jdbc.default.driverClassName=org.postgresql.Driver

   jdbc.default.url=jdbc:postgresql://‘IP_адрес_машины_с_СУБД_PosthreSQL’:‘Порт_PostgreSQL’/sdobase (например, jdbc:postgresql://192.168.0.10:5432/sdobase)

9. Опционально! GlassFish по умолчанию запрещает удаленные подключения к административной консоли домена. Если такие подключения необходимы, то выполнить: /home/portal/sdo/ps/glassfish3/glassfish/bin/*asadmin enable-secure-admin*

10. Запуск домена pserp осуществляется командой:

    /home/portal/sdo/ps/glassfish3/glassfish/bin/asadmin start-domain pserp

11. Остановка домена осуществляется командой:

    /home/portal/sdo/ps/glassfish3/glassfish/bin/asadmin stop-domain pserp

12. Доступ в установленную Систему осуществляется через интернет браузер по адресу «IP-адрес:8080»

7. Проектное решение по формированию ролей и полномочий

7.1. Назначение проектного решения

Данное проектное решение предназначено для описания средств разграничения доступа к объектам системы дистанционного обучения. Кроме того, проектное решение определяет ответственных за создание, наполнение и сопровождение ролей, порядок предоставления доступа.

7.2. Права доступа к объектам системы дистанционного обучения

Каждое действие субъекта с объектом системы определяется его правами доступа. Для функционирования системы рекомендовано использовать для объектов права доступа, приведенные в Приложении 1. Права доступа приведены в разрезе объектов.

7.3. Типовая структура ролей

Для обеспечения удобного и прозрачного разграничения доступа пользователей к объектам системы дистанционного обучения организована следующая структура ролей:

- технические роли;
- функциональные роли.

7.3.1. Технические роли

Технические роли предназначены для настройки системы.

7.3.1.1. Роль «Administrator»

Системы дистанционного обучения поставляется с единственным пользователем «Test», который определяет Администратора системы.

Определение Администратора системы описано в документе «Руководство системного программиста».

Администратору системы доступна вся функциональность системы с возможностью настройки и редактирования.

Администратор осуществляет:

- Ведение оргструктуры и пользователей системы;

- распределение прав доступа к объектам системы по ролям;
- организацию групп пользователей;
- привязку ролей к группам пользователей;
- определение состава пользователей в той или иной группе.

При этом предполагается, что пользователь системы входит в состав одного и только одного структурного подразделения.

7.3.1.2. Роль «PowerUser»

Техническая роль «PowerUser»» присваивается автоматически пользователю системы, при его первоначальной идентификации в системе.

Данная роль позволяет просматривать информацию, доступ к просмотру которой не ограничен дополнительно, т.е. информацию, открытую для всех пользователей системы. Это позволяет уменьшить объем настроек ролей для групп пользователей.

7.3.2. Функциональные роли

Каждой функциональной роли в системе можно присвоить несколько прав доступа для управления объектами .

В Приложении 2 приведен рекомендуемый вариант настройки ролей для успешного функционирования системы.

Добавление/удаление функциональных ролей для работы в системе осуществляется на основании заявок на добавление/удаление ролей. Шаблон заявки представлен в Приложении 5.

7.4. Группы пользователей.

Для облегчения администрирования доступа исполнителей к объектам системы предусмотрена возможность объединения пользователей в группы по профилю их работ. На группу назначается совокупность ролей, которые определяют права доступа всех пользователей, включенных в данную группу. В Приложении 3 приведен возможный перечень групп для пользователей системы.

Добавление/удаление групп пользователей для работы в системе дистанционного обучения осуществляется на основании заявок на добавление/удаление групп пользователей. Шаблон заявки представлен в Приложении 6.

7.5. Разграничение прав доступа пользователей системы к объектам системы

Разграничение прав доступа пользователя системы осуществляется назначением им множества ролей, которые определяют права доступа к тем или иным объектам системы.

Назначение ролей пользователю возможно двумя способами:

- Назначение роли из списка ролей;
- Добавление пользователя в группу пользователей.

При необходимости, одного и того же пользователя можно добавить в несколько групп или добавить ему дополнительные роли из общего перечня ролей.

Доступ пользователя к объектам системы будет определяться совокупностью ролей, назначенных на группы, в которые он входит и дополнительным множеством ролей, назначенных непосредственно данному пользователю.

Пользователи системы, которые не будут включены ни в одну группу пользователей системы, обладающую посредством назначения данной группе ролей, правами доступа к тем или иным объектам системы и на которые не будут назначены роли из общего списка ролей, смогут просмотреть информацию системы общего доступа. Доступ к просмотру информации общего пользования будет определена ролью «PowerUser», которая присваивается автоматически пользователю системы, при его первоначальной идентификации в системе.

7.6. Предоставление прав доступа пользователям.

Предоставление доступа для работы в системе осуществляется на основании заявок на предоставление/изменение прав доступа пользователей. Шаблон заявки представлен в Приложении 4.

8. Руководство администратора системы

8.1. Назначение раздела

Данный раздел предназначен для описания работы Администратора с системой дистанционного обучения.

8.2. Запуск системы и идентификация администратора в системе

Запуск системы дистанционного обучения производится в WEB-браузере по адресу, указанному при установке системы.

Исполнитель, имеющий права на администрирование системы, получает учетную запись Администратора системы и возможность входа в систему с правами администратора. Первоначальное назначение прав доступа для Администратора описано в документе «Руководство системного программиста»

8.3. Права и обязанности администратора в системе

Администратором системы должен быть назначен квалифицированный пользователь.

Администратор осуществляет администрирование прав доступа пользователей на основе заявок на предоставление ИТ-ресурсов:

- Ведение оргструктуры и пользователей системы;
- распределение прав доступа к объектам системы по ролям;
- организацию групп пользователей;
- привязку ролей к группам пользователей;
- определяет состав пользователей в той или иной группе;
- привязку ролей к отдельным пользователям системы.

При этом предполагается, что пользователь системы входит в состав одного и только одного структурного подразделения.

8.3.1. Работа с ролями

Привязка прав доступа к объектам ситсемы и определяемые этими правами действия с тем или иным объектом описаны в Приложении 1.

Рекомендуемая привязка прав доступа к ролям и определяемые этими ролями действия описаны в Приложении 2.

С учетом рекомендуемой настройки ролей разработан документ «Руководство оператора».

Структура ролей может быть изменена Администратором в целях оптимизации настройки работы пользователей, но строго с учетом привязки прав доступа к объектам системы и определяемых этими правами действий с тем или иным объектом.

Далее описываются действия Администратора, рекомендованные для создания, изменения, удаления ролей, определения прав доступа, назначенных на роли, назначение пользователей, организаций, групп пользователей на роль.

Для работы с ролями Администратор выбирает пункт меню «Перейти к» и подпункт «Панель управления». Панель управления доступна только Администратору.

Из левого меню надо выбрать пункт меню «Роли» в подразделе «Портал».

При этом появится окно работы с ролями (**Ошибка! Источник ссылки не найден.**).

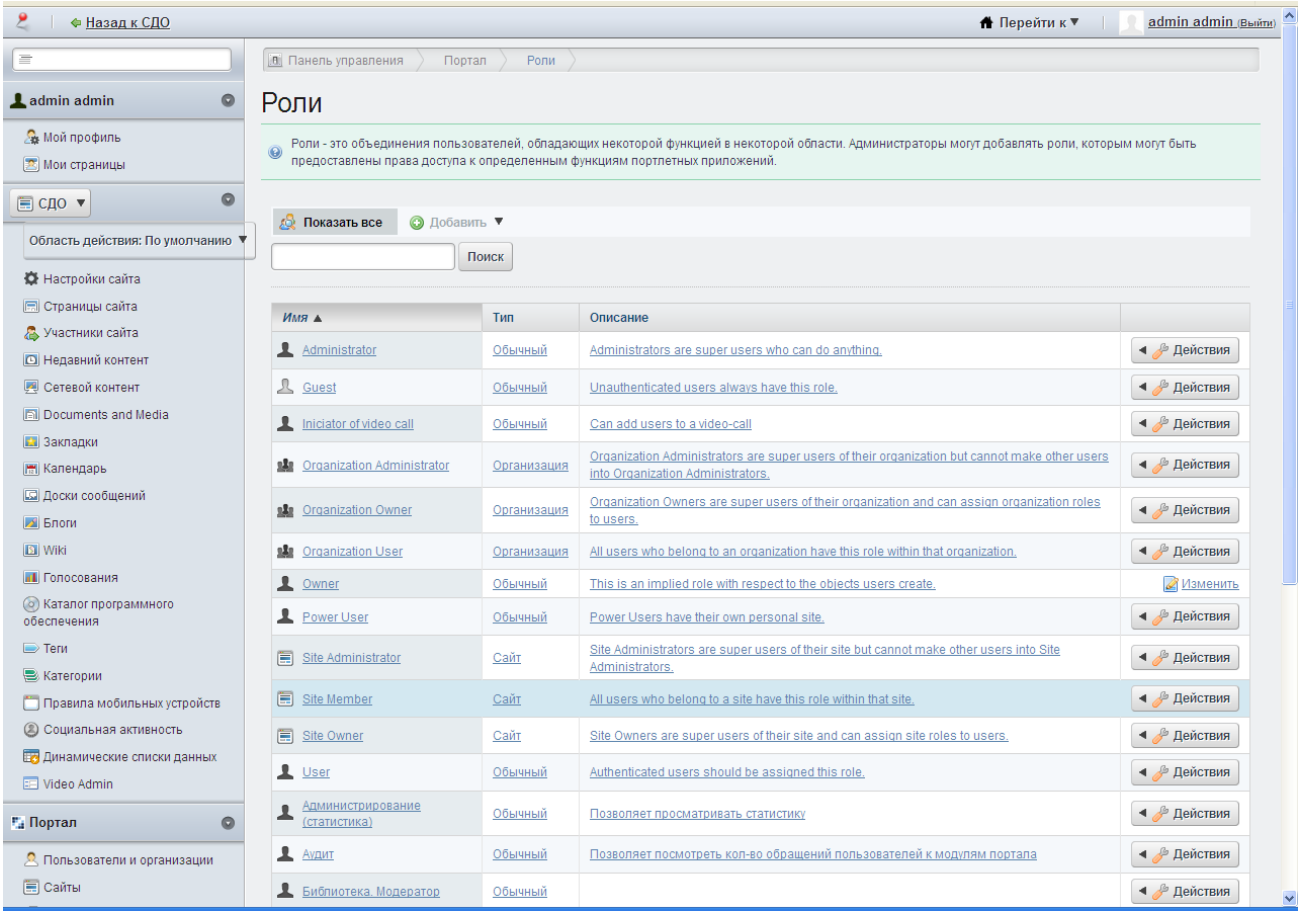

Рисунок 1. Окно работы с ролями

Добавление новой роли

Для добавления новой роли Администратор нажимает пункт меню «Добавить» и выбирает подпункт «Обычная роль». Открывается окно добавления новой роли (**Ошибка! Источник ссылки не найден.**).

Вводится имя, заголовок и описание роли, после этого Администратор нажимает кнопку «Сохранить» для сохранения новой роли или кнопку «Отмена» для выхода без сохранения новой роли.

Выход из данного окна производится по ссылке «Назад» или выбором пункта меню, в которое необходимо перейти

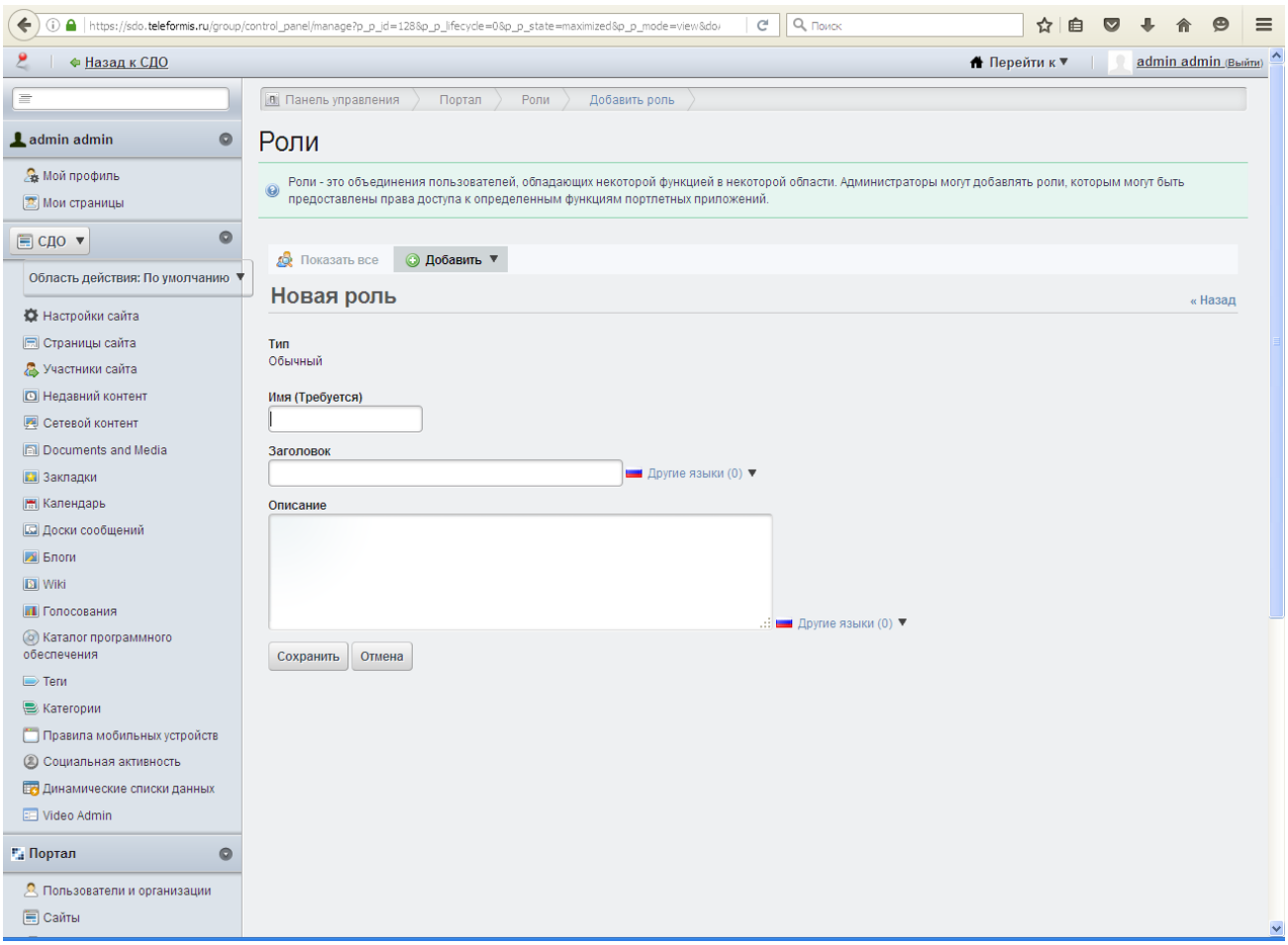

Рисунок 2. Окно ввода новой роли.

Изменение роли

Для изменения роли Администратор нажимает кнопку «Действия» на роли, которую надо изменить и выбирает действие «Изменить» или вкладку «Изменить» в окнах изменения прав доступа или назначения участников.

При этом открывается окно аналогичное окну ввода роли, в котором можно изменить имя, заголовок и описание роли.

После необходимых изменений Администратор нажимает кнопку «Сохранить» для сохранения изменений или кнопку «Отмена» для выхода без сохранения изменений.

Выход из данного окна производится по ссылке «Назад» или выбором пункта меню, в которое необходимо перейти

Определение прав доступа на роль

Для определения прав доступа на роль администратор нажимает кнопку «Действия» на роли, права доступа на которую необходимо определить и выбирает действие «Определить права доступа» или вкладку «Определить права доступа» в окнах изменения или назначения участников

При этом открывается окно определения прав доступа на роль (**Ошибка! Источник ссылки не найден.**).

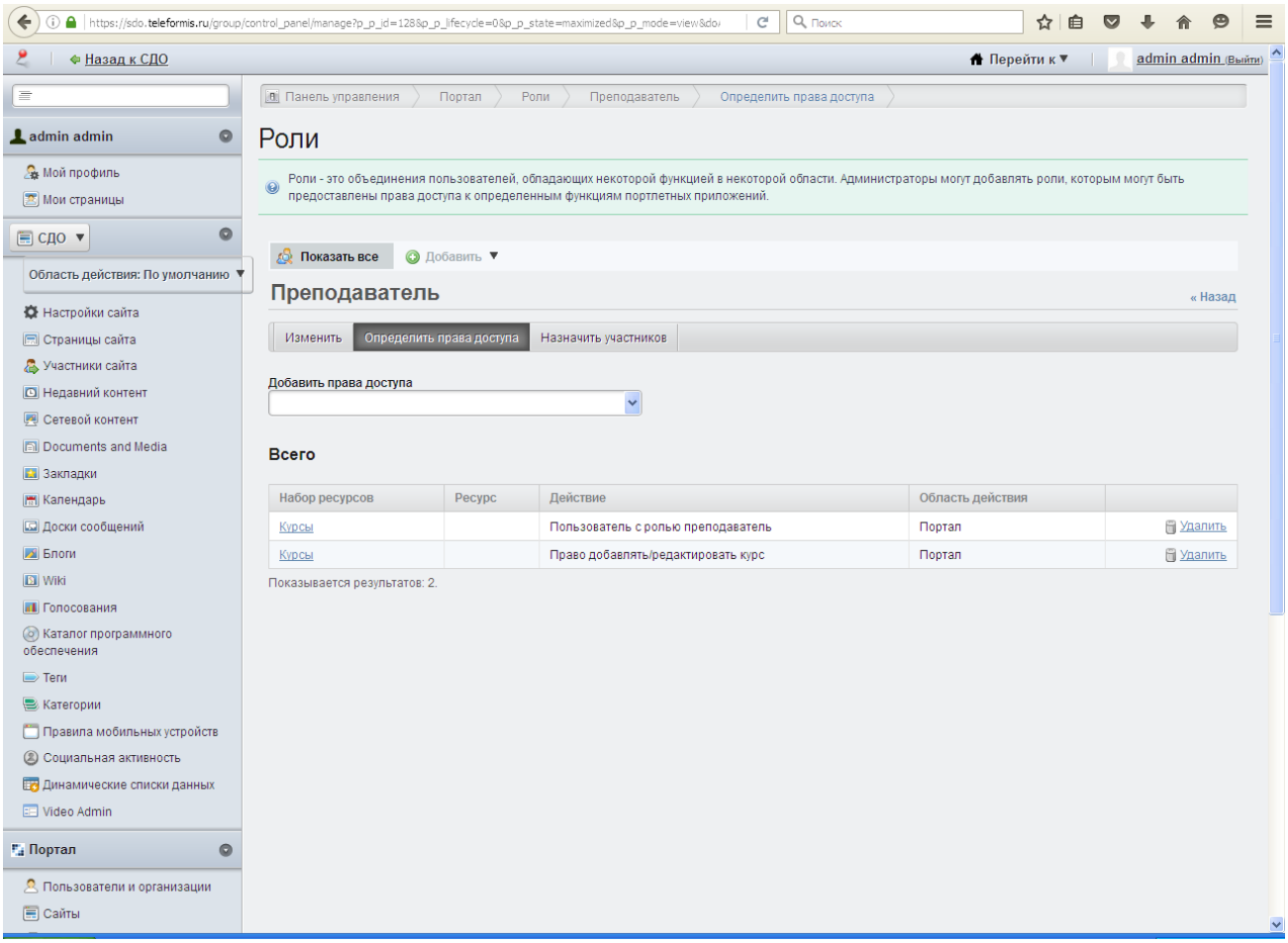

Рисунок 3. Окно определения прав доступа на роль.

В окне определения прав доступа на роль показываются все права доступа, назначенные на данную роль, в разделе «Всего» с выбранными действиями.

Для удаления назначенных прав доступа с роли, Администратор выбирает ссылку «Удалить» на праве, которое надо удалить.

Для добавления новых прав на действия из уже назначенного набора ресурсов, Администратор нажимает ссылку с названием ресурса, на котором надо добавить, удалить, изменить права на действия.

При этом открывается окно добавления, удаления, изменения прав на действия с этим ресурсом (**Ошибка! Источник ссылки не найден.**).

Для добавления новых ресурсов выбирается ресурс в выпадающем списке «Добавить права доступа».

При этом открывается окно добавления, удаления, изменения прав на действия с этим ресурсом.

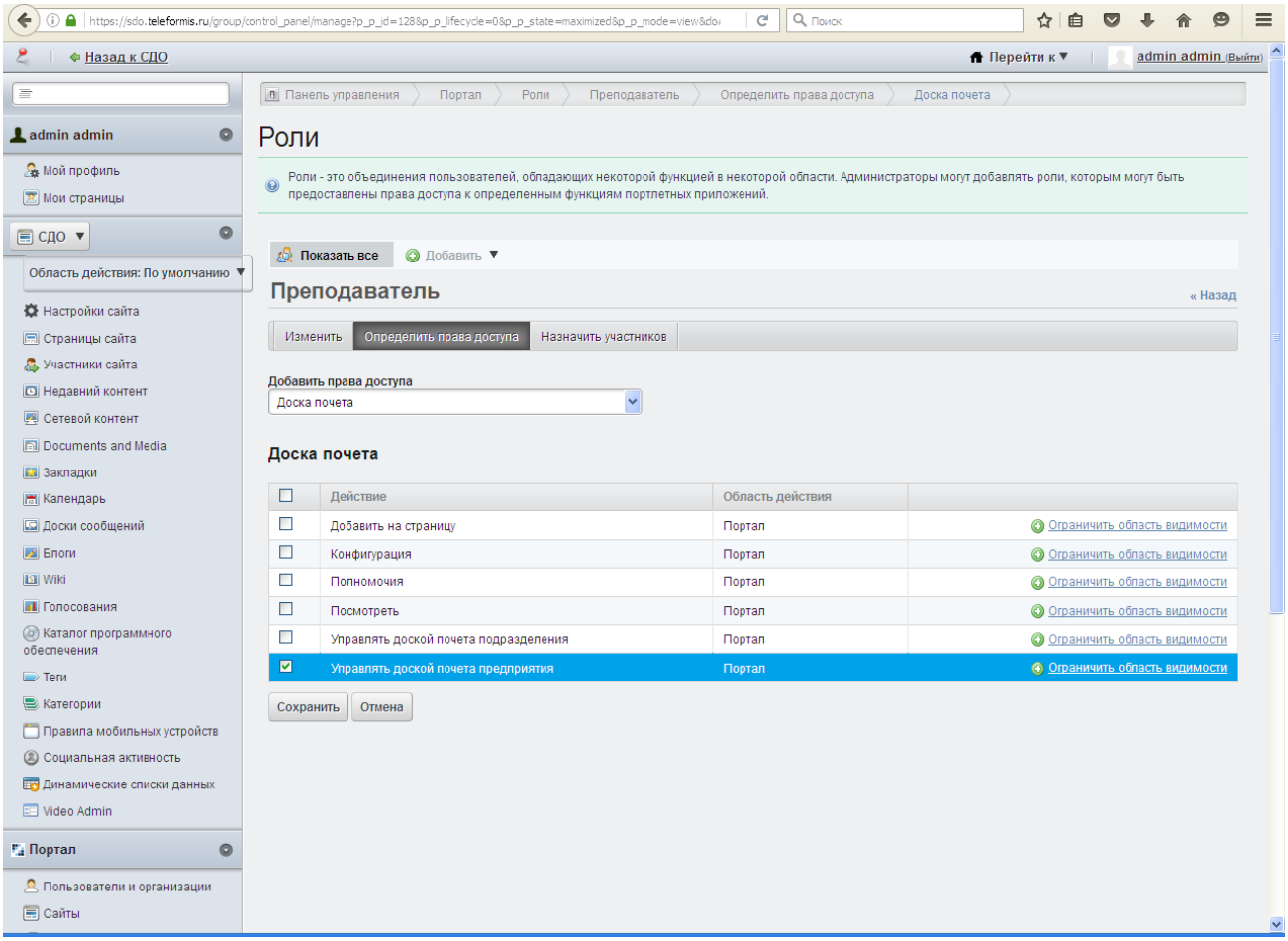

Рисунок 4. Окно добавления, удаления, изменения прав на действия с выбранным ресурсом.

Администратор выбирает необходимые действия и нажимает кнопку «Сохранить». Для выхода без сохранения сделанных изменений Администратор нажимает кнопку «Отмена»

Назначение участников

Роль можно назначать как на конкретных пользователей, так и на организации или группы пользователей:

1. Назначение/удаление роли на конкретных пользователей

Для назначения роли на конкретного пользователя Администратор нажимает кнопку «Действия» на роли, на которую необходимо назначить участников и выбирает действие «Назначить участников»» или вкладку «Изменить участников» в окнах изменения или назначения прав доступа и выбирает вкладку «Пользователи».

Открывается окно назначения пользователей на данную роль (**Ошибка! Источник ссылки не найден.**).

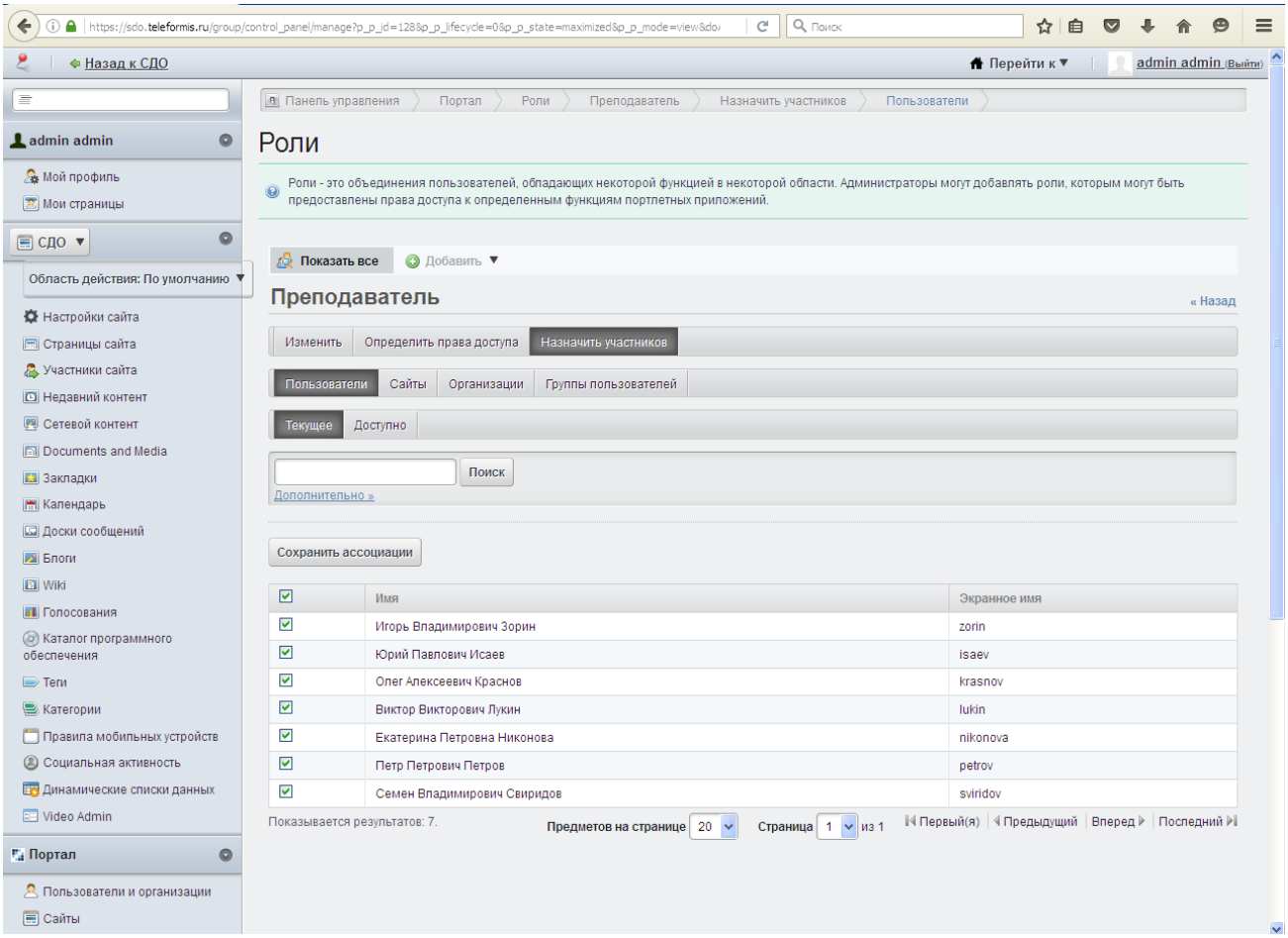

Рисунок 5. Окно назначения пользователей на роль.

В окне в закладке «Текущее» указываются все пользователи уже назначенные на роль.

Для удаления пользователя с роли необходимо снять галочку с удаляемого пользователя и нажать кнопку «Сохранить ассоциации»

Для поиска пользователя в назначенных пользователях на данную роль необходимо воспользоваться поиском пользователя портала. Для этого вводится фрагмент фамилии, имени или отчества пользователя в поисковое поле и нажимается кнопка «Поиск».

Для более расширенного варианта поиска необходимо выбрать ссылку «Дополнительно» рядом с полем ввода фрагмента поиска и откроется окно расширенного поиска (**Ошибка! Источник ссылки не найден.**) по следующим полям: Имя, Отчество, Фамилия, экранное имя, адрес email, статус. В расширенном поиске можно задать варианты поиска: все из следующих полей или любое.

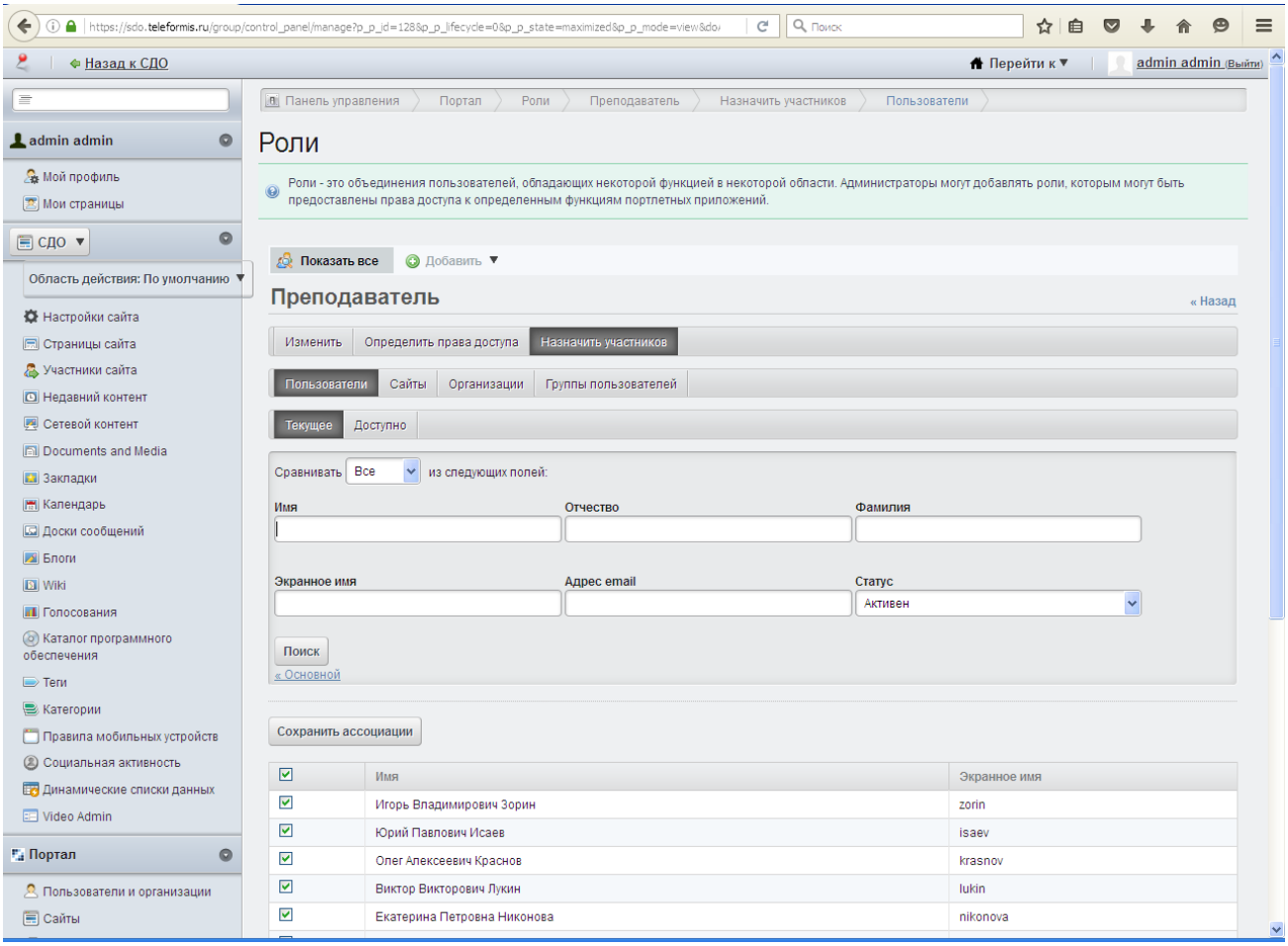

Рисунок 6. Расширенный поиск пользователей.

Возврат к основному варианту поиска возможен по ссылке «Основной» рядом с кнопкой «Поиск»

Администратор вводит необходимое для поиска сочетание фрагментов поиска и нажимает кнопку «Поиск».

Во вкладке «Доступно» поднимаются все пользователи системы.

Для назначения нового пользователя на роль необходимо установить галочку на назначаемого пользователя и нажать кнопку «Сохранить ассоциации».

Во вкладке «Доступно» работает поиск пользователей доступных для назначения на данную роль аналогично поиску в закладке «Текущие», в которой ищутся пользователи уже назначенные на данную роль.

1. Назначение/удаление роли на организации.

Для назначения роли на организацию Администратор нажимает кнопку «Действия» на роли, на которую необходимо назначить участников и выбирает действие «Назначить участников»» или

вкладку «Изменить участников» в окнах изменения или назначения прав доступа и выбирает вкладку «Организации».

Открывается окно назначения организаций на данную роль. При назначении организаций на роль, все пользователи данной организации будут иметь данную роль. Организациями являются все структурные подразделения предприятия.

Назначение/удаление организации на роль работает аналогично назначению/удалению отдельных пользователей на роль: с закладками «Текущие» и «Доступные» с возможностью поиска.

2. Назначение/удаление роли на группы пользователей.

Для назначения роли на группу пользователей Администратор нажимает кнопку «Действия» на роли, на которую необходимо назначить участников и выбирает действие «Назначить участников»» или вкладку «Изменить участников» в окнах изменения или назначения прав доступа и выбирает вкладку «Группы пользователей».

Открывается окно назначения групп пользователей на данную роль. При назначении группы пользователей на роль, все пользователи данной группы будут иметь данную роль. Назначение/удаление организации на роль работает аналогично назначению/удалению отдельных пользователей на роль: с закладками «Текущие» и «Доступные» с возможностью поиска.

Выход из окон назначения пользователей/организаций/групп пользователей на роль осуществляется по ссылке «Назад» или выбором пункта меню, в которое надо перейти.

Просмотр пользователей

Для просмотра отдельных пользователей, назначенных на роль, Администратор нажимает кнопку «Действия» на роли, на которой необходимо просмотреть участников и выбирает действие «Просмотр пользователей».

При этом открывается окно с привязанными пользователями к данной роли. Следует учесть, что в данном перечне показываются только пользователи, на которых непосредственно назначалась роль как на отдельных пользователей. Пользователи, которые унаследовали эту роль в результате назначения ее на структурное подразделение, в котором они находятся или на группу пользователей не показываются в данном списке.

Для открепления пользователя от роли, Администратор помечает его галочкой и нажимает кнопку «Отключить»

В данном режиме работает поиск пользователей, назначенных на роль, аналогично поиску в окне назначения пользователей на роль.

Удалить

Для удаления роли Администратор нажимает кнопку «Действия» на роли, которую необходимо удалить и выбирает действие «Удалить». При этом появляется запрос на подтверждение удаления значения: «Вы уверены в том, что хотите это удалить?». Для подтверждения удаления необходимо ответить «Ok», для отмены удаления – «Отмена».

8.3.2. Организация групп пользователей

Рекомендуемая структура групп пользователей приведена в Приложении 3 .

Структура групп пользователей может быть изменена Администратором для оптимизации настройки работы пользователей.

Далее описываются действия Администратора, рекомендованные для создания, изменения, удаления групп пользователей, назначения на группы пользователей ролей и пользователей.

Для работы с ролями Администратор выбирает пункт меню «Перейти к» и подпункт «Панель управления». Панель управления доступна только Администратору.

Из левого меню надо выбрать пункт меню «Группы пользователей» в подразделе «Портал».

При этом появится окно работы с группами пользователей (**Ошибка! Источник ссылки не найден.**).

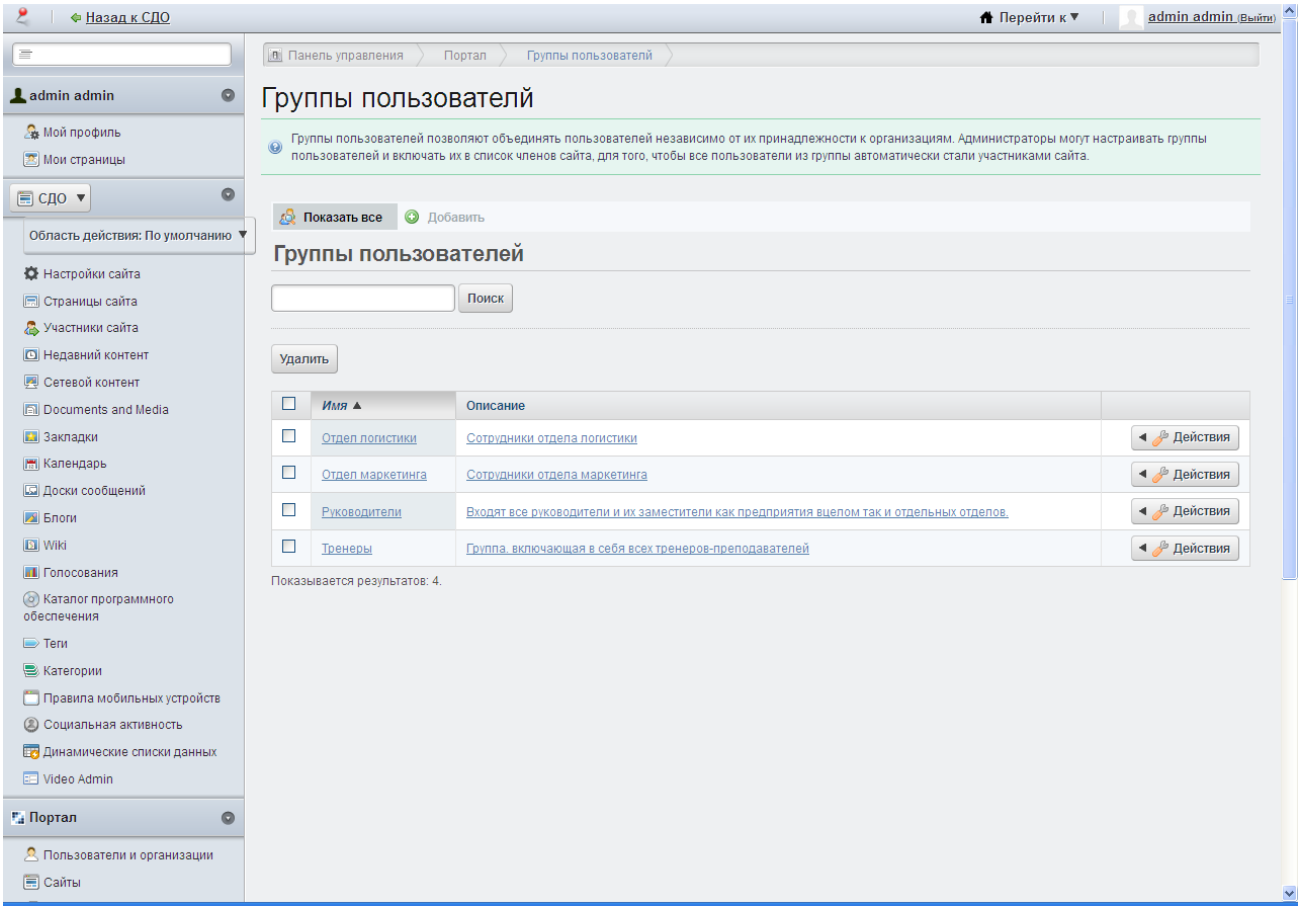

Рисунок 7. Окно работы с группами пользователей.

Добавление новой группы пользователей.

Для добавления новой группы пользователей Администратор нажимает пункт меню «Добавить». Открывается окно добавления новой группы (**Ошибка! Источник ссылки не найден.**).

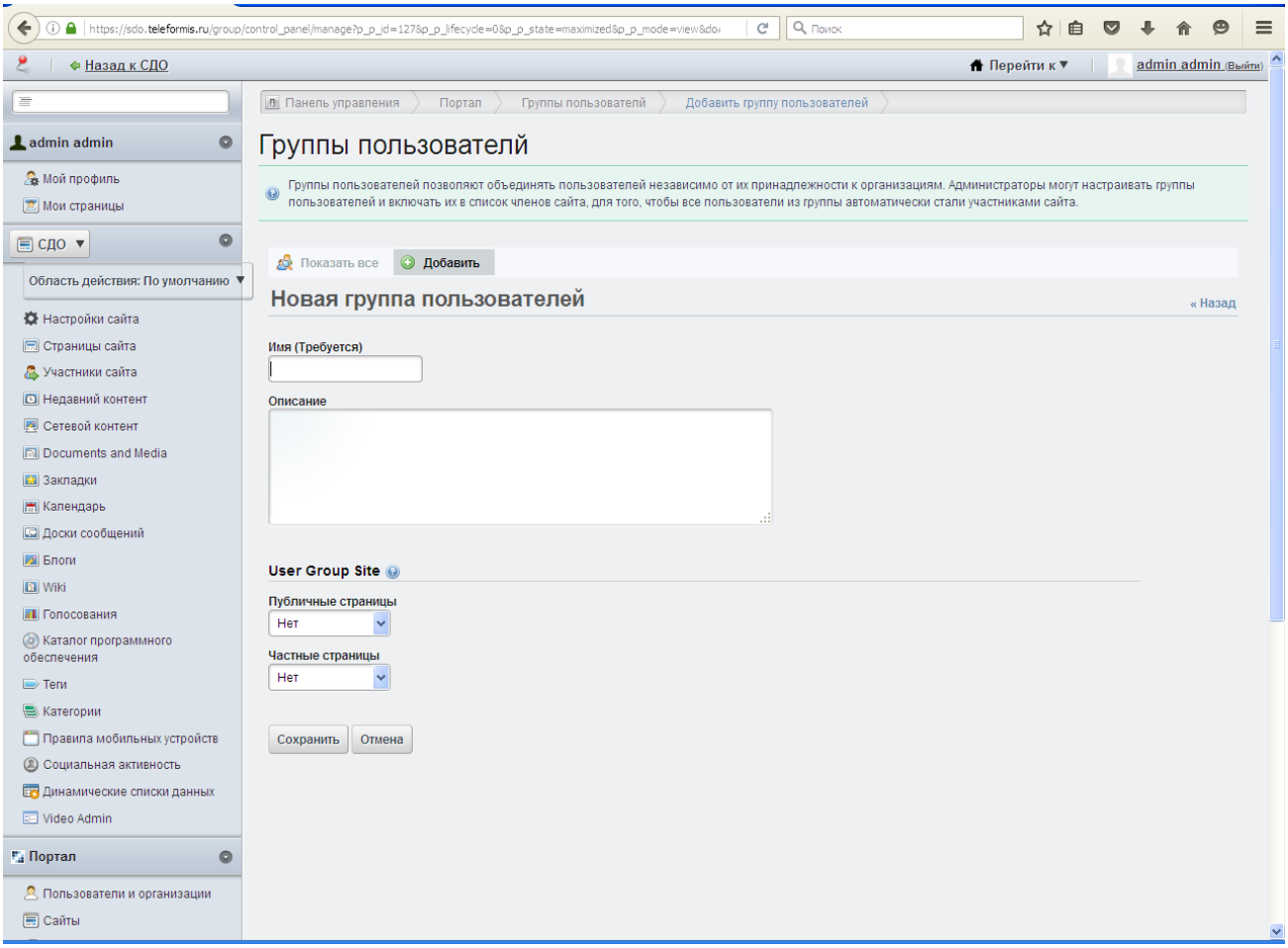

Рисунок 8. Окно ввода новой группы пользователей.

Вводится имя и описание группы, после этого Администратор нажимает кнопку «Сохранить» для сохранения новой группы или кнопку «Отмена» для выхода без сохранения новой группы.

Выход из данного окна производится по ссылке «Назад» или выбором пункта меню, в которое необходимо перейти.

Изменение группы пользователей

Для изменения группы Администратор нажимает кнопку «Действия» на группе, которую надо изменить и выбирает действие «Изменить».

При этом открывается окно, аналогичное окну ввода группы, в котором можно изменить имя и описание группы.

После необходимых изменений Администратор нажимает кнопку «Сохранить» для сохранения изменений или кнопку «Отмена» для выхода без сохранения изменений.

Выход из данного окна производится по ссылке «Назад» или выбором пункта меню, в которое необходимо перейти.

Назначить участников

Для назначения участников группы Администратор нажимает кнопку «Действия» на группе, в которую надо назначить участников и выбирает действие «Назначить участников».

При этом открывается окно назначения участников на группу (**Ошибка! Источник ссылки не найден.**).

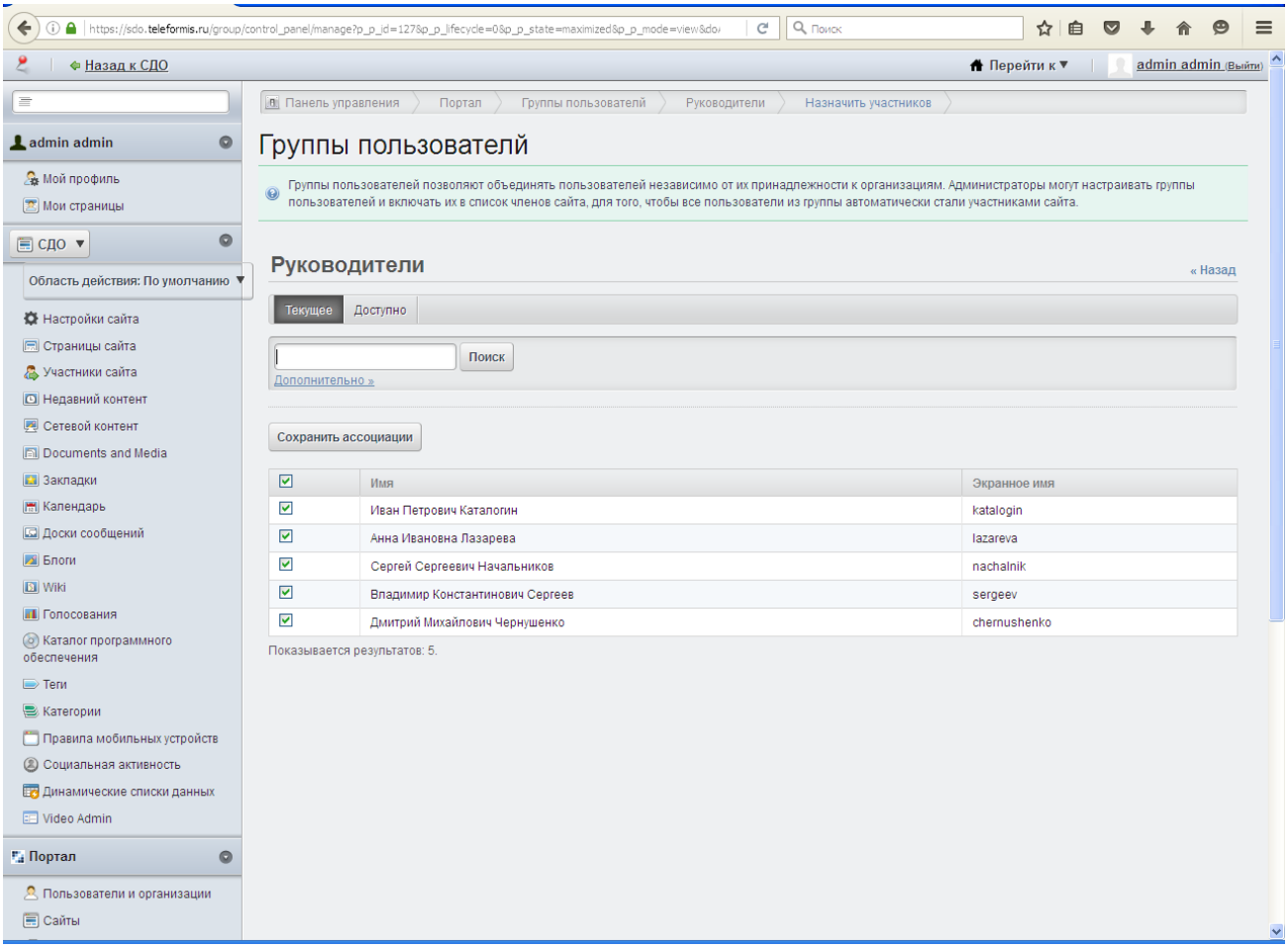

Рисунок 9. Окно назначения участников на группу.

В окне в закладке «Текущее» указываются все пользователи, уже входящие в данную группу.

Для удаления пользователя из группы необходимо снять галочку с удаляемого пользователя и нажать кнопку «Сохранить ассоциации».

Для поиска пользователя в назначенных пользователях в данную группу, необходимо воспользоваться поиском пользователя портала. Для этого вводится фрагмент фамилии, имени или отчества пользователя в поисковое поле и нажимается кнопка «Поиск».

Для более расширенного варианта поиска необходимо выбрать ссылку «Дополнительно» рядом с полем ввода фрагмента поиска и откроется окно расширенного поиска (**Ошибка! Источник ссылки не найден.**) по следующим полям: Имя, Отчество, Фамилия, экранное имя, адрес email, статус. В расширенном поиске можно задать варианты поиска: все из следующих полей или любое.

Возврат к основному варианту поиска возможен по ссылке «Основной» рядом с кнопкой «Поиск»

Администратор вводит необходимое для поиска сочетание фрагментов поиска и нажимает кнопку «Поиск».

Во вкладке «Доступно» поднимаются все пользователи системы.

Для назначения нового пользователя в группу необходимо установить галочку на назначаемого пользователя и нажать кнопку «Сохранить ассоциации».

Во вкладке «Доступно» работает поиск пользователей доступных для назначения на данную роль аналогично поиску в закладке «Текущие», в которой ищутся пользователи уже назначенные на данную роль.

Выход из окна назначения пользователей в группу осуществляется по ссылке «Назад» или выбором пункта меню, в которое надо перейти.

Удалить

Для удаления группы Администратор нажимает кнопку «Действия» на группе, которую необходимо удалить и выбирает действие «Удалить». При этом появляется запрос на подтверждение удаления: «Вы уверены в том, что хотите это удалить?». Для подтверждения удаления необходимо ответить «Ok», для отмены удаления – «Отмена».

Система не позволяет удалить группу, в которой находятся пользователи. Для удаления группы нужно сначала удалить всех пользователей портала из данной группы.

8.3.3. Привязка ролей к группам пользователей

Рекомендуемая привязка ролей к группам пользователей приведена в Приложении 3.

Привязка ролей к группам пользователей может быть изменена Администратором для оптимизации настройки работы пользователей.

Если роль назначена на группу пользователей, то все пользователи, назначенные в данную группу, имеют эту роль как унаследованную от группы.

Назначение ролей на группы описано в п. **Ошибка! Источник ссылки не найден.** данного руководства, в описании действия «Назначение участников» в подразделе «назначение/удаление роли на группы пользователей»

8.3.4. Определение состава пользователей в той или иной группе

Администратор добавляет пользователя в ту или иную группу согласно заявке на предоставление ИТ-услуги. Шаблон данной заявки приведен в Приложении 4.

Пользователь портала может входить в несколько групп. При этом он будет наследовать все роли, назначенные группам, в которые он входит.

Включение пользователей в группу возможно двумя способами:

- со стороны группы. Данное назначение описано в п.**Ошибка! Источник ссылки не найден.** в действии «Назначить участников»;
- со стороны пользователей. Данное назначение описывается ниже.

Для назначения пользователя в группу Администратор выбирает пункт меню «Перейти к» и подпункт «Панель управления». Панель управления доступна только Администратору.

Из левого меню необходимо выбрать пункт меню «Пользователи и организации» в подразделе «Портал».

При этом открывается окно управления организациями и пользователями портала (**Ошибка! Источник ссылки не найден.**).

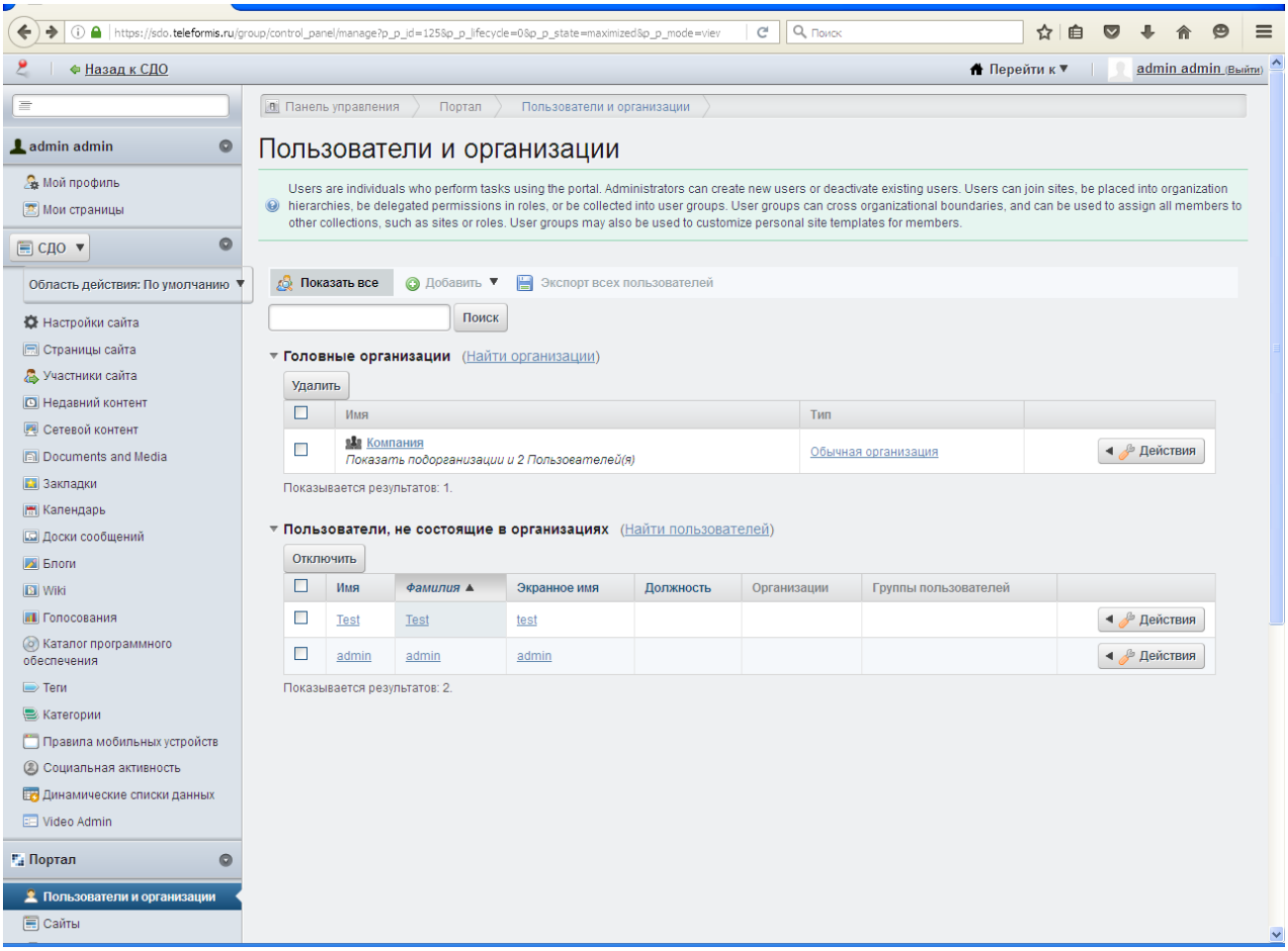

Рисунок 10. Окно управления организациями и пользователями портала.

Предполагается, что пользователь системы, за исключением технических пользователей, таких как «Test», «Администратор», входит в состав одного и только одного структурного подразделения.

Администратор для назначения пользователя в группу пользователей должен выбрать пользователя. Это можно сделать несколькими способами:

- Выбрать по дереву структурных подразделений нужное структурное подразделение. Выбор структурного подразделения осуществляется, начиная с головной организации выбором ссылки сначала головной организации, затем структурного подразделения 1 уровня и т.д. При выборе структурного подразделения любого уровня в нижней части экрана выдается список пользователь данного структурного подразделения (**Ошибка! Источник ссылки не найден.**).

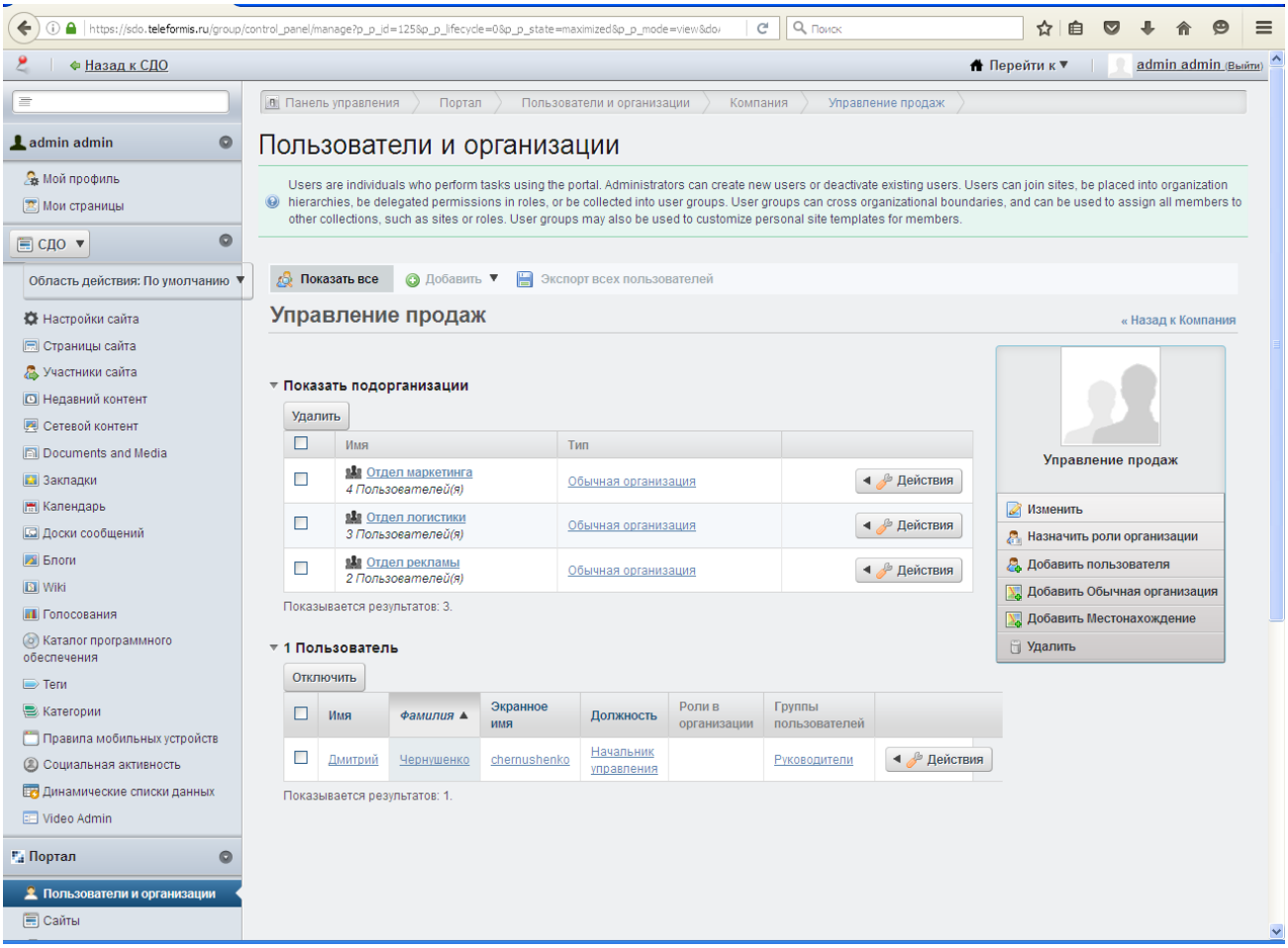

Рисунок 11. Окно выбора структурного подразделения.

Для выбора пользователя Администратор нажимает на ссылку выбираемого пользователя (его имя, отчество и фамилию). При этом открывается окно личных данных пользователя (**Ошибка! Источник ссылки не найден.**).

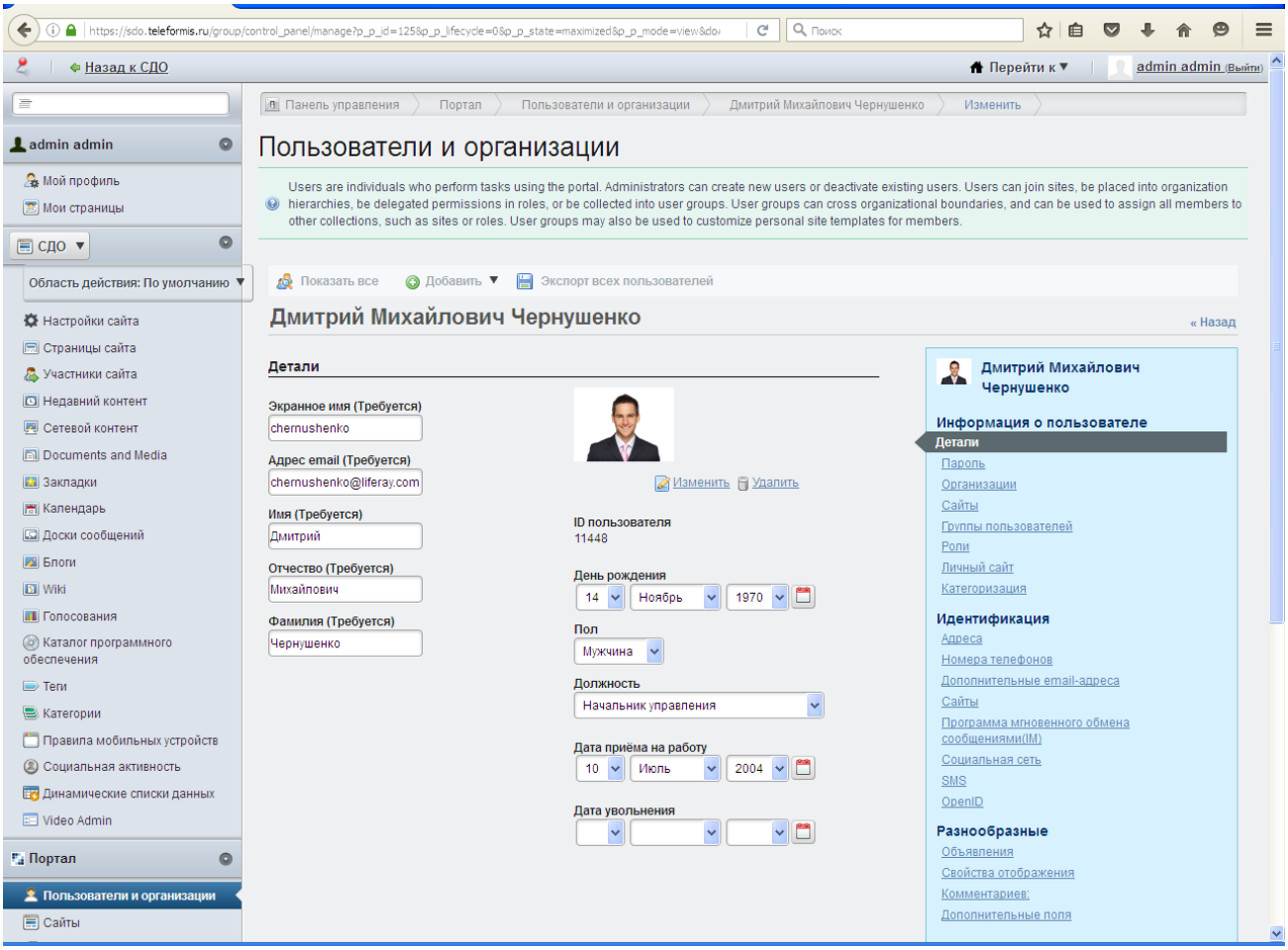

Рисунок 12. Окно личных данных пользователя.

- Найти структурное подразделение сотрудника поиском или найти самого сотрудника.

  Поиск структурного подразделения или сотрудника осуществляется в общем поиске окна управления организациями и пользователями системы. Для этого в поле поиска вводится фрагмент поиска. Данный поиск предназначен как для поиска структурного подразделения, так и для поиска сотрудников подразделений. По введенному фрагменту проводится сразу два поиска: подразделений и сотрудников (**Ошибка! Источник ссылки не найден.**).

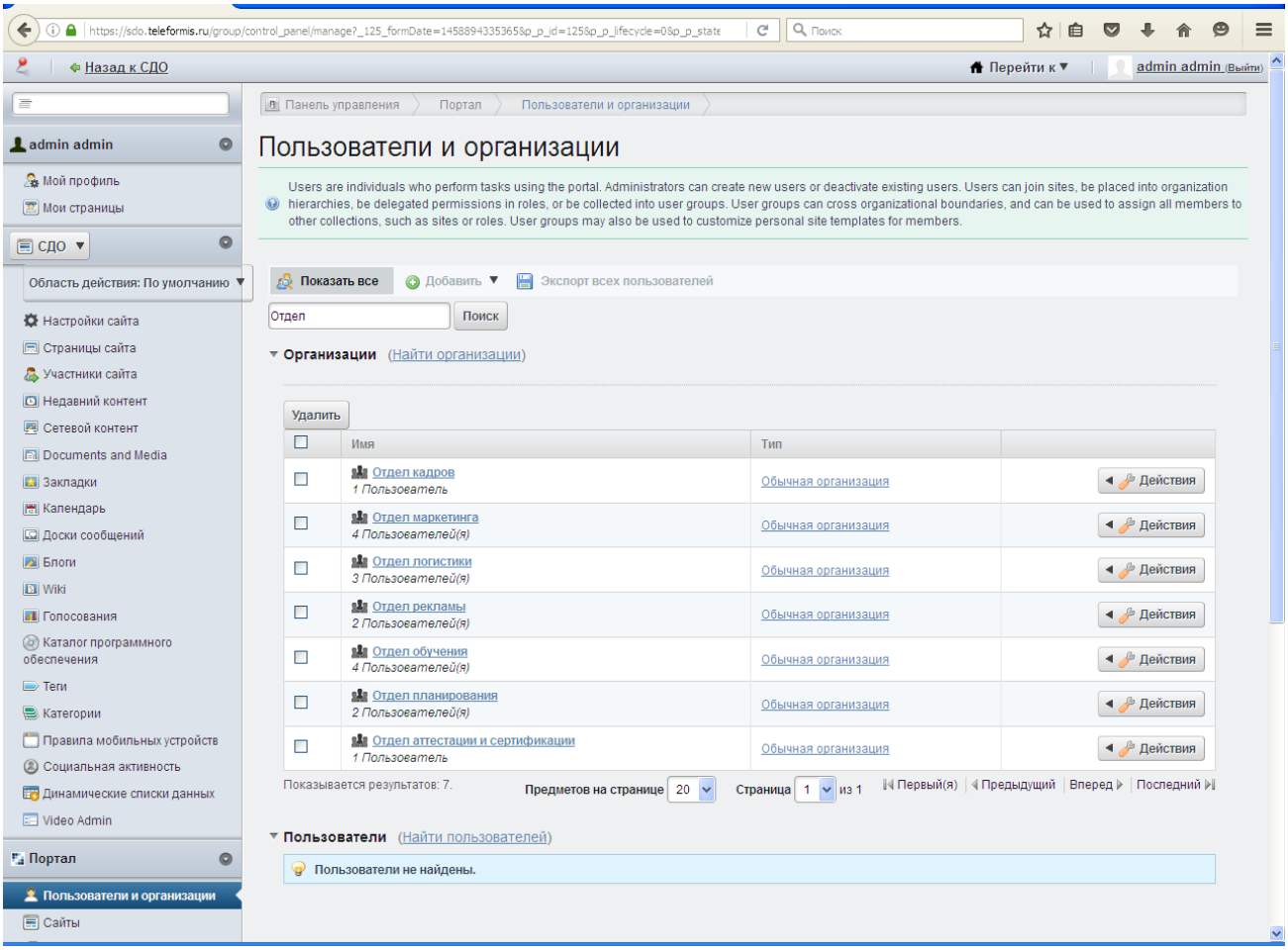

Рисунок 13. Окно с результатами общего поиска.

После общего поиска открывается окно с результатами поиска, в котором можно выбрать структурное подразделение из найденных подразделений, для этого необходимо нажать ссылку-название подразделения.

При выборе структурного подразделения любого уровня в нижней части экрана выдается список пользователь данного структурного подразделения.

Для выбора пользователя администратор нажимает на ссылку выбираемого пользователя (его имя, отчество и фамилию). При этом открывается окно личных данных пользователя.

В окне с результатами поиска можно сразу выбрать нужного пользователя, нажав на ссылку выбираемого пользователя (его имя, отчество и фамилию). При этом открывается окно личных данных пользователя.

В окне с результатами общего поиска можно конкретизировать поиск по подразделению – нажав ссылку «Найти организацию» или по сотрудникам, нажав ссылку «Найти пользователей». В данных поисках будет искаться соответственно или только структурные подразделения или пользователи портала. В данных поисках возможен поиск по фрагменту - основной поиск, либо по сочетанию полей. Для поиска по сочетанию полей в общем поиске выбирается ссылка

«Дополнительно». Для возврата в основной поиск всегда выбирается ссылка «Основной».

Результатом поиска пользователя тем или иным способом является окно с личными данными пользователя.

Для добавления пользователя в группу Администратор в окне личных данных пользователя выбирает из правого меню пункт «Группы пользователей».

При этом открывается окно с перечнем групп, в которые входит выбранный пользователь (**Ошибка! Источник ссылки не найден.**).

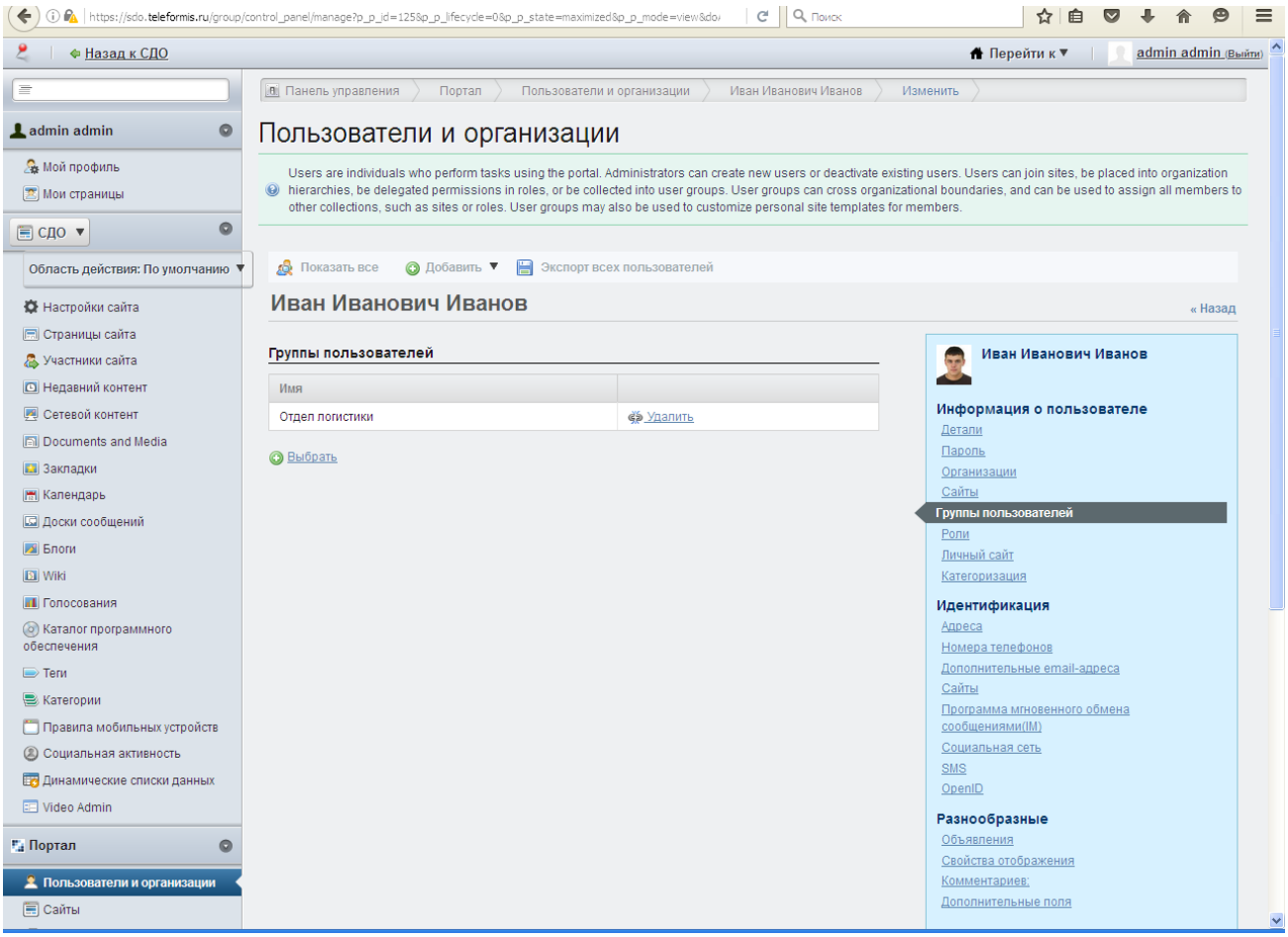

Рисунок 14. Окно с группами, в которые входит пользователь.

Удаление выбранного пользователя из группы

Для удаления пользователя из группы Администратор нажимает ссылку «Удалить» в строке той группы, из которой необходимо удалить пользователя.

Добавление выбранного пользователя в новую группу

Для добавления пользователя в новую группу Администратор нажимает ссылку «Выбрать» под перечнем групп, в которые назначен пользователь.

При этом открывается окно выбора группы, в которую надо поместить пользователя, в котором по фрагменту названия группы можно найти необходимую группу. Для этого необходимо ввести фрагмент поиска в поле поиска и нажать кнопку «Поиск». При пустом поле поиска на экран поднимаются все группы портала (**Ошибка! Источник ссылки не найден.**).

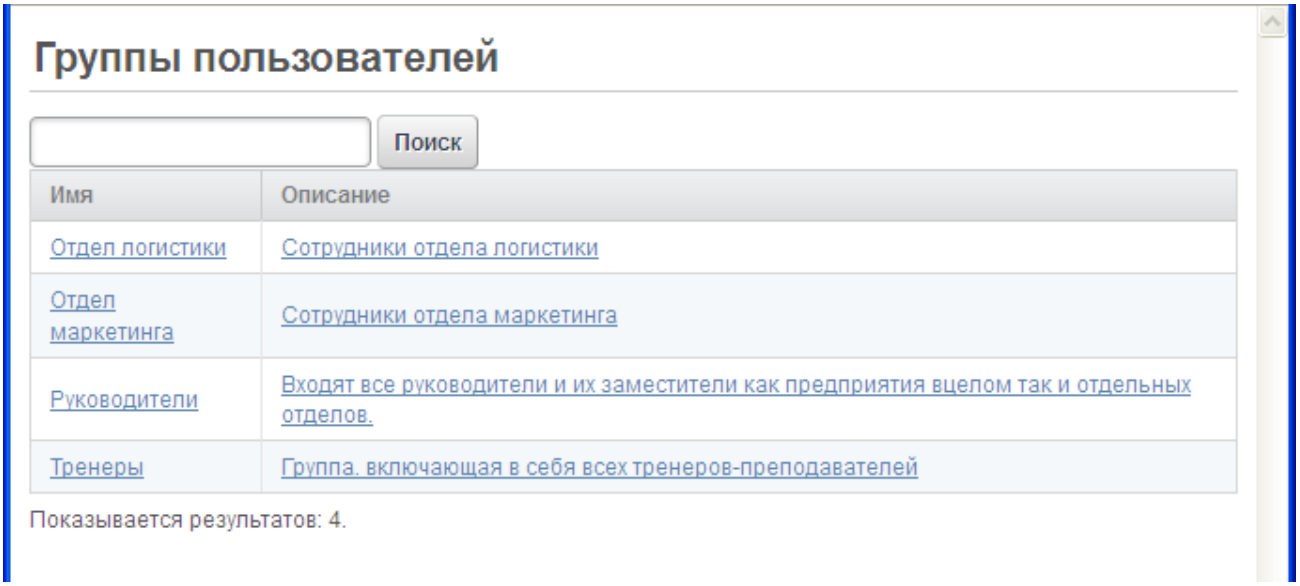

Рисунок 15 Окно выбора группы.

Для выбора группы, в которую необходимо поместить пользователя Администратор нажимает ссылку-название или описание группы.

При этом выбранная группа появляется в списке групп, в которые входит пользователь.

Сохранение удаления/добавления пользователя в группу

Для сохранения сделанных изменений: удаления пользователя из группы или добавления пользователя в группы, Администратору необходимо нажать кнопку «Сохранить» в конце правого меню.

Для выхода из окна личных данных сотрудника без сохранения всех изменений, которые были совершены с данным пользователем, в данном окне Администратору необходимо нажать кнопку «Отмена» в конце правого меню.

8.3.5. Привязка ролей к отдельным пользователям

Администратор добавляет пользователя в ту или иную группу согласно заявке на предоставление ИТ-услуги. Шаблон данной заявки приведен в Приложении 4.

Пользователь системы получает роли следующими способами:

- наследует все роли, назначенные на группы пользователей, в которые он входит;
- назначение роли непосредственно на этого пользователя.

В данном разделе руководства рассматривается назначение ролей непосредственно на пользователя.

Назначение роли непосредственно на пользователя возможно двумя способами:

- со стороны роли. Данное назначение описано в п.**Ошибка! Источник ссылки не найден.** в действии «Назначение участников» в подразделе «Назначение/удаление роли на конкретных пользователей»;
- со стороны пользователей. Данное назначение описывается ниже.

Для назначения роли на пользователя Администратор выбирает пункт меню «Перейти к» и подпункт «Панель управления». Панель управления доступна только Администратору.

Из левого меню надо выбрать пункт меню «Пользователи и организации» в подразделе «Портал».

При этом открывается окно управления организациями и пользователями системы.

При этом предполагается, что пользователь портала, за исключением технических пользователей, таких как «Test», «Администратор», входит в состав одного и только одного структурного подразделения.

Администратор для назначения пользователю роли должен выбрать пользователя. Это можно сделать несколькими способами. Выбор пользователя в окне управления организациями и пользователями системы подробно описан в п. **Ошибка! Источник ссылки не найден.**.

После выбора пользователя Администратор в окне личных данных пользователя в правом меню выбирает пункт «Роли».

При этом открывается окно управления ролями на выбранном пользователе (**Ошибка! Источник ссылки не найден.**).

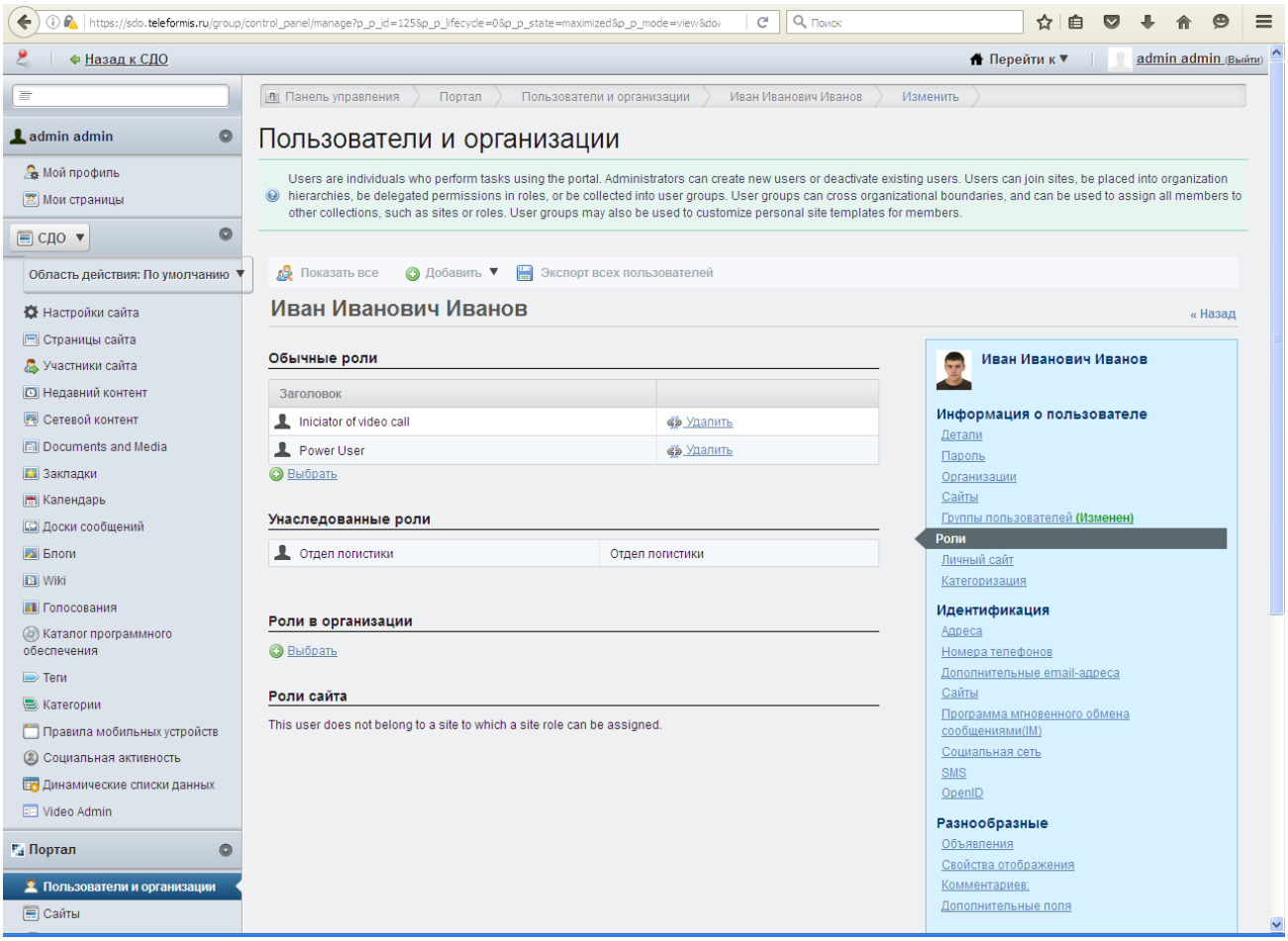

Рисунок 16. Окно управления ролями на пользователе.

В разделе «Унаследованные роли» показываются группы, в которые входит пользователь. Следует учесть, что пользователь наследует роли, назначенные на группы, в которые он входит. Описание назначения ролей на группы приведено в п. **Ошибка! Источник ссылки не найден.** данного документа. Описание включения пользователя в группы приведено в п. **Ошибка! Источник ссылки не найден.** данного документа.

В разделе «Обычные роли» данного окна указываются роли, назначенные непосредственно на данного пользователя.

Удаление роли, назначенной на пользователя

Для удаления роли Администратор нажимает ссылку «Удалить» на строке с ролью, предназначенной для удаления.

Добавление новой роли на пользователя

Для добавления новой роли на выбранного пользователя Администратор нажимает ссылку «Выбрать» под разделом «Обычные роли».

При этом открывается окно выбора ролей (**Ошибка! Источник ссылки не найден.**).

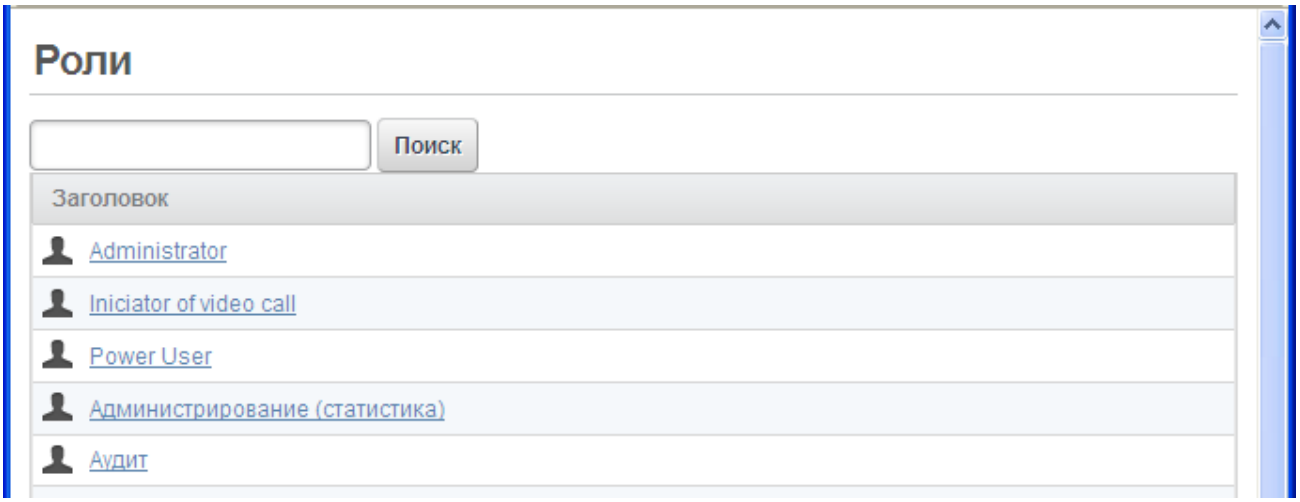

Рисунок 17. Окно выбора ролей

Администратор выбирает роль, которую необходимо добавить и нажимает ссылку-название роли.

Выбор роли возможен выбором на странице. Переход по страницам производится ссылками: «Первый», «Последний», «Предыдущий», «Следующий».

В окне присутствует поиск роли по фрагменту ее названия. Для этого Администратор вводит фрагмент поиска в поле поиска и нажимает кнопку «Поиск».

Выбранная роль добавляется в раздел «Обычные роли» окна управления ролями на пользователе.

Сохранение удаления/добавления ролей пользователю

Для сохранения сделанных изменений: удаления роли пользователя или добавления роли пользователю, Администратору необходимо нажать кнопку «Сохранить» в конце правого меню.

Для выхода из окна личных данных сотрудника без сохранения всех изменений, которые были совершены с данным пользователем, в данном окне Администратору необходимо нажать кнопку «Отмена» в конце правого меню.

8.3.6. Особенности создания ролей для разграничения прав доступа к папкам, подпапкам документов или отдельным документам

При создании папки, подпапки или документа модератор документов или пользователь, имеющий полномочия на назначение прав доступа на папку, подпапку или конкретный документ определяет права доступа другим ролям. Для такого варианта разграничений прав доступа на каждую папку вводится столько ролей, сколько нужно групп пользователей с разными правами доступа к объекту.

Рассмотрим наиболее простой пример.

Для папки «Тестовая папка» необходимо разграничить доступ следующим образом:

- Пользователи системы, не видящие данную папку совсем;
- Пользователи системы, имеющие право просматривать данную папку целиком, или частично: по отдельным папкам или даже документам;
- Пользователи портала, имеющие полные права на папку целиком или частично: по отдельным папкам или даже документам.

Вводим три обычные роли без прав доступа, описанных в п.**Ошибка! Источник ссылки не найден.**:

- Тестовая папка (просмотр)
- Тестовая папка (изменения)
- Тестовая папка (просмотр ролей для назначения прав доступа)

Для данных ролей вводим права доступа по ролям.

Для этого Администратор в окне работы с ролями (**Ошибка! Источник ссылки не найден.**) выбирает:

- роль «Тестовая папка (просмотр)», нажимает кнопку «Действия», выбирает действие «Права доступа» и выставляет галочку в графе «Посмотреть» для ролей «Документы (модератор)» и «Тестовая папка (просмотр ролей для назначения прав доступа)».
- роль «Тестовая папка (изменения)», нажимает кнопку «Действия», выбирает действие «Права доступа» и выставляет галочку в графе «Посмотреть» для ролей «Документы (модератор)» и «Тестовая папка (просмотр ролей для назначения прав доступа)».

Тем самым Администратор разрешает при назначении прав на объекты пользователям с ролями «Документы (модератор)» и «Тестовая папка (просмотр ролей для назначения прав доступа) назначать права доступа на роли «Тестовая папка (просмотр)» и «Тестовая папка (изменения)».

Описание назначения прав доступа к объекту: проекту, папке, документу, на указанные роли приводится в документе «Руководство оператора»

8.3.7. Настройка уровней показа оргструктуры.

В связи с тем, что вложенность оргструктуры может быть достаточно большой, вводится настройка уровней показа оргструктуры.

Настройка уровней показа производится пользователем с правами администратора. Для настройки уровней администратор выбирает пункт меню «Главная», подпункт «Оргструктура» и нажимает кнопку в виде гаечного ключа «Опции». Данная кнопка появляется только у администратора в правом верхнем углу экрана. Далее администратор выбирает пункт «Конфигурация». При этом открывается окно настройки уровней показа оргструктуры , в котором администратор настраивает глубину отображения для главной организации и для подразделений. Администратор вводит значения в данные поля и нажимает кнопку «Сохранить». Значения глубины показа не могут быть менее 2.

Приложение 1. Права доступа в разрезе объектов

№ п/п	Объект	Право доступа	Разрешенное действие
1	Справочник «Места проведения мероприятий»	Управлять справочником «Места проведения мероприятий»	Добавлять, изменять и удалять записи в справочнике «Места проведения мероприятий»
2	Справочник «Мероприятия»	Управлять справочником «Мероприятия»	Добавлять, изменять и удалять записи в справочнике «Мероприятия»
3	Справочник «Цели мероприятия»	Управлять справочником «Цели мероприятия»	Добавлять, изменять и удалять записи в справочнике «Цели мероприятия»
5	Справочник «Типы отпусков»	Управлять справочником «Типы отпусков»	Добавлять, изменять и удалять записи в справочнике «Типы отпусков»
6	Расписание мероприятий	Управлять календарем предприятия	Управление календарем предприятия, согласно выставленным правам: добавлять события, экспортировать все события
7	Личный кабинет	Прав доступа не требуется	Доступны все действия владельцу календаря
8	Доска почета предприятия	Управлять доской почета предприятия	Добавление сотрудника на доску почета предприятия, удаление сотрудника с доски почета предприятия

№ п/п	Объект	Право доступа	Разрешенное действие
9	Доска почета подразделения	Управлять доской почета подразделения	Добавление сотрудника на доску почета своего подразделения или подразделения, которое определено в справочнике «Подразделения для просмотра новостей, досок почета и мероприятий» для подразделения пользователя удаление сотрудника с доски почета своего подразделения
10	Новости предприятия	Управлять новостями предприятия	Добавление (при наличии дополнительного права «Добавить запись»), изменение, удаление новости предприятия, добавление, изменение, удаление комментария к новости предприятия
11	Новости подразделения	Управлять новостями подразделения	Добавление (при наличии дополнительного права «Добавить запись»), изменение, удаление новости своего подразделения или подразделения, которое назначено в справочнике «Подразделения для просмотра новостей, досок почета и мероприятий» для подразделения пользователя, добавление, изменение, удаление комментария к новости своего подразделения

№ п/п	Объект	Право доступа	Разрешенное действие
12	Форум	Назначаются все стандартные права из раздела «Контент сайта», подраздела «Доски сообщений» в частях «Доски сообщений», «Категория форума», «Сообщение форума», «Тема доски сообщений» без полномочий. Также назначается право из раздела «Приложения сайта», подраздела «Доски сообщений» «Посмотреть»	Управлять форумом
13	График отпусков	Подтвердить отпуск, просмотр графиков отпусков всех подразделений	Подтверждение/отказ заявок на отпуск сотрудников, просмотр графиков отпусков всех отделов, при наличии права доступа: просмотр графиков отпусков всех подразделений. Просмотр графика отпусков своего отдела не требует дополнительного права.
14	Отсутствующие сотрудники (предприятие)	Управлять данными по отсутствующим сотрудникам (предприятие)	Позволяет вводить и просматривать данные по отсутствующим сотрудникам в целом по предприятию
15	Календарь праздников	Добавить запись	Позволяет настраивать календарь праздников
16	Руководители	Посмотреть	Позволяет назначить руководителей и их уровень в структурном подразделении

№ п/п	Объект	Право доступа	Разрешенное действие
17	Штатное расписание	Управлять штатным расписанием	Позволяет вводить и изменять штатное расписание по каждому структурному подразделению
18	Руководитель, отвечающий на вопросы сотрудников	Руководство предприятия (вопросы сотрудников)	Появляется в перечне руководителей, которым возможно задать вопрос в электронной приемной
19	Модератор вопросов руководству	Управлять вопросами к руководству	Позволяет удалять чужие вопросы.
20	Руководитель, к которому можно записаться на прием	Руководство предприятия (запись сотрудника на прием)	Появляется в перечне руководителей, к которым возможно записаться на прием в электронной приемной
21	Запись на прием к руководству (модератор и/или сотрудник, имеющий право записывать на прием других сотрудников)	Управлять расписанием записей на прием к руководству, Управлять записью на прием другого сотрудника	Позволяет управлять возможными периодами записи на прием к тому или иному руководителю и удаление записи на прием любого сотрудника. Позволяет записать на прием любого другого сотрудника (запись на прием самого себя не требует дополнительных прав)
22	Оргструктура		Просмотр оргструктуры не требует дополнительного права доступа

№ п/п	Объект	Право доступа	Разрешенное действие
23	Заявки	Восстановить шаблон заявки, добавить шаблон заявки, изменить шаблон заявки, удалить шаблон заявки	Позволяет управлять шаблона заявок пользователя. Работа с заявками не требует дополнительного права доступа
24	Статистика	Посмотреть, Просмотр обращений пользователей к модулям системы	Позволяет просмотреть кол-во обращений пользователей к модулям системы
25	Управление документами	Назначаются все стандартные права из раздела «Контент сайта», подраздела «Documents and Media»	Позволяет управлять проектным офисом с созданием папок, подпапок, документов и разграничением прав по ролям на отдельные папки, подпапки и т.д.

№ п/п	Объект	Право доступа	Разрешенное действие
26	Разграничение прав доступа к отдельным папкам, подпапкам и т. д. при управлении документами	При создании/ изменении папки, подпапки или документа модератор или исполнитель, имеющий на то право, создает права доступа из перечня: «Доступ», «Добавить документ», «Добавить ярлык», «Добавить подпапку», «Удалить», «Полномочия», «Сохранить», «Посмотреть». Права доступа назначаются на роли, которые при своем создании имеют право доступа «Посмотреть» на рекомендуемую роль «Управление документами (модератор)» и/или «Управление документами. Название объекта (просмотр ролей для назначения прав доступа)»	Разграничение прав доступа к отдельным папкам, подпапкам, документам

№ п/п	Объект	Право доступа	Разрешенное действие
27	Пользователи и организации	«Добавить организацию», «Добавить пользователя» из раздела «Портал», подраздела «Общий». «Посмотреть» из раздела «Панель управления: Портал», подраздела «Пользователи и организации». «Назначить участников», «Посмотреть», «Сохранить», «Удалить», «Управлять подчиненными организациями», «Управлять пользователями» из раздела «Портал», подраздела «Пользователи и организации», части «Организация». «Посмотреть», «Сохранить», «Удалить» из раздела «Портал», подраздела «Пользователи и организации», части «Пользователь».	Модифицировать оргструктуру предприятия в системе.

№ п/п	Объект	Право доступа	Разрешенное действие
28	Блоги руководителей	«Управлять блогами» из раздела «Приложения сайта» подраздела «Новости»; «Добавить запись» из раздела «Контент сайта» подраздела «Новости» части «Дневник»	Управлять своим блогом
29	Курсы. Преподаватель, куратор	Пользователь с ролью преподаватель	Позволяет назначить пользователя системы преподавателем на курс/раздел или куратором курса
30	Курсы (модератор)	Право добавлять/редактировать курс	Создавать, изменять, наполнять курсы.

Приложение 2. Структура функциональных ролей

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
1	Справочник «Места проведения мероприятий»	Основное право доступа: «Управлять справочником «Места проведения мероприятий» из раздела «Приложения сайта», подраздела «Справочники»	Добавлять, изменять и удалять записи в справочнике «Места проведения мероприятий»
2	Справочник «Мероприятия»	Основное право доступа: «Управлять справочником «Мероприятия»»» из раздела «Приложения сайта», подраздела «Справочники»	Добавлять, изменять и удалять записи в справочнике «Мероприятия»
3	Справочник «Цели мероприятий»	Основное право доступа: «Управлять справочником «Цели мероприятий» из раздела «Приложения сайта», подраздела «Справочники»	Добавлять, изменять и удалять записи в справочнике «Цели мероприятий»
4	Справочник «Типы отпусков»	Основное право доступа: «Управлять справочником «Типы отпусков» из раздела «Приложения сайта», подраздела «Справочники»	Добавлять, изменять и удалять записи в справочнике «Типы отпусков»

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
5	Календарь предприятия	Основное право доступа: «Управлять календарем предприятия» из раздела «Приложения сайта», подраздела «Календарь» Дополнительные права на выбор: «Добавить событие» из раздела «Контент сайта», подраздела «Календарь», части «Календарь», экспорт всех событий из раздела «Контент сайта», подраздела «Календарь», части «Календарь»	Управление календарем предприятия, согласно выставленным правам: добавлять события, экспортировать все события
6	Новостная лента (подразделение)	Основное право доступа: «Управлять новостями подразделения» из раздела «Приложения сайта», подраздела «Новости» Дополнительное право: «Добавить запись» из раздела «Контент сайта», подраздела «Новости»	Добавление (при наличии дополнительного права «Добавить запись»), изменение, удаление новости своего подразделения или подразделения назначенного в справочнике «Подразделения для просмотра новостей, досок почета, мероприятий и опросов» для подразделения пользователя, изменение, удаление чужих комментариев к новости своего подразделения Добавление комментария, изменение и удаление своих комментариев не требует назначения роли.

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
7	Новостная лента (предприятие)	Основное право доступа: «Управлять новостями предприятия» из раздела «Приложения сайта», подраздела «Новости» Дополнительное право: «Добавить запись» из раздела «Контент сайта», подраздела «Новости»	Добавление (при наличии дополнительного права «Добавить запись»), изменение, удаление новости предприятия, изменение, удаление чужих комментариев к новости предприятия Добавление комментария, изменение и удаление своих комментариев не требует назначения роли.
8	Доска почета (подразделение)	«Управлять доской почета подразделения» из раздела «Приложения сайта», подраздела «Доски почета»	Добавление сотрудника на доску почета своего подразделения, или подразделения, которое определено в справочнике «Подразделения для просмотра новостей, досок почета, мероприятий и опросов» для подразделения пользователя, удаление сотрудника с доски почета своего подразделения, или подразделения, которое определено в справочнике «Подразделения для просмотра новостей, досок почета, мероприятий и опросов» для подразделения пользователя
9	Доска почета (предприятие)	«Управлять доской почета предприятия» из раздела «Приложения сайта», подраздела «Доски почета»	Добавление сотрудника на доску почета предприятия, удаление сотрудника с доски почета предприятия

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
10	Модератор форума	Назначаются все стандартные права из раздела «Контент сайта», подраздела «Форум» в частях «Доски сообщений», «Категория форума», «Сообщение форума», «Тема доски сообщений без полномочий». Также назначается право из раздела «Приложения сайта», подраздела «Форум» «Посмотреть»	Управлять форумом.
11	Начальник отдела	Основное право доступа: «Подтвердить отпуск» из раздела «Приложения сайта», подраздела «График отпусков». Дополнительные права: «Просмотр графиков отпусков всех подразделений предприятия» из раздела «Приложения сайта», подраздела «График отпусков».	Подтверждать отпуска сотрудников. При наличии дополнительного права просматривать графики отпусков других отделов. Просмотр графика отпусков своего отдела не требует доп. прав доступа.

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
12	Сотрудник отдела кадров (ввод данных по отсутствующим сотрудникам предприятия)	Основное право доступа: «Управлять данными по отсутствующим сотрудникам (Предприятие)» из раздела «Приложения сайта», подраздела «Данные по отсутствующим сотрудникам»	Ввод, удаление и просмотр данных об отсутствующих сотрудниках в целом по предприятию
13	Модератор вопросов в электронной приемной	Основное право доступа: «Управлять вопросами к руководству» из раздела «Приложения сайта», подраздела «Вопрос руководству»	Удаление любых вопросов сотрудников
14	Руководитель (ответы на вопросы сотрудников)	Основное право доступа: «Руководство предприятия (вопросы сотрудников)» из раздела «Приложения сайта», подраздела «Вопрос руководству»	Появляется в списке руководителей, которым возможно задавать вопросы в электронной приемной. Отвечать на заданные ему вопросы сотрудников.
15	Модератор записи на прием в электронной приемной	Основное право доступа: «Управлять расписанием записей на прием к руководству» из раздела «Приложения сайта», подраздела «Запись на прием»	Позволяет управлять возможными периодами записи на прием к тому или иному руководителю и удаление записи на прием любого сотрудника.

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
16	Руководитель, к которому можно записаться на прием	Основное право доступа: «Руководство предприятия (запись сотрудников на прием)» из раздела «Приложения сайта», подраздела «Запись на прием»	Появляется в списке руководителей, к которым можно записаться на прием в электронной приемной.
17	Сотрудник для записи других сотрудников на прием	Основное право доступа: «Управлять записью на прием другого сотрудника» из раздела «Приложения сайта», подраздела «Запись на прием»	Позволяет записать на прием любого другого сотрудника (запись на прием самого себя не требует дополнительных прав)
18	Управление шаблонами заявок пользователей	Основные права доступа: «Восстановить шаблон заявки», «Добавить шаблон заявки», «Изменить шаблон заявки», «Удалить шаблон заявки» из раздела «Приложения сайта», подраздела «Заявки пользователей»	Позволяет восстанавливать, добавлять, изменять, удалять шаблоны заявок при назначенных соответствующих правах доступа.
19	Статистика	Основные права доступа: «Посмотреть», «Просмотр обращений пользователей к модулям системы» из раздела «Приложения сайта», подраздела «Статистика»	Позволяет просмотреть кол-во обращений пользователей к модулям системы

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
20	Документы (модератор)	Назначаются все стандартные права из раздела «Контент сайта», подраздела «Documents and Media»	Позволяет управлять документами
21	Отдельные роли при необходимости разграничить права доступа на папки , подпапки и документы	На роль назначается право доступа «Посмотреть» для роли «Проектный офис (модератор)» и/или «Проектный офис. Название объекта (просмотр ролей для назначения прав доступа)»	Позволяет назначать на данную роль права доступа к папке, подпапке и т.д. Таким механизмом достигается при необходимости разграничение прав доступа на отдельные папки, подпапки и документы

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
22	Модератор оргструктуры	На роль добавляются следующие права доступа: «Добавить организацию», «Добавить пользователя» из раздела «Портал», подраздела «Общий». «Посмотреть» из раздела «Панель управления: Портал», подраздела «Пользователи и организации». «Назначить участников», «Посмотреть», «Сохранить», «Удалить», «Управлять подчиненными организациями», «Управлять пользователями» из раздела «Портал», подраздела «Пользователи и организации», части «Организация». «Посмотреть», «Сохранить», «Удалить» из раздела «Портал», подраздела «Пользователи и организации», части «Пользователь».	Модификация оргструктуры предприятия

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
23	Модератор блога	На роль назначается право доступа «Управлять блогами» из раздела «Приложения сайта» подраздела «Новости» , «Добавить запись» из раздела «Контент сайта» подраздела «Новости» части «Дневник»	Позволяет добавлять, изменять, удалять новости в своем блоге, редактировать и удалять комментарии любых пользователей (добавление, изменение и удаление своих комментариев не требует дополнительного права). Дополнительное право «Добавить запись» позволяет работать с черновиками своих новостей в своем блоге.
24	Аудит	Без прав доступа	Позволяет получить доступ к просмотру аудита системы. Доступ к подпункту меню «Аудит» в пункте «Администрирование»
25	Сотрудник отдела кадров (штатное расписание)	Основное право доступа: «Управлять штатным расписанием» из раздела «Приложения сайта», подраздела «Штатное расписание»	Позволяет управлять штатным расписанием по подразделениям
26	Сотрудник отдела кадров (календарь праздников)	Основное право доступа: «Добавить запись» из раздела «Приложения сайта», подраздела «Календарь праздников»	Позволяет настроить календарь праздников
27	Сотрудник отдела кадров (руководители)	Основное право доступа: «Посмотреть» из раздела «Приложения сайта», подраздела «Руководители»	Позволяет настроить руководителей разного уровня в структурных подразделениях

№ п/п	Роль	Необходимые права доступа	Разрешенное действие
28	Преподаватель	Основные права доступа: «Пользователь с ролью преподаватель», «Право добавлять/редактировать курс» из раздела «Приложения сайта», подраздела «Курсы»	Позволяет выбирать сотрудника в списке преподавателей и кураторов; добавлять, редактировать и наполнять курсы; просматривать отчет по успеваемости (доступ к пункту меню «Отчеты», подпункту «Отчет по успеваемости»); управлять бизнес кейсами (доступ к пункту меню «Библиотека», подпункту «Управления бизнес кейсами»)

Приложение 3. Группы исполнителей

№ п/п	Группа	Роли	Разрешенное действие
1	Группа пользователей (подразделение)	«Новостная лента (подразделение)», «Доска почета (подразделение)»	Работа с новостными лентами, досками почета своего подразделения
2	Группа пользователей (предприятие)	Все роли управления справочниками, «Календарь предприятия», «Новостная лента (предприятие)», «Доска почета (предприятие), «Модератор форума», «Модератор вопросов электронной приемной», «Модератор записи на прием в электронной приемной», «Управление шаблонами заявок пользователей», «Аудит», «Проектный офис (модератор).	Работа со справочниками, работа с календарями, новостными лентами, досками почета, форумом, вопросами сотрудников руководителям в электронной приемной, управлять записью на прием к тому или иному руководителю, управление шаблонами заявок пользователей, позволяет просмотреть кол-во обращений пользователей к модулям системы, управление документами.
3	Сотрудники отдела кадров	«Сотрудник отдела кадров (ввод данных по отсутствующим сотрудникам предприятия)» «Сотрудник для записи других сотрудников на прием», «Модератор оргструктуры».	Ввод и просмотр отсутствующих сотрудников в целом по предприятию. Позволяет записать на прием любого другого сотрудника. Модификация оргструктуры предприятия.

№ п/п	Группа	Роли	Разрешенное действие
4	Руководство предприятия	«Начальник отдела», «Руководитель, отвечающий на вопросы сотрудников», «Руководитель, к которому можно записаться на прием», «Модератор блога»	Подтверждать отпуска сотрудников, получать вопросы сотрудников/отвечать на вопросы сотрудников, получать электронную запись на прием, вести свой блог.
5	Преподаватели	«Преподаватель»	Быть преподавателем на курсе или разделе курса, куратором курса; добавлять, редактировать и наполнять курсы.
6	Сотрудники, объединенные в группы по признаку одинаковых прав доступа к одним и тем же документам.	Отдельные роли при необходимости разграничить права доступа на папки документов, подпапки и т.д.	Таким механизмом достигается при необходимости разграничение прав доступа на отдельные папки, подпапки документов или сами документы