|  |
| --- |
| **Объектно-ориентированная система Adem iRIS** |
| Вопросы интеграции с провайдером ролей Microsoft AzMan |
|  |
| Введение, краткий обзор провайдера ролей, конфигурирование клиентской части **Adem iRIS** и т. д. |
|  |
| **Чигвинцев И. Г.** |
| **10.07.2013** |
|  |

Оглавление

[Введение 3](#_Toc367448207)

[Провайдер ролей Microsoft AzMan 4](#_Toc367448208)

[Оснастка провайдера 4](#_Toc367448209)

[Установка провайдера 5](#_Toc367448210)

[Версии провайдера 5](#_Toc367448211)

[Хранилище данных авторизации 6](#_Toc367448212)

[Тип хранилища 6](#_Toc367448213)

[Версия схемы хранилища 7](#_Toc367448214)

[Настройка клиентской части Adem iRIS 9](#_Toc367448215)

[Windows-группы пользователей “ADEM Administrators” и “ADEM Users” 9](#_Toc367448216)

[Командная строка универсального клиента Adem.iRIS.Client.exe 10](#_Toc367448217)

[Ключ azman 10](#_Toc367448218)

[Ключ role 13](#_Toc367448219)

[Ролевой контент пользователя 17](#_Toc367448220)

[Структура файла конфигурации Adem.RoleProvider.dll.config 18](#_Toc367448221)

[XML-формат 18](#_Toc367448222)

[Скелетон 18](#_Toc367448223)

[Секция <Prepare> 20](#_Toc367448224)

[Секция <Scanning> 20](#_Toc367448225)

[Секция <Authorization> 21](#_Toc367448226)

[Секция <Checking> 22](#_Toc367448227)

[Особенности работы в локальных сетях 24](#_Toc367448228)

[Примерный алгоритм взаимодействия универсального клиента и провайдера ролей 25](#_Toc367448229)

[Работа с хранилищем данных авторизации, поставляемым с Adem iRIS 26](#_Toc367448230)

[Открытие хранилища 26](#_Toc367448231)

[Объекты хранилища 28](#_Toc367448232)

[Определения операций 29](#_Toc367448233)

[Определения задач 30](#_Toc367448234)

[Определения ролей 32](#_Toc367448235)

[Группы приложения 33](#_Toc367448236)

[Назначения ролей 35](#_Toc367448237)

[Интерфейс универсального клиента 36](#_Toc367448238)

[Примеры 38](#_Toc367448239)

[Пример 1. Создание и назначение роли с выборочным редактированием 38](#_Toc367448240)

[Пример 2. Создание и назначение роли только для поиска 50](#_Toc367448241)

[Интеграция с Active Directory 51](#_Toc367448242)

# Введение

Использование провайдера ролей позволяет придать прикладному программному обеспечению (**Adem iRIS**) дополнительную гибкость в области разграничения полномочий и распределения функциональности среди пользователей программы.

Дело в том что, разработчик не обязан знать, что за пользователи работают в локальной сети заказчика, и какая функциональность им необходима в тот или иной промежуток времени - это прерогатива администраторов **Adem iRIS** со стороны заказчика. Но, если предъявлены соответствующие требования, разработчик обязан предоставить некий механизм, позволяющий администраторам **Adem iRIS** решать возникающие проблемы. Таковым механизмом и является провайдер ролей.

С одной стороны, провайдер имеет знакомый администраторам сети интерфейс доступа к спискам пользователей и групп операционной системы. С другой стороны, провайдер (на уровне определения операций) максимально интегрирован с функциональностью **Adem iRIS**. Многообразие сочетаний (ролей) необходимой функциональности в совокупности с пользователями операционной системы и придаёт гибкость программному продукту. Некоторое количество (вполне очевидных) ролей заранее встроено в программное обеспечение и, в принципе, всегда может быть расширено. Но заранее сформировать роли на все случаи жизни фактически невозможно, поэтому провайдер через свой интерфейс позволяет администраторам **Adem iRIS** со стороны заказчика выполнить это в любое время без необходимости обращения к разработчику программного обеспечения.

# Провайдер ролей Microsoft AzMan

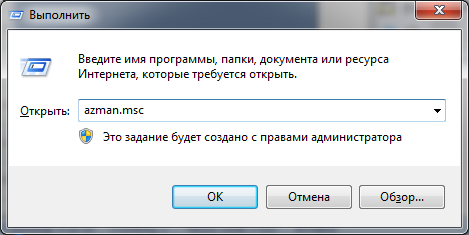
В русскоязычной транскрипции - Диспетчер авторизации или провайдер ролей.

В англоязычной транскрипции - Authorization manager (AzMan).

## Оснастка провайдера

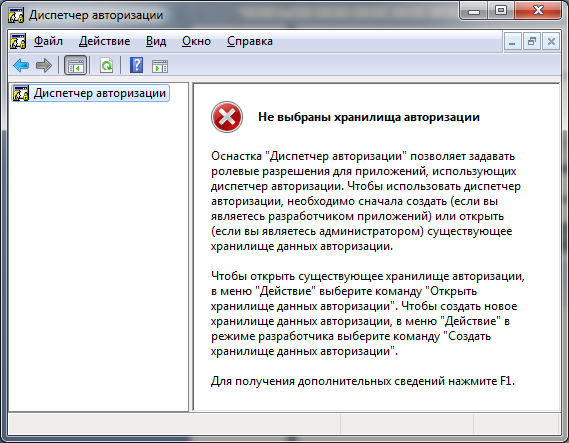
Для проверки работоспособности провайдера ролей на компьютере клиента необходимо выполнить команду, запускающую так называемую оснастку (snap-in) провайдера:

*Пуск Выполнить azman.msc*

**

*Рис. 1. Запуск провайдера ролей (диспетчера авторизации).*

После выполнения данной команды должно появиться окно провайдера ролей:



*Рис. 2. Исходное состояние провайдера ролей.*

Если появилось иное сообщение, то необходимо провести процедуру установки провайдера**.**

## Установка провайдера

Провайдер ролей **Microsoft AzMan**, начиная с **“Microsoft Windows 2003 Service Pack 1”** или выше, входит в состав операционных систем.

Если на компьютере клиента установлена операционная система **“Microsoft Windows XP Service Pack 2”** или выше, то необходимо предварительно установить пакет **“Microsoft Windows Server 2003 Administration Tools Pack Service Pack 1”** или выше (провайдер ролей входит в его состав).

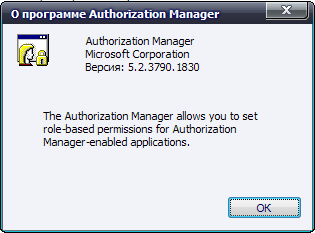
Пакет **”Microsoft Windows Server 2003 Administration Tools Pack Service Pack 1”** входит в поставку **Adem iRIS.** Также его можно получить, обратившись по ссылке <http://www.microsoft.com/downloads/details.aspx?FamilyID=e487f885-f0c7-436a-a392-25793a25bad7&DisplayLang=en>.

Более подробно об установке провайдера ролей **Microsoft AzMan** на различные операционные системы можно узнать, обратившись по ссылке <http://msdn.microsoft.com/en-us/library/ff649313.aspx>.

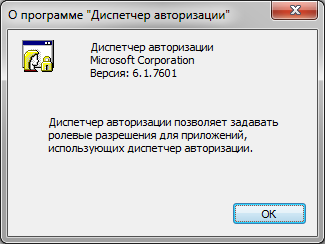
## 

## Версии провайдера

Версия провайдера ролей зависит от операционной системы, установленной на компьютере.



*Рис. 3. Версия провайдера ролей в операционной системе* ***Microsoft Windows XP****.*

**

*Рис. 4. Версия провайдера ролей в операционной системе* ***Microsoft Windows 7****.*

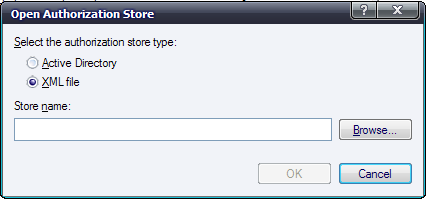
# Хранилище данных авторизации

Хранилище данных авторизации (в английской транскрипции – authorization store) можно рассматривать как некий набор данных, на основании которого провайдер ролей выдаёт заключение о доступности выполнения конкретным пользователем той или иной функции прикладного программного обеспечения.

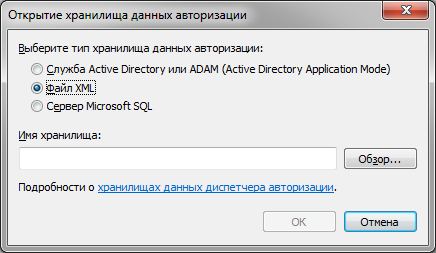
## 

## Тип хранилища

Возможности провайдера ролей в зависимости от его версии различаются, и это необходимо иметь в виду администраторам **Adem iRIS**.



*Рис. 5. Открытие хранилища данных авторизации в операционной системе* ***Microsoft Windows XP.***



*Рис. 6. Открытие хранилища данных авторизации в операционной системе* ***Microsoft Windows 7.***

Из рисунка 5 видно, что в операционной системе **Microsoft Windows XP** невозможно подключить хранилище данных авторизации, размещённое на сервере **Microsoft SQL.**

На данный момент система **Adem iRIS** работает:

1. С хранилищами данных авторизации, размещёнными в файлах XML.

В поставке клиентской части **Adem iRIS** имеются два хранилища:

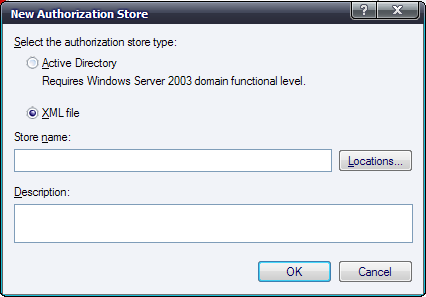
- русскоязычный вариант (используется по умолчанию): **<Клиент Adem iRIS>\ru-RU\Adem.RoleProvider.xml**,

- англоязычный вариант: **<Клиент Adem iRIS>\en-US\Adem.RoleProvider.xml**.

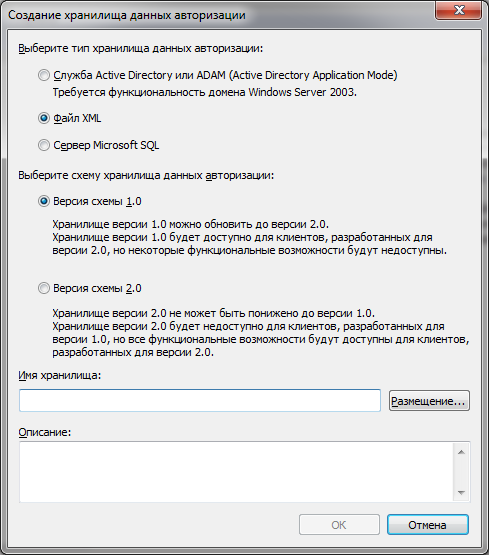
1. С хранилищами данных авторизации, размещёнными в структуре **Active Directory**. Таковые в поставке отсутствуют, поэтому их необходимо предварительно сформировать . В последней главе приведена подробная инструкция.

## Версия схемы хранилища

При создании нового хранилища данных авторизации с помощью провайдера ролей появляется диалог



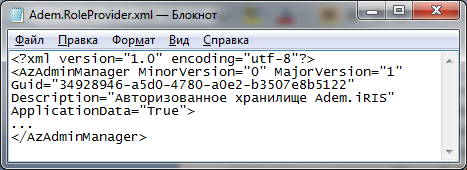
*Рис. 7. Создание нового хранилища данных авторизации в операционной системе* ***Microsoft Windows XP.***



*Рис. 8. Создание нового хранилища данных авторизации в операционной системе* ***Microsoft Windows 7.***

Как видно из рисунка 7, в операционной системе **Microsoft Windows XP** версия схемы хранилища не указывается (по умолчанию присваивается версия с номером 1). Если версия схемы хранилища не равна 1, то в операционной системе **Microsoft Windows XP** провайдер ролей работать не будет - появится сообщение об ошибке. Для обеспечения работоспособности **Adem iRIS** на клиентских компьютерах с различными операционными системами в поставляемых хранилищах **Adem.RoleProvider.xml** указана версия 1. В операционных системах **Microsoft Windows 7** желательно (но не обязательно) указать версию 2, так как с версией 1 провайдер ролей в итоге работает чуть медленнее.

В уже созданных хранилищах данных авторизации на основе файла XML версию схемы можно поменять с помощью любого текстового редактора (аргумент **MajorVersion** в секции **AzAdminManager**).



Версия схемы  
хранилища данных авторизации

*Рис. 9. Изменение версии схемы хранилища данных авторизации****.***

После редактирования файла XML не забудьте сохранить его именно в кодировке **UTF-8**.

# Настройка клиентской части Adem iRIS

Данная настройка сводится:

1. к редактированию файла конфигурации **Adem.RoleProvider.dll.config** с помощью любого текстового редактора (либо посредством запуска универсального клиента **Adem.iRIS.Client.exe** с ключом **azman**) - с целью установки различных режимов взаимодействия с провайдером ролей.

По умолчанию в этом файле все необходимые параметры уже установлены и должны поддерживать работу при использовании системы **Adem iRIS**:

* 1. на локальном компьютере,
  2. в “одноранговой” локальной сети (много списков пользователей),
  3. в локальной сети “с выделенным компьютером” (единый список пользователей) - с определёнными оговорками, которые будут рассмотрены ниже.

1. к редактированию хранилища данных авторизации посредством оснастки **azman.msc** провайдера ролей - с целью определения уровней доступа пользователей и назначения пользователям соответствующих ролей.

# Windows-группы пользователей “ADEM Administrators” и “ADEM Users”

В данной версии **Adem iRIS** (с ролевым контентом) принадлежность пользователя к Windows-группе пользователей **”ADEM Administrators”** влияет лишь на результат выполнения двух ключей (**azman** и **role**) командной строки универсального клиента **Adem.iRIS.Client.exe**. Так, например, управление отображением кнопки “Правка” в универсальном клиенте осуществляется через назначение пользователю соответствующей роли, а не признаком принадлежности к группе **”ADEM Administrators”**, как было в предыдущих версиях**.**

Также необходимо отметить, что (по умолчанию) в хранилище данных авторизации заранее осуществлены следующие назначения:

1. Пользователям, входящим в Windows-группу **”ADEM Administrators”**, назначена роль **“Администратор”**.
2. Пользователям, входящим в Windows-группу **”ADEM Users”**, назначена роль **“Пользователь”**.

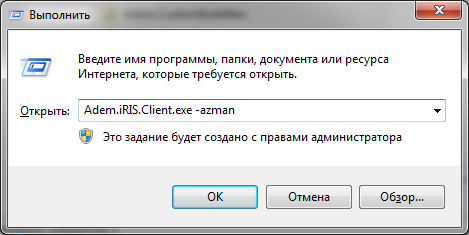
Всё, что касается принадлежности пользователей к данным Windows-группам, определено требованиями системы **ADEM CAD/CAM/CAPP**, в состав которой входит **Adem iRIS**, а не самой **Adem iRIS**.

# Командная строка универсального клиента Adem.iRIS.Client.exe

В командную строку универсального клиента **Adem.iRIS.Client.exe** добавлены три новых ключа: **azman**, **role** и **runas**.

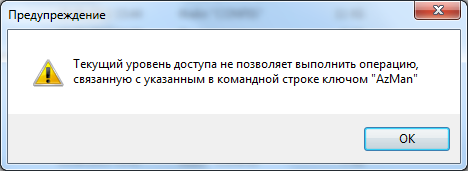
## Ключ azman

Данный ключ имеет более высокий приоритет по сравнению с другими ключами командной строки и используется для редактирования файла конфигурации **Adem.RoleProvider.dll.config** либо создания (или восстановления) хранилища данных авторизации.

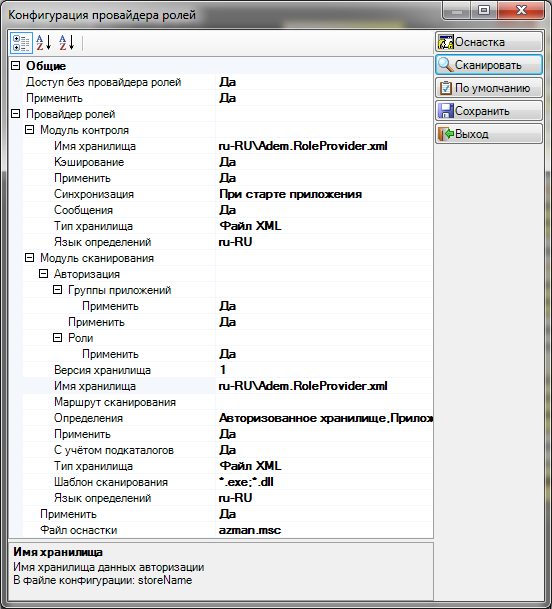


*Рис. 10. Запуск универсального клиента с ключом* ***azman.***

Как уже было отмечено выше, результат выполнения данной команды зависит от принадлежности пользователя к Windows-группе **”ADEM Administrators”**.



*Рис. 11. Результат выполнения ключа* ***azman*** *(пользователь не входит в состав* ***”ADEM Administrators”****).*



Запуск оснастки провайдера ролей

Имя соответствующего атрибута  
в файле конфигурации **Adem.RoleProvider.dll.config**

Если указанный файл не существует,  
то при сканировании он создаётся.  
  
Если файл был создан ранее,  
то при сканировании выполняется восстановление его содержимого.

Редактирование содержимого секции <Roles>  
на данный момент возможно лишь через текстовый редактор.

Редактирование содержимого секции <ApplicationGroups>  
на данный момент возможно лишь через текстовый редактор.

Сохранение внесённых изменений

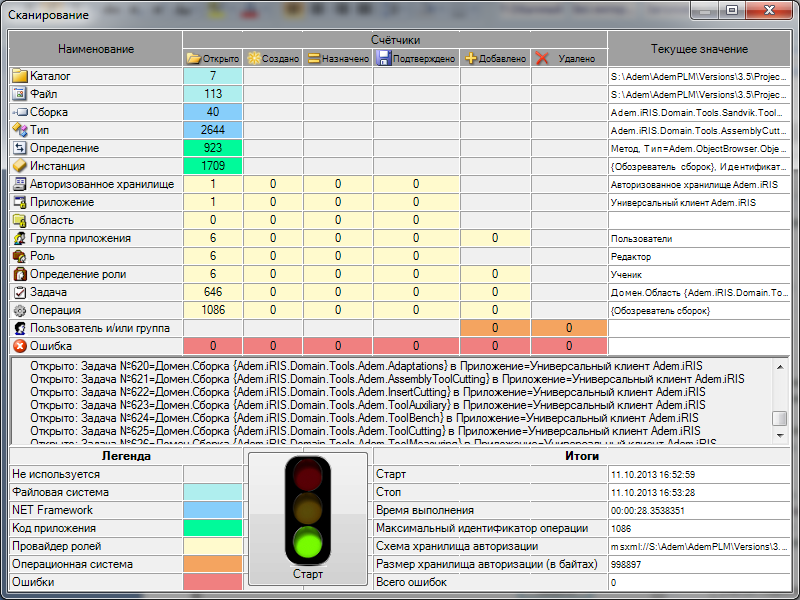
Установка значений по умолчанию

Создание или восстановление хранилища данных авторизации

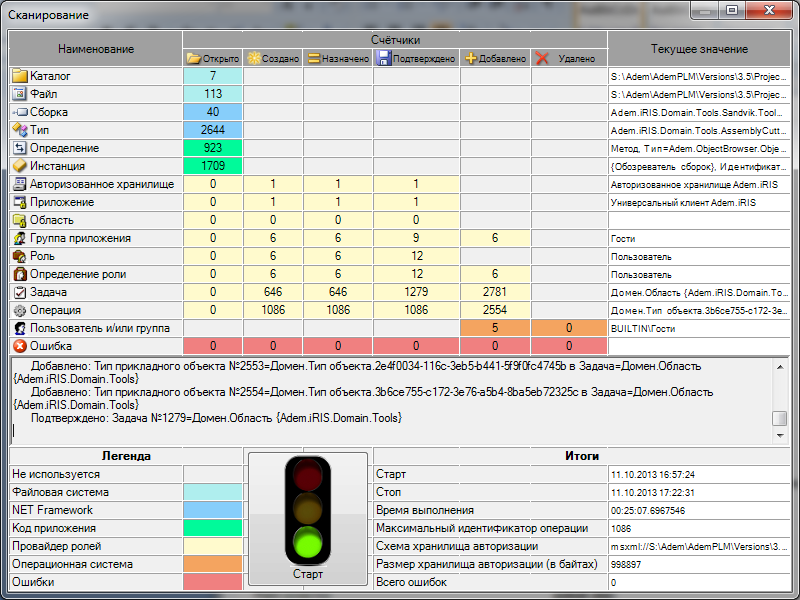
*Рис. 12. Результат выполнения ключа* ***azman*** *(пользователь входит в состав* ***”ADEM Administrators”****).*

На рисунке 12 приведено окно редактирования файла конфигурации **Adem.RoleProvider.dll.config**. Более подробно о содержимом данного файла будет рассказано ниже в отдельной главе.

При нажатии кнопки **Сканировать** запускается автоматический процесс создания (если файл отсутствует) либо восстановления хранилища данных авторизации. Результат приведён на рис. 13 и 14.



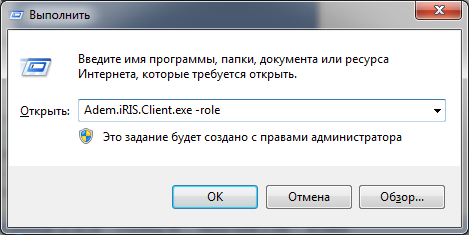
*Рис. 13. Результат выполнения процесса сканирования (восстановление хранилища).*



*Рис. 14. Результат выполнения процесса сканирования (создание хранилища).*

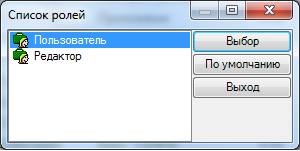
## Ключ role

Данный ключ предназначен для указания роли пользователя перед стартом универсального клиента.

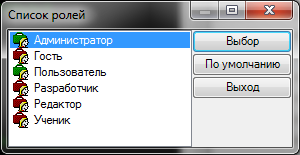
******

*Рис. 15. Запуск универсального клиента с ключом* ***role.***

Результат выполнения данной команды также зависит от принадлежности пользователя к Windows-группе **”ADEM Administrators”**.



*Рис. 16. Результат выполнения ключа* ***role*** *(пользователь не входит в состав* ***”ADEM Administrators”****).*



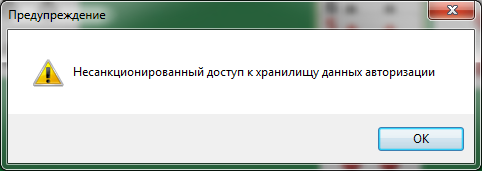
Роль, не имеющая привязки к пользователю в хранилище данных авторизации  
(иконка красного цвета)

Роль, имеющая привязку к пользователю  
в хранилище данных авторизации  
(иконка зелёного цвета)

*Рис. 17. Результат выполнения ключа* ***role*** *(пользователь входит в состав* ***”ADEM Administrators”****).*

На рисунке 16 приведены только доступные для пользователя роли, а на рисунке 17 приведены все роли, сформированные в хранилище данных авторизации.

Несмотря на отсутствие привязки, роль (например, ”Редактор” на рисунке 17) можно использовать - привязка в хранилище данных авторизации создастся автоматически (при условии, что файл хранилища доступен пользователю для редактирования на уровне файловой системы). По окончании работы с универсальным клиентом (при условии нормального завершения программы) привязка автоматически удалится из хранилища данных авторизации. Если же работа с универсальным клиентом завершится некорректно, то привязка останется в хранилище. В этом случае её можно удалить с помощью оснастки провайдера ролей. Если файл хранилища по каким-либо причинам (например, установлен атрибут **”Только чтение”**) недоступен пользователю для редактирования, то появится сообщение:

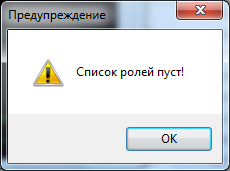


*Рис. 18. Предупреждение о несанкционированном доступе.*

Как видно, например, из рисунков 16 и 17, у пользователя может быть одновременно несколько ролей, имеющих привязку. В данной ситуации (если в командной строке ключ **role** не указывать, либо в диалоге списка ролей нажать кнопку **”По умолчанию”)** так называемый ролевой контент пользователя будет состоять именно из этих нескольких ролей, а доступ провайдером ролей будет определяться по принципу логического суммирования ”ИЛИ”. Вообще говоря, нежелательно допускать привязку к пользователю нескольких ролей из-за серьёзно усложняющейся логики определения доступа, что при невнимательном редактировании хранилища данных авторизации может привести к неумышленному предоставлению возможности выполнения функции, не предназначенной для пользователя.

Если пользователь не входит в состав группы **”Adem Administators”** и для него определена только одна роль, то выполнение ключа **role** проигнорируется (диалог списка ролей не появится, так как не из чего выбирать), а универсальный клиент продолжит работу.

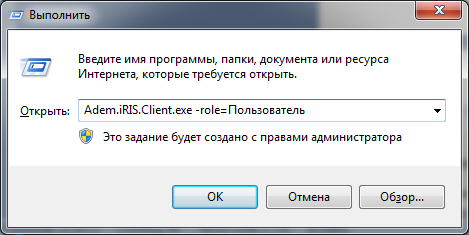
Если пользователь не входит в состав группы **”Adem Administators”** и для него не определено ни одной роли, то универсальный клиент прерывается и выводится предупреждение:



*Рис. 19. Список ролей не определён для пользователя.*

Аналогичное сообщение появляется и при полном отсутствии ролей в хранилище данных авторизации.

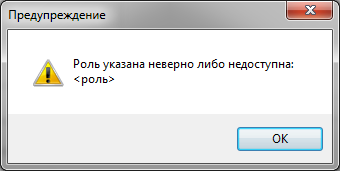
У ключа **role** существует ещё один синтаксис:



*Рис. 20. Запуск универсального клиента с указанием конкретной роли****.***

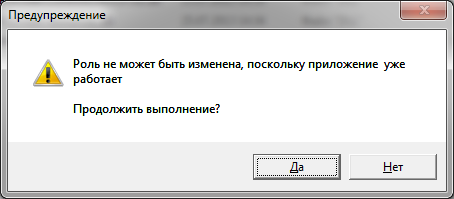
В данном случае диалог списка ролей не появится (выбор роли уже выполнен в командной строке).

Если указана роль, отсутствующая в списке хранилища данных авторизации, либо является недоступной для пользователя, то универсальный клиент прерывается и появляется следующее предупреждение:



*Рис. 21. Ошибочное указание роли в командной строке****.***

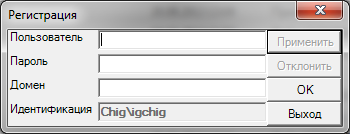
Если универсальный клиент стартует с ключом **role** (с указанием роли или без указания) и с ключом **hosting=true** (используется по умолчанию), а хост уже размещён в оперативной памяти, то при попытке изменить роль появится предупреждение:



*Рис. 22. Неудачная попытка изменения роли****.***

## Ключ runas

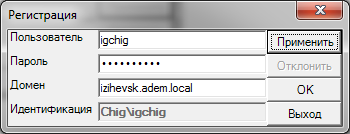
Данный ключ предназначен для смены пользователя перед стартом универсального клиента. Этот ключ может быть полезен в случаях с доменной организацией компьютерной сети.



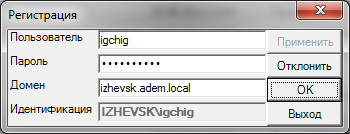
Завершение работы

Кнопка используется для отмены  
последней регистрации пользователя

После ввода имени пользователя  
 кнопка **Применить** становится доступной  
и можно выполнить регистрацию



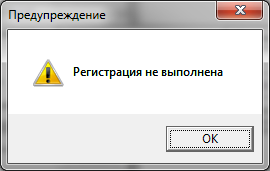
Для регистрации на локальном сервере  
поле **Домен** можно не заполнять



После успешной регистрации кнопка **Отклонить** становится доступной  
и можно последнюю регистрацию отменить, вернувшись к исходному значению

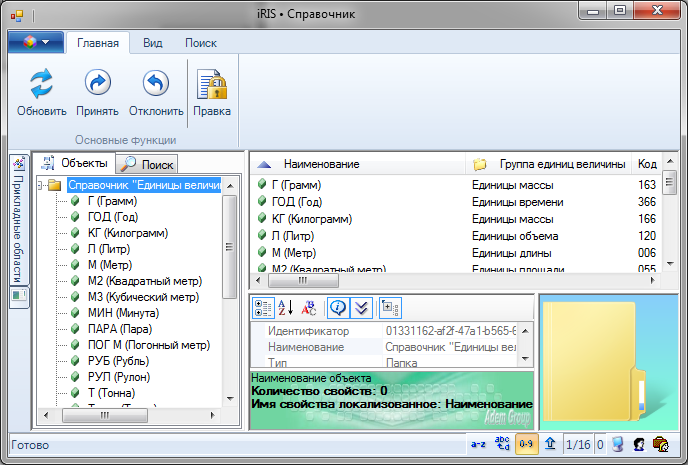
Продолжение работы в качестве пользователя,  
указанного в поле **Идентификация**

Текущая идентификация пользователя



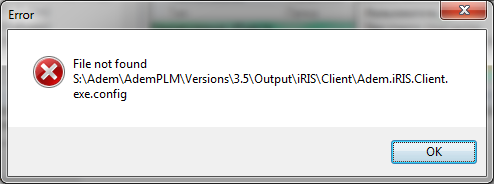
При неудачной регистрации  
 появляется соответствующее предупреждение

После успешной регистрации и загрузки универсального клиента:



**Пользователь**   
При старте: Chig\igchig  
При выполнении: IZHEVSK\igchig

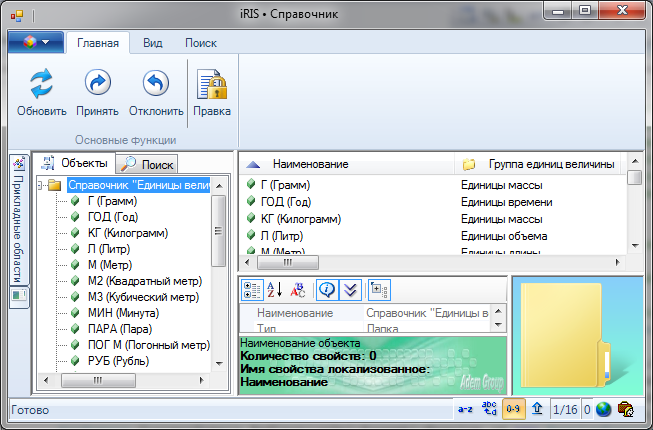
После успешной регистрации не исключено появление и такого сообщения:



Это связано с тем, что перед сменой пользователя программа была запущена с сетевого подключения (логический диск S:), а у нового пользователя такое подключение отсутствует. Необходимо иметь ввиду, что данная регистрация пользователя не восстанавливает сетевые подключения.

# Ролевой контент пользователя

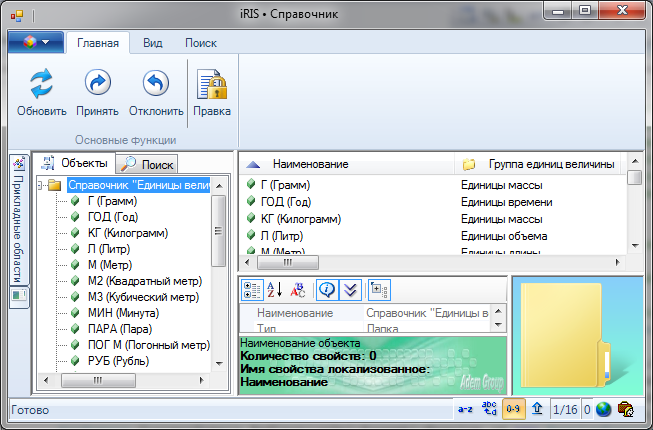
После успешной загрузки универсального клиента можно посмотреть, какой в итоге пользователю назначен ролевой контент:



**Ролевой контент**  
Администратор  
Пользователь

*Рис. 23. Универсальный клиент с назначенным ролевым контентом****.***

Если в файле конфигурации провайдер ролей отключен, то ролевой контент не задаётся:



**Ролевой контент не определён**

*Рис. 24. Универсальный клиент, не имеющий ролевого контента****.***

# Структура файла конфигурации Adem.RoleProvider.dll.config

## XML-формат

Файл конфигурации хранится в формате XML (Extensible Markup Language), позволяющем сохранять иерархическую структуру данных. XML-формат удобно использовать, поскольку при объектно-ориентированном подходе в программировании сохранённые данные можно фактически напрямую, без лишних затрат на преобразование, отобразить в объектах соответствующих классов.

Данный формат использует синтаксис так называемых тэгов (в английской транскрипции – tag):

1. тэг, не являющийся иерархической структурой, имеет синтаксис <ИмяТэга/>
2. тэг, содержащий иерархическую структуру, имеет синтаксис <ИмяТэга></ИмяТэга>
3. комментарий имеет синтаксис **<!-- Текст -->**
4. атрибуты тэга имеют синтаксис ИмяАтрибута=”Значение”

Как правило, в файлах формата XML требуется редактировать лишь те места, которые, согласно синтаксису, соответствуют полю ”Значение”**.**

Файл конфигурации можно редактировать любым текстовым редактором (важно лишь сохранить в кодировке **UTF-8**), либо с помощью универсального клиента, запускаемого с ключом **azman.**

## Скелетон

Скелетоном (в английской транскрипции – skeleton) будем называть полную структуру файла конфигурации. Поскольку, во-первых, некоторые атрибуты могут быть помечены разработчиком как необязательные; во-вторых, часть значений атрибутов могут совпадать с заданными по умолчанию значениями, то в итоге реально используемый файл конфигурации может значительно отличаться от его скелетона. На рисунке 26 приведена полная структура файла конфигурации с используемыми по умолчанию значениями атрибутов.

Всё, что находится за пределами тэга <RoleProviderSection></RoleProviderSection>, является обязательной частью и редактированию не подлежит.

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<configSections>

<section name="RoleProviderSection"

type="Adem.RoleProvider.RoleProviderSection,Adem.RoleProvider"/>

</configSections>

<!-- Здесь расположена редактируемая часть файла конфигурации -->

</configuration>

*Рис. 25. Не подлежащая редактированию часть файла конфигурации****.***

Атрибут enabled используется как некий переключатель, разрешающий или запрещающий обработку данного тэга и всех вложенных (важно!) в него тэгов. Данный атрибут аналогично используется во всех других тэгах, по умолчанию имеет значение ”true” и является необязательным. Атрибут enabled=”false” для тэга <RoleProviderSection> означает, что всё взаимодействие с провайдерами ролей будет отключено, а доступ для пользователей будет определяться атрибутом checkedByDefault (по умолчанию имеет значение ”true” и также является необязательным). При checkedByDefault=”true” всё для пользователей разрешено, при checkedByDefault=”false” всё запрещено.

Вообще говоря, провайдеров ролей может быть задействовано много - от разных поставщиков и с различной функциональностью. Так как мы рассматриваем только один провайдер ролей, то и <RoleProviderSection> содержит только один тэг - <AzManProvider>, атрибут которого с именем snapIn (по умолчанию имеет значение ”azman.msc” и является необязательным) определяет вызов так называемой оснастки, т. е. запускает на выполнение программу провайдера ролей. Атрибут enabled тэга <AzManProvider> разрешает или запрещает работу уже конкретного провайдера ролей. В свою очередь, тэг <AzManProvider> содержит три тэга (или секции) – их рассмотрим в отдельности.

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<configSections>

<section name="RoleProviderSection"

type="Adem.RoleProvider.RoleProviderSection,Adem.RoleProvider"/>

</configSections>

<RoleProviderSection enabled="true" checkedByDefault="true">

<AzManProvider enabled="true" snapIn="azman.msc">

<Prepare enabled="true" prefixName="AzName" prefixDescription="AzDescription"/>

<Scanning enabled="true" path="" pattern="\*.exe;\*.dll" subdirectories="true"

storeName="ru-RU\Adem.RoleProvider.xml" storeMedium="msxml" storeVersion="1"

culture="ru-RU" definitions=“Авторизованное хранилище, Типы прикладных объектов,

Приложения, Группы приложений,

Пользователи и группы пользователей,

Назначения ролей, Определения ролей,

Области задач, Определения задач,

Определения операций, Определения методов”>

<AuthorizationStoreByDefault enabled="true" identifier=""

type="Adem.AzMan.ClientAzManAuthorizationStore,Adem.RoleProvider"/>

<ApplicationByDefault enabled="true" identifier=""

type="Adem.AzMan.ClientAzManApplication,Adem.RoleProvider"/>

<ScopeByDefault enabled="false" identifier="" type=""/>

<Authorization enabled="true">

<ApplicationGroups enabled="true">

<ApplicationGroup enabled="true" identifier=""

type="Adem.AzMan.AdministratorsAzManApplicationGroup,Adem.RoleProvider">

<Identity enabled="true" mode="Include" name="BUILTIN\Администраторы"/>

<Identity enabled="true" mode="Include" name="ADEM Administrators"/>

</ApplicationGroup>

<ApplicationGroup enabled="true" identifier=""

type="Adem.AzMan.UsersAzManApplicationGroup,Adem.RoleProvider">

<Identity enabled="true" mode="Include" name="BUILTIN\Пользователи"/>

<Identity enabled="true" mode="Include" name="ADEM Users"/>

</ApplicationGroup>

<ApplicationGroup enabled="true" identifier=""

type="Adem.AzMan.GuestsAzManApplicationGroup,Adem.RoleProvider">

<Identity enabled="true" mode="Include" name="BUILTIN\Гости"/>

</ApplicationGroup>

<ApplicationGroup enabled="true" identifier=""

type="Adem.AzMan.EditorsAzManApplicationGroup,Adem.RoleProvider"/>

<ApplicationGroup enabled="true" identifier=""

type="Adem.AzMan.DisciplesAzManApplicationGroup,Adem.RoleProvider"/>

<ApplicationGroup enabled="true" identifier=""

type="Adem.AzMan.DevelopersAzManApplicationGroup,Adem.RoleProvider"/>

</ApplicationGroups>

<Roles enabled="true">

<Role enabled="true" identifier=""

type="Adem.AzMan.AdministratorAzManRole,Adem.RoleProvider"/>

<Role enabled="true" identifier=""

type="Adem.AzMan.UserAzManRole,Adem.RoleProvider"/>

<Role enabled="true" identifier=""

type="Adem.AzMan.GuestAzManRole,Adem.RoleProvider"/>

<Role enabled="true" identifier=""

type="Adem.AzMan.EditorAzManRole,Adem.RoleProvider"/>

<Role enabled="true" identifier=""

type="Adem.AzMan.DiscipleAzManRole,Adem.RoleProvider"/>

<Role enabled="true" identifier=""

type="Adem.AzMan.DeveloperAzManRole,Adem.RoleProvider"/>

</Roles>

</Authorization>

</Scanning>

<Checking enabled="true" checkMode="Startup" caching="true" showMessage="true"

storeName="ru-RU\Adem.RoleProvider.xml" storeMedium="msxml" culture="ru-RU">

<AuthorizationStoreByDefault enabled="true" identifier=""

type="Adem.AzMan.ClientAzManAuthorizationStore,Adem.RoleProvider"/>

<ApplicationByDefault enabled="true" identifier=""

type="Adem.AzMan.ClientAzManApplication,Adem.RoleProvider"/>

<ScopeByDefault enabled="false" identifier="" type=""/>

</Checking>

</AzManProvider>

</RoleProviderSection>

</configuration>

*Рис. 26. Скелетон файла конфигурации (полная структура)****.***

## Секция <Prepare>

Данная секция предназначена только для разработчиков программного обеспечения. Атрибуты prefixName и prefixDescription используются для извлечения из ресурсных файлов локализованных текстовых фрагментов при формировании определений операций, задач, ролей и т. п. Оба атрибута являются необязательными.

## Секция <Scanning>

Настройки данной секции применяются только при создании либо восстановлении хранилища данных авторизации (при нажатии кнопки **“Сканировать”** в редакторе конфигурации провайдера ролей).

|  |  |  |  |
| --- | --- | --- | --- |
| Атрибут | Значение по умолчанию | Допустимые значения | Описание |
| enabled | “true” | “true”  “false” | Разрешается или запрещается сканирование файлов. |
| path | “” | Корректное имя каталога | Маршрут сканирования файлов (по умолчанию это каталог размещения клиентской части **Adem iRIS**). |
| pattern | “\*.exe;\*.dll” |  | Типы сканируемых файлов (по умолчанию это исполняемые файлы и файлы динамически загружаемых библиотек). |
| subdirectories | “true” | “true”  “false” | Признак сканирования подкаталогов. |
| storeVersion | "1" | "1"  "2" | Версия хранилища данных авторизации (применяется только при создании хранилища, но не при восстановлении).  Для совместимости с **Windows XP** необходимо указать “1”. |
| storeMedium | "msxml" | "msxml"  "mssql"  "msldap" | Среда размещения хранилища данных авторизации и применяется только при создании хранилища. Значения "mssql" и "msldap" пока использовать нельзя. |
| storeName | "ru-RU\Adem.RoleProvider.xml" | Корректное имя файла | Файл хранилища данных авторизации для сохранения результатов сканирования. |
| culture | "ru-RU" | "ru-RU"  "en-US" | Язык формирования определений.  “ru-RU” - русскоязычный вариант  “en-US” - англоязычный вариант |
| definitions | “Авторизованное хранилище, Типы прикладных объектов,  Приложения, Группы приложений,  Пользователи и группы пользователей, Назначения ролей, Определения ролей, Области задач, Определения задач, Определения операций,  Определения методов” | Любое  (через запятую) сочетание из перечисленных значений в графе “Значение по умолчанию” | Перечень определений (в терминологии провайдера ролей), которые генерируются в процессе сканирования файлов и в итоге составляют содержимое хранилища данных авторизации. |

Все перечисленные в таблице атрибуты не являются обязательными.

Секции <AuthorizationStoreByDefault>, <ApplicationByDefault> и <ScopeByDefault> также предназначены только для разработчиков программного обеспечения. Атрибут type определяет соответственно тип авторизованного хранилища по умолчанию, тип приложения по умолчанию и тип области задач по умолчанию. Атрибут identifier используется для идентификации инстанции объекта, производного от указанных типов.

Секция <Authorization> входит в состав секции <Scanning>, но её описание специально выделено в отдельную главу.

## Секция <Authorization>

Данная секция разделена в свою очередь на две секции: <ApplicationGroups> и <Roles>. Обе эти секции являются коллекциями групп приложения (тэги <ApplicationGroup>) и ролей (тэги <Role>) соответственно.

Набор тэгов <ApplicationGroup> представляет собой реализованный в данной версии **Adem iRIS** набор групп приложения:

|  |  |  |
| --- | --- | --- |
| Наименование | Тип | Описание |
| Разработчики | DevelopersAzManApplicationGroup | Предоставляется максимальный доступ. |
| Администраторы | AdministratorsAzManApplicationGroup | Предоставляется максимальный доступ, за исключением доступа к информации, необходимой разработчикам программного обеспечения. |
| Редакторы | EditorsAzManApplicationGroup | То же, что и у администраторов, за исключением служебной информации и некоторых элементов управления. |
| Пользователи | UsersAzManApplicationGroup | То же, что и у редакторов, но объекты прикладной области доступны только для выбора и просмотра. |
| Ученики | DisciplesAzManApplicationGroup | То же, что и у редакторов, за исключением возможности сдачи на сервер созданных либо модифицированных объектов прикладной области . |
| Гости | GuestsAzManApplicationGroup | Полное отсутствие доступа. |

Необходимо отметить, что группа приложения это не Windows-группа, а группа, реализованная именнно в провайдере ролей для предоставления дополнительной гибкости в управлении доступом пользователей. Атрибуты type и identifier тэгов <ApplicationGroup> предназначены для редактирования только разработчиками программного обеспечения. В свою очередь, каждый из тэгов <ApplicationGroup> содержит коллекцию тэгов <Identity>.

Набор тэгов <Role> представляет собой реализованный в данной версии **Adem iRIS** набор ролей:

|  |  |  |
| --- | --- | --- |
| Наименование | Тип | Описание |
| Разработчик | DeveloperAzManRole | Предоставляется максимальный доступ. |
| Администратор | AdministratorAzManRole | Предоставляется максимальный доступ, за исключением доступа к информации, необходимой разработчикам программного обеспечения. |
| Редактор | EditorAzManRole | То же, что и у администраторов, за исключением служебной информации и некоторых элементов управления. |
| Пользователь | UserAzManRole | То же, что и у редакторов, но объекты прикладной области доступны только для выбора и просмотра. |
| Ученик | DiscipleAzManRole | То же, что и у редакторов, за исключением возможности сдачи на сервер созданных либо модифицированных объектов прикладной области . |
| Гость | GuestAzManRole | Полное отсутствие доступа. |

Атрибуты type и identifier тэгов <Role> предназначены для редактирования только разработчиками программного обеспечения. Каждый из тэгов <Role> также содержит коллекцию тэгов <Identity>.

Тэг <Identity> используется для привязки пользователя или Windows-группы пользователей к сформированным в хранилище данных авторизации ролям либо группам приложения.

|  |  |  |  |
| --- | --- | --- | --- |
| Атрибут | Значение по умолчанию | Допустимые значения | Описание |
| name | “” | Корректное имя | Имя пользователя в операционной системе либо имя Windows-группы пользователей. |
| mode | “Include” | “Include”  “Exclude” | Включение либо исключение из формируемого списка. |
| enabled | “true” | “true”  “false” | Разрешает либо запрещает обработку текущего тэга. |

Все перечисленные в таблице атрибуты, за исключением атрибута name, являются необязательными.

Из рисунка 24 видно, что некоторые привязки по умолчанию уже выполнены.

|  |  |  |  |
| --- | --- | --- | --- |
| Группа приложения | Windows-группа либо пользователь | Атрибут mode | Описание |
| Администраторы | BUILTIN\Administrators ADEM Administrators | “Include” | Все пользователи, входящие в указанные Windows-группы, в универсальном клиенте получат доступ, соответствующий группе приложения “Администраторы”. |
| Пользователи | BUILTIN\Administrators ADEM Administrators | “Include” | Все пользователи, входящие в указанные Windows-группы, в универсальном клиенте получат доступ, соответствующий группе приложения “Пользователи”. |
| Гости | BUILTIN\Guests | “Include” | Все пользователи, входящие в указанную Windows-группу, в универсальном клиенте получат доступ, соответствующий группе приложения “Гости”. |

## Секция <Checking>

Настройки данной секции используются непосредственно в процессе работы универсального клиента.

|  |  |  |  |
| --- | --- | --- | --- |
| Атрибут | Значение по умолчанию | Допустимые значения | Описание |
| enabled | “true” | “true”  “false” | Разрешается или запрещается выполнение контроля доступа. |
| checkMode | “Startup” | “Startup”  “Runtime” | У провайдера ролей есть свой внутренний кэш. При значении “Startup” этот кэш в процессе работы универсального клиента не обновляется. При значении “Runtime” соблюдается полная синхронизация данных, но за счёт обновления кэша в момент выполнении контроля доступа, что приводит к замедлению работы. |
| caching | “true” | “true”  “false” | Разрешается или запрещается кэширование результатов контроля доступа. Кэширование позволяет ускорить процесс прохождения контроля за счёт того, что при повторных действиях обращение к провайдеру ролей не выполняется, а результат контроля доступа берётся из внутреннего кэша универсального клиента. |
| showMessage | “true” | “true”  “false” | Разрешается или запрещается вывод сообщений об ограничении доступа. |
| storeMedium | "msxml" | "msxml"  "mssql"  "msldap" | Среда размещения хранилища данных авторизации. Значения "mssql" и "msldap" пока использовать нельзя. |
| storeName | "ru-RU\Adem.RoleProvider.xml" | Корректное имя файла | Файл хранилища данных авторизации, используемый при контроле доступа. |
| culture | "ru-RU" | "ru-RU"  "en-US" | Язык определений в хранилище данных авторизации.  “ru-RU” - русскоязычный вариант  “en-US” - англоязычный вариант |

Секции <AuthorizationStoreByDefault>, <ApplicationByDefault> и <ScopeByDefault> предназначены только для разработчиков программного обеспечения.

*Рис. 27. Файл конфигурации (исключены все необязательные атрибуты при условии, что их значения совпадают с заданными по умолчанию значениями)****.***

<?xml version="1.0" encoding="utf-8" ?>

<configuration>

<configSections>

<section name="RoleProviderSection"

type="Adem.RoleProvider.RoleProviderSection,Adem.RoleProvider"/>

</configSections>

<RoleProviderSection>

<AzManProvider>

<Scanning>

<Authorization>

<ApplicationGroups>

<ApplicationGroup

type="Adem.AzMan.AdministratorsAzManApplicationGroup,Adem.RoleProvider">

<Identity name="BUILTIN\Администраторы"/>

<Identity name="ADEM Administrators"/>

</ApplicationGroup>

<ApplicationGroup

type="Adem.AzMan.UsersAzManApplicationGroup,Adem.RoleProvider">

<Identity name="BUILTIN\Пользователи"/>

<Identity name="ADEM Users"/>

</ApplicationGroup>

<ApplicationGroup

type="Adem.AzMan.GuestsAzManApplicationGroup,Adem.RoleProvider">

<Identity name="BUILTIN\Гости"/>

</ApplicationGroup>

<ApplicationGroup

type="Adem.AzMan.EditorsAzManApplicationGroup,Adem.RoleProvider"/>

<ApplicationGroup

type="Adem.AzMan.DisciplesAzManApplicationGroup,Adem.RoleProvider"/>

<ApplicationGroup

type="Adem.AzMan.DevelopersAzManApplicationGroup,Adem.RoleProvider"/>

</ApplicationGroups>

<Roles>

<Role type="Adem.AzMan.AdministratorAzManRole,Adem.RoleProvider"/>

<Role type="Adem.AzMan.UserAzManRole,Adem.RoleProvider"/>

<Role type="Adem.AzMan.GuestAzManRole,Adem.RoleProvider"/>

<Role type="Adem.AzMan.EditorAzManRole,Adem.RoleProvider"/>

<Role type="Adem.AzMan.DiscipleAzManRole,Adem.RoleProvider"/>

<Role type="Adem.AzMan.DeveloperAzManRole,Adem.RoleProvider"/>

</Roles>

</Authorization>

</Scanning>

<Checking />

</AzManProvider>

</RoleProviderSection>

</configuration>

# Особенности работы в локальных сетях

Рассмотрим два основных типа локальных сетей с точки зрения хранения списков пользователей и групп:

1. “Одноранговая” - списки пользователей хранятся на каждом компьютере и могут существенно отличаться друг от друга;
2. “С выделенным сервером” - используется единый список пользователей, хранящийся на сервере.

Обратившись к рисункам 5 и 6, делаем вывод, что в случаях размещения хранилища данных авторизации в средах **“Active Directory”** или **“SQL Server”** мы будем взаимодействовать с единым хранилищем, а в случае **“Файл XML”** у нас есть два варианта:

1. Размещение хранилища на каждом компьютере:
2. Размещение хранилища на компьютере, выполняющем роль файлового сервера.

Поскольку провайдер ролей работает непосредственно со списками пользователей, то в итоге мы должны учитывать все возможные комбинации:

1. Децентрализованные списки пользователей и децентрализованные хранилища данных авторизации (по умолчанию в настройках используется именно этот вариант из соображений максимальной совместимости),
2. Централизованный список пользователей и децентрализованные хранилища данных авторизации,
3. Децентрализованные списки пользователей и централизованное хранилище данных авторизации (по-видимому, самый сложный вариант, поскольку в настройках необходимо будет указывать ещё и имена компьютеров),
4. Централизованный список пользователей и централизованное хранилище данных авторизации (лучший выбор с точки зрения администрирования сетей и управления доступом пользователей).

Отметим ещё раз, что:

1. на данный момент **Adem iRIS** может работать пока только со средой **“Файл XML”**,
2. настройка размещения файла определяется значением атрибута storeName в секции <Checking> (см. рисунок 26),
3. по умолчанию хранилища данных децентрализованы (указан относительный маршрут),
4. при таком подходе хранилища данных авторизации не являются защищёнными от несанкционированного доступа.

Для использования централизованного хранилища данных авторизации необходимо указать абсолютный маршрут к файлу, предварительно поместив его на файловый сервер, например:

<Checking storeName=”\\FileServ\Storage\ru-RU\Adem.RoleProvider.xml”/>

Поскольку речь идёт именно о файловом сервере, то доступ к файлу необходимо определить на уровне файловой системы (для всех, за исключением администраторов, можно установить атрибут **“Только чтение”**).

# Примерный алгоритм взаимодействия универсального клиента и провайдера ролей

Атрибут  
**culture**

Нет

Формирование  
имени операции

Атрибут  
**caching**

Атрибут  
**culture**

Атрибут  
**definitions**

Настройки  
процесса  
в секции  
**Checking**файла  
конфигурации

Вывод результатов

Обращение к файлу

Сканирование файлов

**Провайдер ролей  
Microsoft AzMan**

Режим Startup?

Хранилище данных авторизации

Создание или открытие:  
  
 хранилища авторизации  
 приложений  
 операций  
 задач  
 определений ролей  
 групп приложений  
 назначений ролей

Сканирование типов

Конец функции  
**Sample**

Конец

Начало

Да

Нет

Вывод сообщений разрешён?

Да

Выполнение функции **Sample**

Нет

Да

Доступ разрешён?

Да

Добавление результата  
в кэш-таблицу

Кэширование разрешено?

Нет

Нет

Результат есть  
в кэш-таблице?

Да

Кэширование разрешено?

Формирование  
имени операции

**Процесс  
контроля доступа**

**Процесс сканирования**

Начало функции  
**Sample**

Нет

Контроль доступа реализован?

Да

Вывод сообщения об ограничении доступа

**Универсальный клиент Adem iRIS**

**COM-объект**

Сканирование каталогов

Атрибут  
**pattern**

Атрибут  
**checkMode**

Нет

Атрибут **storeName**секции **Checking**

Да

Кэш-  
таблица

Есть указанная операция?

Атрибут  
**caching**

Нет

Да

Контроль доступа по имени операции

Атрибут  
**showMessage**

**Оснастка  
azman.msc**

Диалог  
**Открыть хранилище данных авторизации**

Интерфейс

См. рис. 33

Кэш-  
таблица

Настройки процесса  
в секции  
**Scanning**файла конфигурации

Процесс активируется  
по кнопке **“Сканирование”**при запуске  
универсального клиента  
с ключом **azman**

Атрибуты  
**path**  
**subdirectories**

Обращение к файлу

Application.pngOperation.pngTask.pngRoleDefinition.pngGroup.pngStore.pngRole.png

Атрибут  
**storeName  
c**екции **Scanning**

**Файловая система**

*Рис. 28. Примерный алгоритм взаимодействия****.***

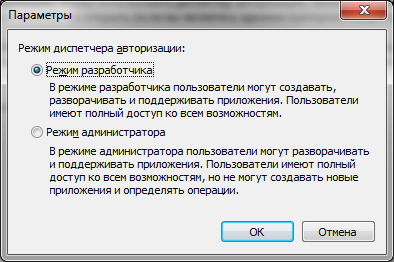
# Работа с хранилищем данных авторизации, поставляемым с Adem iRIS

Как уже отмечалось ранее, в поставку **Adem iRIS** включены заранее сгенерированные хранилища данных авторизации (на русском и английском языках). Наступил момент ознакомиться с их содержимым.

## Открытие хранилища

1. Запускаем оснастку провайдера ролей, как показано на рисунке 1
2. В окне диспетчера авторизации (рисунок 2) выполняем команду:

*Меню Действие Параметры…*

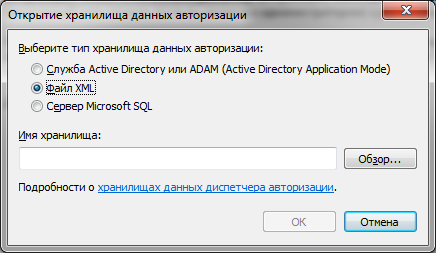
1. В окне **“Параметры”** (рисунок 29) выбираем **“Режим разработчика”** и нажимаем **“ОК”** ****

*Рис. 29. Выбор режима диспетчера авторизации****.***

1. Далее выполняем команду:

*Меню Действие Открыть хранилище данных авторизации…*

1. В окне **“Открытие хранилища данных авторизации”** (рисунок 30) выбираем **“Файл XML”** и нажимаем кнопку **“Обзор…”**



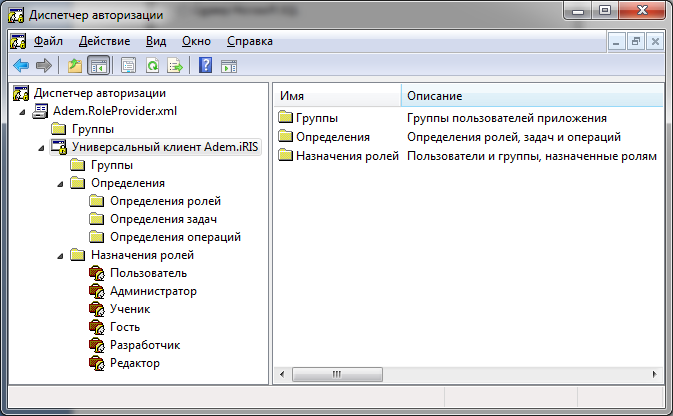
*Рис. 30. Открытие хранилища данных авторизации****.***

1. По маршруту  **<Клиент Adem iRIS>\ru-RU** выбираем файл **Adem.RoleProvider.xml**
2. После нажатия кнопки **“OK”** должны увидеть окно как на рисунке 31.



*Рис. 31. Хранилище данных авторизации загружено.*

1. В левой панели раскрываем по максимуму все узлы (рисунок 32)



*Рис. 32. Структура хранилища данных авторизации.*

## Объекты хранилища

**Провайдер ролей  
(оснастка azman.msc)**

**Операционная система**

Windows и  
Active Directory

*RoleProvider.png*

*Users.png*

Группы и пользователи

*User.png*

Легенда

Диспетчер   
авторизации

Создаваемые пользователем объекты

Группы и пользователи Windows

Вложенные коллекции

Создаваемые провайдером ролей папки

Связи, формируемые при создании объектов

Связи, формируемые при добавлении объектов

Связи, формируемые при назначении объектов

Тип связи  
”один к одному”

Тип связи  
”один ко многим”

Тип связи  
”много ко многим”

Возможно появление сообщения о зацикливании

См. рис. 41

См. рис. 42, 43

*Group.png*

См. рис. 44

См. рис. 40

См. рис. 36, 37

См. рис. 34, 35

Эта часть схемы отвечает за распределение полномочий между администраторами и делегирование им прав на редактирование хранилища данных авторизации.

На данный момент такая возможность в **Adem iRIS** не задействована в связи с отсутствием необходимости.

*RoleDefinition.png*

*Рис. 33. Схема взаимодействия объектов хранилища.*Group.pngRole.pngTask.pngOperation.pngTask.pngGroup.pngRole.pngRoleDefinition.pngFolder.pngFolder.pngFolder.pngFolder.pngFolder.pngFolder.pngFolder.pngFolder.pngFolder.pngFolder.pngFolder.pngFolder.pngScope.pngApplication.pngStore.png

Определения задач

Определения ролей

Группы

Определения

Назначения ролей

Определения операций

Определения задач

Определения ролей

Назначения ролей

Группы

Группы

Определения

Приложение

Хранилище авторизации

Задача

Определение роли

Назначение роли

Исключить

Включить

Группа приложения

Группа приложения

Исключить

Включить

Исключить

Включить

Группа приложения

Назначение роли

Операция

Задача

Определение роли

Область

Диспетчер авторизации

Каждый из объектов хранилища имеет своё собственное имя, на которое провайдер ролей **Microsoft AzMan** накладывает определённые ограничения. Так, например, у большинства объектов длина имени не должна превышать 64 символа. К тому же эти имена должны быть уникальны в пределах их области действия. В процессе сканирования (при генерации операций и задач) применяется определённый механизм наименования объектов, использующий систему префиксов и так называемую точечную нотацию. Кроме того, каждый из объектов имеет текстовое поле, именуемое описанием и допускающее 1024 символа.

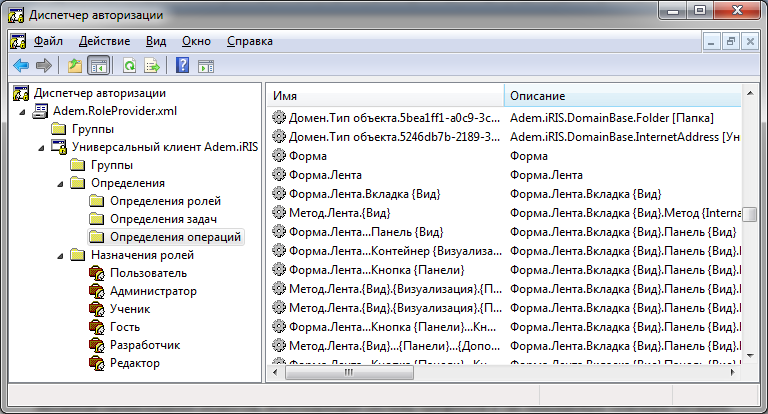
## Определения операций

Основным объектом хранилища является **операция** (значокOperation.png), поскольку именно на основе сопоставления её имени с именем, формируемым функцией **Sample** (см рис. 33), провайдером ролей определяется, разрешено ли для конкретного пользователя дальнейшее выполнение функции **Sample**. Но операции могут быть созданы и размещены только в объекте **приложение** (значок Application.png). В свою очередь, приложение может быть создано и размещено только в объекте **хранилище авторизации** (значок Store.png). Таким образом, эти объекты (набор операций, приложение, хранилище) являются обязательными для корректного функционирования провайдера ролей. Как следствие, провайдер ролей в режиме администратора (см. рис. 29) предотвращает создание новых приложений и модификацию определений операций.

При удалении операции из хранилища или при её переименовании выполнение соответствующей функции будет недоступно. При создании новой операции невозможно выполнить её привязку к какой-либо функции универсального клиента, поэтому в этом нет никакого смысла. Поэтому настоятельно не рекомендуется изменять существующий в хранилище набор операций.

Все остальные объекты (задачи, определения ролей, группы приложения, области, назначения ролей) не являются обязательными и могут быть, в принципе, удалены, но тогда необходимо будет заново сформировать роли и выполнить их назначение.

При выполнении сортировки операций по полю описания отображается (с помощью точечной нотации) иерархия элементов управления универсального клиента (см. рис. 34).



См. рис. 35

*Рис. 34. Фрагмент списка операций.*

Operation.pngOperation.pngOperation.pngOperation.png

**К интерфейсу  
универсального клиента**

Операция

В имени операции  
используются **прочие** префиксы

Данные операции  
представляют собой  
**элементы управления**  
(имеющие средства визуализации)

**Определения операций**

**К прикладной  
области**

Операция

В имени операции  
используется префикс  
**Домен**

Данные операции  
представляют собой  
**типы объектов**прикладной области

**К методам  
универсального клиента**

Операция

В имени операции  
используется префикс  
**Метод+**

Данные операции   
представляют собой  
**методы работы  
с типами объектов**  
прикладной области

Операция

В имени операции  
используется префикс  
**Метод**

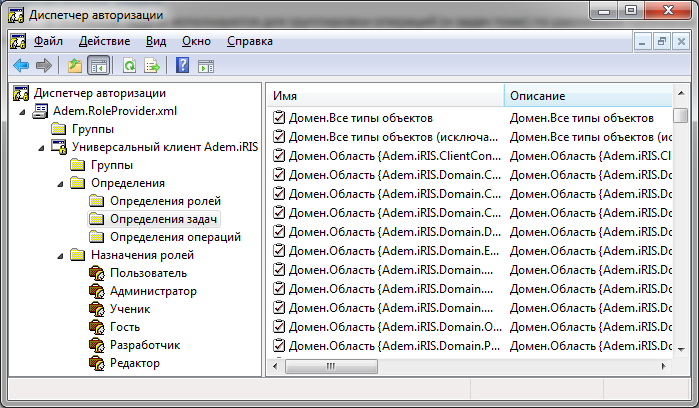
Данные операции  
представляют собой  
**прочие методы**

*Рис. 35. Подмножества операций, использующих префиксы в имени.*

## Определения задач

В основном задачи (значок Task.png) используются для группировки операций (и задач тоже) по различным признакам и являются основным элементом для формирования содержимого ролей. Как уже было отмечено выше, напрямую работать с операциями не рекомендуется. Поэтому задачи, содержащие в своём составе только одну операцию, фактически “дублируют” эту операцию, но такими задачами уже можно манипулировать без опаски случайного удаления (задачу всегда можно восстановить и даже присвоить ей произвольное имя).

При формировании новых ролей или при модификации существующих используйте именно задачи.



См. рис. 37

*Рис. 36. Фрагмент списка задач.*

**К прикладной  
области**

Задача

В имени задачи  
используется префикс  
**Домен**

Данные задачи  
группируют операции  
с таким же префиксом

**Определения задач**

**К интерфейсу  
универсального клиента**

Данные задачи  
группируют операции,  
связанные с интерфейсом универсального клиента

Задача

В имени задачи  
используются **прочие** префиксы

**К методам  
универсального клиента**

Данные задачи  
группируют операции  
с таким же префиксом

Задача

В имени задачи  
используется префикс  
**Метод+**

Данные задачи  
группируют операции  
с таким же префиксом

Задача

В имени задачи  
используется префикс  
**Метод**

Задача

Задача

В имени задачи используется префикс  
**Ролевой контент.<имя роли>.Функциональность+Домен**

Задача

Задача

В имени задачи используется префикс  
**Ролевой контент.<имя роли>.Функциональность**

Задача

Задача

В имени задачи используется префикс  
**Ролевой контент.<имя роли>.Интерфейс**

**К формированию ролей**

В именах задач используется префикс  
**Ролевой контент**

*Рис. 37. Подмножества задач, использующих префиксы в имени.*

Многократная способность задач включать в себя другие задачи позволяет манипулировать ими на более высоком, так скажем, абстрактном уровне, что в целом упрощает формирование ролей. С этой целью созданы, например, задачи с префиксом **Ролевой контент**.

Сортировка задач по описанию располагает задачи верхнего уровня (с префиксом **Ролевой контент**) в начало списка.

Сразу хотелось бы обратить ваше внимание на состав задач с префиксом **Ролевой контент.<имя роли>.Функциональность+Домен**. Дело в том, что решение о предоставлении либо о запрете выполнения той или иной функции над тем или иным объектом прикладной области принимается на основе пересечения двух множеств:

- задач с префиксом **Метод+**

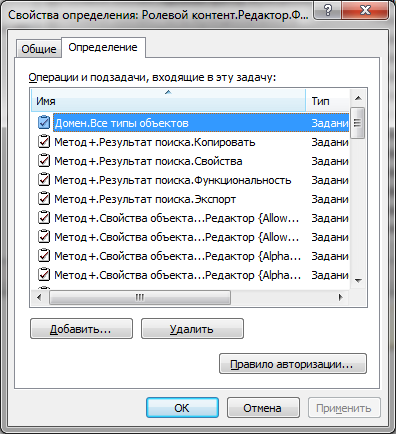
- задач с префиксом **Домен**

Поэтому для выполнения функций над объектами прикладной области оба множества должны быть обязательно сведены вместе в какой-либо одной задаче, чтобы результат пересечения не был пустым.

Как видно из рис. 38, в состав задачи включены задачи с префиксом **Метод+** и одна задача с префиксом **Домен**, которая, в свою очередь, содержит все задачи, олицетворяющие типы объектов прикладной области.

По умолчанию список разрешённых функций (задач с префиксом **Метод+**) зависит от роли, а список разрешённых типов (задач с префиксом **Домен**) включает в себя все типы объектов прикладной области.

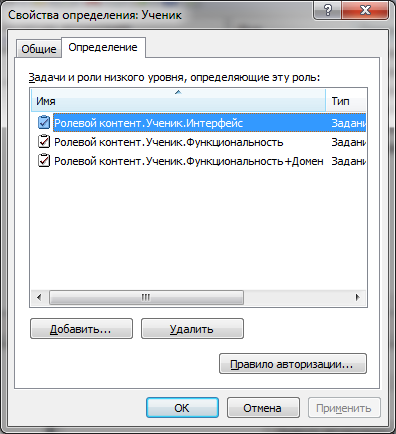
Как следствие, чтобы ограничить доступ к типам объектов прикладной области, необходимо из задачи с префиксом **Ролевой контент.<имя роли>.Функциональность+Домен** удалить задачу с префиксом **Домен.Все типы объектов** и добавить все необходимые задачи с префиксом **Домен.Тип объекта**.



*Рис. 38. Состав задачи* ***Ролевой контент.Редактор.Функциональность+Домен****.*

## Определения ролей

Определение роли - или просто роль (значок RoleDefinition.png)- может включать в себя операции, задачи, другие роли и является, по сути, конечной целью настройки. По окончанию формирования роли остаётся только выполнить её назначение пользователям операционной системы.

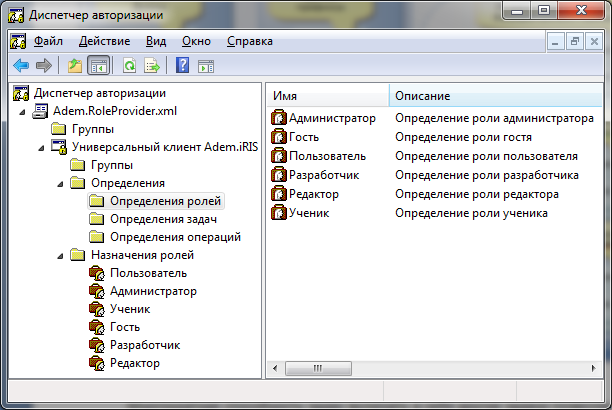


Значение этого префикса зависит от наименования роли.

Каждая из шести сформированных на данный момент ролей содержит в себе три задачи:

1. Задача с префиксом **Интерфейс**отвечает за визуализацию элементов управления универсального клиента.
2. Задача с префиксом **Функциональность**  
   отвечает за выполнение функций, не связанных непосредственно с типами объектов прикладной области.
3. Задача с префиксом **Функциональность+Домен**   
   отвечает за выполнение функций, контролирующих типы объектов прикладной области.

*Рис. 39. Состав роли* ***Ученик****.*



Нет доступа

Тот же доступ,  
что и у роли **Редактор**,  
за исключением  
возможности вносить  
какие-либо изменения  
(только просмотр)

Тот же доступ,  
что и у роли **Администратор**,  
за исключением  
служебной информации,  
предназначенной для администрирования

Тот же доступ,  
что и у роли **Разработчик**,  
за исключением  
информации, необходимой для  
разработки программного обеспечения

Тот же доступ,  
что и у роли **Редактор**,  
за исключением  
возможности сдать на сервер  
внесённые изменения

Полный доступ

*Рис. 40. Список ролей.*

## Группы приложения

Группы приложения (значокGroup.png) используются, в основном, с целью более эффективного манипулирования Windows-группами и пользователями операционной системы, и состоят из двух списков: **Члены группы** и **Исключения**. Оба списка могут содержать в себе другие группы приложения, Windows-группы и пользователей операционной системы.



*Рис. 41. Список групп приложения.*

## 

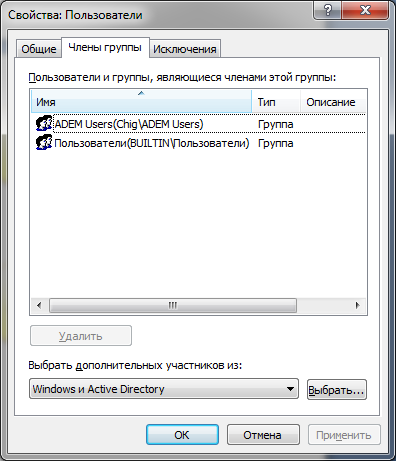
Обратите внимание на то, что провайдер ролей  
самостоятельно указал на принадлежность  
группы **Adem Administrators** компьютеру **Chig.**

При децентрализованном использовании хранилища данных авторизации и при прямом переносе файла хранилища с одного компьютера на другой это обстоятельство может вызвать определённые затруднения.

В файле конфигурации имя компьютера не указано!

Члены группы  
заранее были определены  
вфайле конфигурации **Adem.RoleProvider.dll.config**секции **Scanning**  
(см. рис. 26, 27)

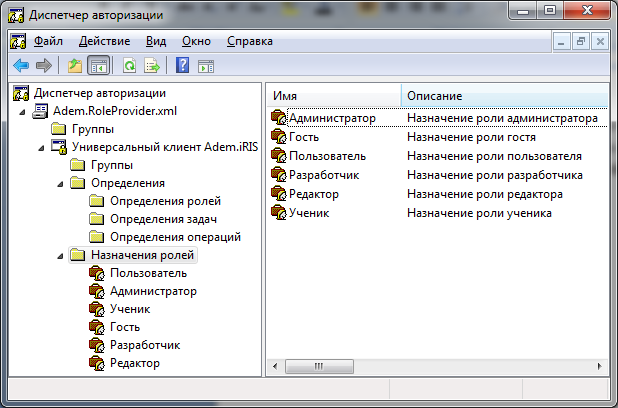
*Рис. 42. Состав группы приложения* ***Администраторы****.*

**

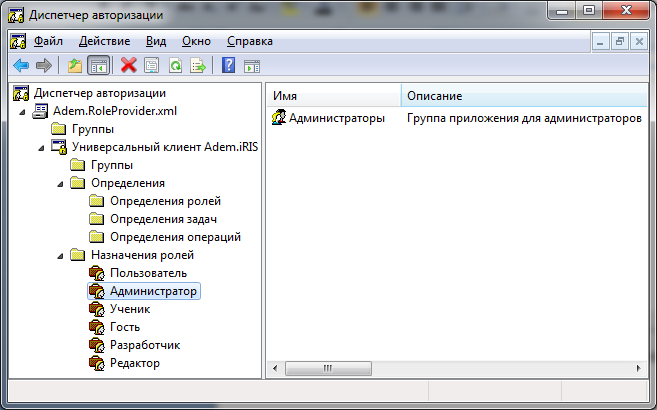
*Рис. 43. Состав группы приложения* ***Пользователи****.*

## Назначения ролей

После того, как с помощью задач будет сформирована роль, выполняют так называемое назначение роли (значок Role.png), то есть выполняют привязку Windows-групп и/или пользователей операционной системы (либо прямым указанием, либо посредством заранее сформированных групп приложения) к нужной роли.



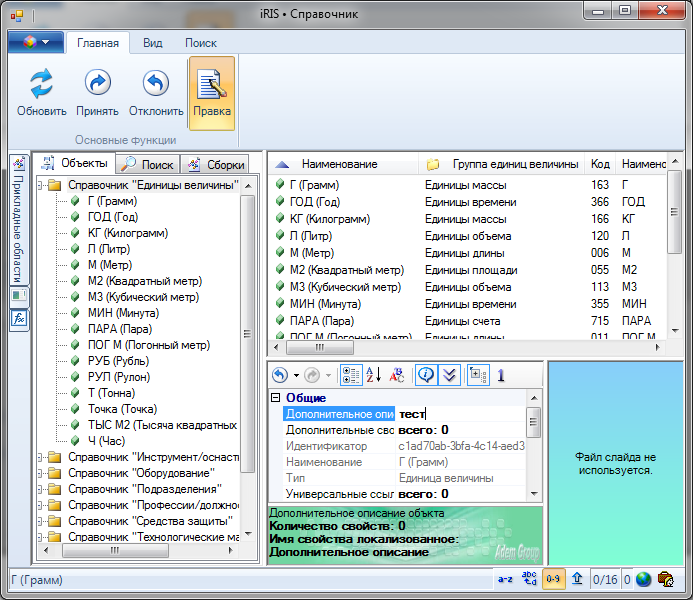
*Рис. 44. Список назначений ролей.*



Назначение роли выполнено  
не прямым указанием Windows-групп и/или пользователей,  
а опосредованно, через группу приложения **Администраторы**  
(см рис. 42)

*Рис. 45. Роли* ***Администратор*** *назначена группа приложения* ***Администраторы****.*

# Интерфейс универсального клиента



**2**

**3**

**1**

**4**

**6**

**7**

**8**

**9**

**10**

**11**

**12**

**13**

**14**

**15**

**16**

**18**

**19**

**20**

**21**

**22**

**17**

**23**

**25**

**24**

**39**

**5**

**26**

**27**

**31**

**32**

**33**

**34**

**38**

**36**

**37**

**30**

**29**

**35**

**28**

**40**

**41**

**47**

**44**

**45**

**46**

**48**

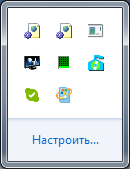
**42**

**49**

**50**

**43**

*Рис. 46. Интерфейс универсального клиента с ролевым контентом* ***Разработчик*** *(полный доступ).*

**

Adem iRIS tasks

**51**

*Рис. 47. Панель* ***Область уведомлений*** *операционной системы.*

Как уже отмечалось выше, в оснастке провайдера ролей при сортировке задач либо операций по полю описания с помощью точечной нотации выстраивается иерархия элементов управления универсального клиента. При формировании новой роли эта информация помогает сконструировать необходимый для роли интерфейс клиента. На рис. 46 и в приведённой ниже таблице отображено соответствие между элементами управления и присвоенными им префиксами в описании задач (перечень далеко не полный).

|  |  |
| --- | --- |
| Номер | Префикс в описании задачи |
| 1 | Интерфейс |
| 2 | Интерфейс.Лента |
| 3 | Интерфейс.Лента.Вид |
| 4 | Интерфейс.Лента.Главная |
| 5 | Интерфейс.Лента.Главная.Основные функции |
| 6 | Интерфейс.Лента.Главная.Основные функции.Обновить |
| 7 | Интерфейс.Лента.Главная.Основные функции.Отклонить |
| 8 | Интерфейс.Лента.Главная.Основные функции.Правка |
| 9 | Интерфейс.Лента.Главная.Основные функции.Принять |
| 10 | Интерфейс.Лента.Главная.Панель |
| 11 | Интерфейс.Лента.Главная.Поиск |
| 12 | Интерфейс.Панели |
| 13 | Интерфейс.Панели.Дополнительная функциональность |
| 14 | Интерфейс.Панели.Дополнительные приложения |
| 15 | Интерфейс.Панели.Прикладные области |
| 16 | Интерфейс.Панель.Иерархия |
| 17 | Интерфейс.Панель.Иерархия.Вкладки |
| 18 | Интерфейс.Панель.Иерархия.Вкладки.Объекты |
| 19 | Интерфейс.Панель.Иерархия.Вкладки.Объекты.Справочник объектов |
| 20 | Интерфейс.Панель.Иерархия.Вкладки.Поиск |
| 21 | Интерфейс.Панель.Иерархия.Вкладки.Сборки |
| 22 | Интерфейс.Панель.Иерархия.Список |
| 23 | Интерфейс.Панель.Иерархия.Список.Список объектов |
| 24 | Интерфейс.Панель.Иерархия.Список.Таблица |
| 25 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта |
| 26 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Комментарий |
| 27 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Комментарий.Примечание |
| 28 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов |
| 29 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов.Вложенные объекты |
| 30 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов.Категории |
| 31 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов.Комментарий |
| 32 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов.По алфавиту |
| 33 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов.По категориям |
| 34 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов.По описанию |
| 35 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов.Слияние свойств |
| 36 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов.Отменить ввод |
| 37 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Панель инструментов.Повторить ввод |
| 38 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Содержание |
| 39 | Интерфейс.Панель.Иерархия.Список.Таблица.Свойства объекта.Содержание.Текстовое поле |
| 40 | Интерфейс.Панель.Иерархия.Список.Таблица.Слайд объекта |
| 41 | Интерфейс.Строка состояния |
| 42 | Интерфейс.Строка состояния.Блокировка прокрутки |
| 43 | Интерфейс.Строка состояния.Дополнительная клавиатура |
| 44 | Интерфейс.Строка состояния.Зона приложения |
| 45 | Интерфейс.Строка состояния.Комментарий |
| 46 | Интерфейс.Строка состояния.Прописные или строчные буквы |
| 47 | Интерфейс.Строка состояния.Режим вставки или замены |
| 48 | Интерфейс.Строка состояния.Ролевой контент |
| 49 | Интерфейс.Строка состояния.Счётчик групп |
| 50 | Интерфейс.Строка состояния.Счётчик объектов |
| 51 | Хост.Уведомление |

# Примеры

## Пример 1. Создание и назначение роли с выборочным редактированием

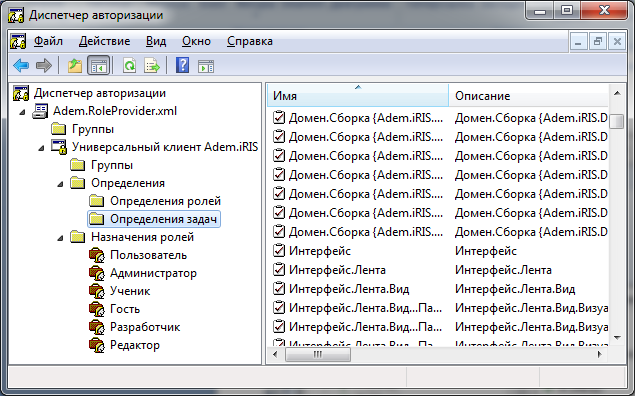
1. Постановка задачи:

Допустим, нам необходима роль **ТЕСТ** с минимально необходимым набором элементов управления, причём имеющая возможность выборочной манипуляции над объектами прикладной области:

* объект **Папка** (просмотр свойств)
* объект **Пила** (все операции)
* для остальных объектов запретим все операции

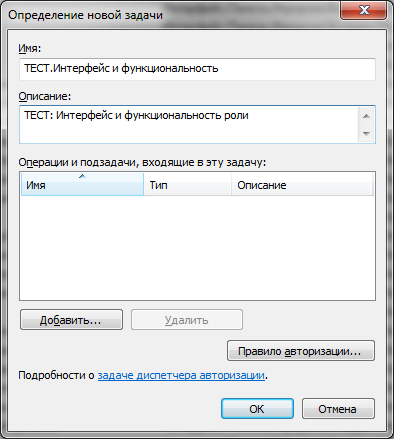
При создании задач желательно пользоваться префиксом (пусть будет **ТЕСТ**), что облегчит их поиск в оснастке провайдера ролей.

1. Открываем хранилище в режиме **Администратор** (см. главу Открытие хранилища).
2. В левой панели выбираем пункт **Определения задач**.



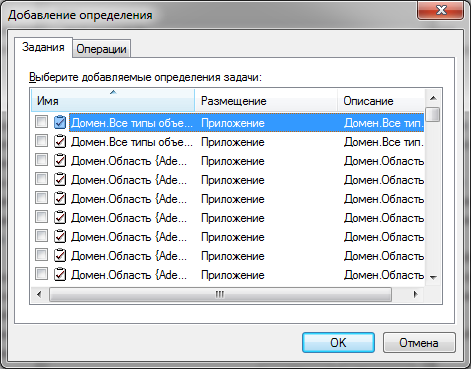
*Рис. 48. Определения задач.*

1. Через контекстное меню выбираем пункт **Постановка новой задачи…**
2. В диалоге **Определение новой задачи** заполняем поля **Имя** и **Описание.**



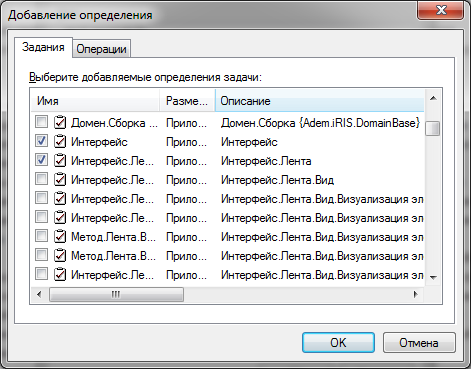
*Рис. 49. Определение новой задачи (****ТЕСТ.Интерфейс и функциональность****).*

1. После этого нажимаем кнопку **Добавить…**
2. В диалоге **Добавление определения** остаёмся на вкладке **Задания** (задачи).

****

*Рис. 50. Добавление определения.*

1. Сортируем по возрастанию поле **Описание** и делаем его максимально видимым.



*Рис. 51. Определения задач отсортированы по полю* ***Описание****.*

1. Ставим “галочки” напротив необходимых нам задач:

- во-первых, выбираем элементы управления (префикс **Интерфейс** в имени задачи),

- во-вторых, выбираем общие методы (префикс **Метод** в имени задачи)

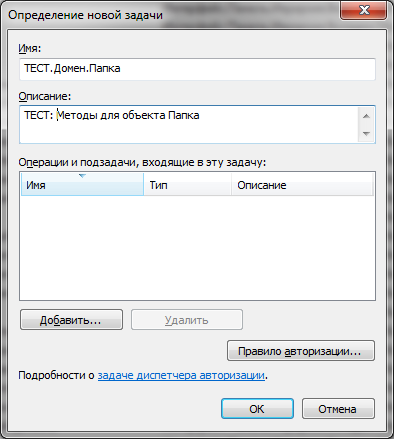
Стоит отметить, что выбирая задачу (например, **Интерфейс.Лента.Вид**) более низкого уровня не надо забывать выбрать и вышестоящие задачи (**Интерфейс** и **Интерфейс.Лента**).

Обязательно добавьте задачи с именами **Хост.Уведомление** и **Хост.Уведомление.Выход**, иначе снять хост можно будет только с помощью команды **Adem.iRIS.Client.exe host=kill.**

В таблице приведён перечень выбранных задач:

|  |
| --- |
| Имена задач для **ТЕСТ.Интерфейс и функциональность** |
| Интерфейс |
| Интерфейс.Лента |
| Интерфейс.Лента.Главная |
| Интерфейс.Лента.Главная.Основные функции |
| Интерфейс.Лента.Главная.Основные функции.Вернуть |
| Метод.Лента.Главная.Основные функции.Вернуть |
| Интерфейс.Лента.Главная.Основные функции.Обновить |
| Метод.Лента.Главная.Основные функции.Обновить |
| Интерфейс.Лента.Главная.Основные функции.Отклонить |
| Метод.Лента.Главная.Основные функции.Отклонить |
| Интерфейс.Лента.Главная.Основные функции.Правка |
| Метод.Лента.Главная.Основные функции.Правка |
| Интерфейс.Лента.Главная.Основные функции.Принять |
| Метод.Лента.Главная.Основные функции.Принять |
| Интерфейс.Лента.Главная.Панель |
| Интерфейс.Панель |
| Интерфейс.Панель.Иерархия |
| Интерфейс.Панель.Иерархия.Вкладки |
| Интерфейс.Панель...Вкладки.Объекты |
| Метод.Панель...Вкладки.Объекты |
| Справочник объектов |
| Метод.Панель.Иерархия...Перемещение разделителя |
| Интерфейс.Панель.Иерархия.Список |
| Метод.Панель...Список...Перемещение разделителя |
| Список объектов |
| Список объектов.Контекстное меню |
| Список объектов...Вставить |
| Список объектов...Выделить всё |
| Метод.Список объектов.Выделить всё |
| Список объектов...Вырезать |
| Список объектов...Импорт |
| Список объектов...Копировать |
| Метод.Список объектов.Контекстное меню |
| Список объектов...Множественный выбор |
| Метод.Список объектов.Множественный выбор |
| Список объектов...Обратить выделение |
| Метод.Список объектов.Обратить выделение |
| Список объектов...Переименовать |
| Список объектов...Разделитель {Выборка} |
| Список объектов...Разделитель {Импорт&Экспорт} |
| Список объектов...Разделитель {Множественный выбор} |
| Список объектов...Разделитель {Модификация} |
| Список объектов...Разделитель {Свойства} |
| Список объектов...Разделитель {Создание} |
| Список объектов...Сбросить выделение |
| Метод.Список объектов.Сбросить выделение |
| Список объектов...Свойства |
| Список объектов...Создать заполненный объект |
| Список объектов...Создать новый объект |
| Список объектов...Создать новый объект типа... |
| Список объектов...Создать пустой объект |
| Список объектов...Удалить |
| Список объектов...Экспорт |
| Интерфейс.Панель.Иерархия.Список.Таблица |
| Метод.Панель...Таблица...Перемещение разделителя |
| Свойства объекта |
| Свойства объекта.Содержание |
| Свойства объекта.Содержание.Всплывающий список |
| Свойства объекта.Содержание.Модальное окно |
| Свойства объекта.Содержание.Текстовое поле |
| Слайд объекта |
| Хост.Уведомление |
| Хост.Уведомление.Контекстное меню |
| Хост.Уведомление.Контекстное меню.Выход |
| Метод.Хост.Уведомление |
| Метод.Хост.Уведомление.Контекстное меню |
| Метод.Хост.Уведомление.Контекстное меню.Выход |

1. Завершаем формирование задачи нажатием кнопки **OK**.
2. Повторяем пункты с 4 по 8, но для задачи **ТЕСТ. Домен.Папка**.



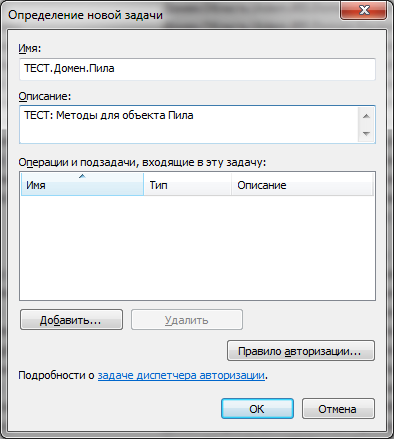
*Рис. 52. Определение новой задачи (****ТЕСТ.Домен.Папка****).*

1. Поскольку определения операций, отвечающие за тип объекта прикладной области, соответствующими задачами не дублируются, то переходим на вкладку **Операции** и выбираем операцию с префиксом **Домен.Тип объекта** в имени, отвечающую за тип **Папка**, предварительно отсортировав операции по полю **Описание**.
2. Переходим на вкладку **Задания** и добавляем все необходимые для объекта **Папка** задачи с префиксом **Метод+** в имени**.**

В таблице приведён перечень выбранных задач и операций:

|  |  |  |
| --- | --- | --- |
| Задачи и операции для **ТЕСТ. Домен.Папка** | | |
| Имя | Описание | Тип |
| Метод+.Свойства объекта...Просмотр |  | Задача |
| Метод+.Список объектов.Свойства |  | Задача |
| Домен.Тип объекта.5bea1ff1-a0c9-3c88-a96b-ef0bdda1b236 | Adem.iRIS.DomainBase.Folder [Папка] | Операция |

1. Завершаем формирование задачи нажатием кнопки **OK**.
2. Повторяем пункты с 4 по 8, но для задачи **ТЕСТ. Домен.Пила**.



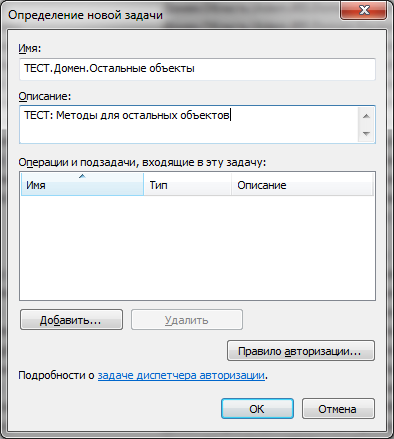
*Рис. 53. Определение новой задачи (****ТЕСТ.Домен.Пила****).*

1. Переходим на вкладку **Операции** и выбираем операцию с префиксом **Домен.Тип объекта** в имени, отвечающую за тип **Пила**.
2. Переходим на вкладку **Задания** и добавляем все необходимые для объекта **Пила** задачи с префиксом **Метод+** в имени**.**

В таблице приведён перечень выбранных задач и операций:

|  |  |  |
| --- | --- | --- |
| Задачи и операции для **ТЕСТ. Домен.Пила** | | |
| Имя | Описание | Тип |
| Метод+.Свойства объекта...Правка.Всплывающий список |  | Задача |
| Метод+.Свойства объекта...Правка.Модальное окно |  | Задача |
| Метод+.Свойства объекта...Правка.Текстовое поле |  | Задача |
| Метод+.Свойства объекта...Просмотр |  | Задача |
| Метод+.Свойства объекта...Редактор {AllowedTypeChecked} |  | Задача |
| Метод+.Свойства объекта...Редактор {AllowedType} |  | Задача |
| Метод+.Свойства объекта...Редактор {Alphabet\_EN} |  | Задача |
| Метод+.Свойства объекта...Редактор {Alphabet\_RU} |  | Задача |
| Метод+.Свойства объекта...Редактор {Color} |  | Задача |
| Метод+.Свойства объекта...Редактор {DateTime} |  | Задача |
| Метод+.Свойства объекта...Редактор {DomainObjectCollection} |  | Задача |
| Метод+.Свойства объекта...Редактор {DomainObject} |  | Задача |
| Метод+.Свойства объекта...Редактор {Enumeration} |  | Задача |
| Метод+.Свойства объекта...Редактор {FileName} |  | Задача |
| Метод+.Свойства объекта...Редактор {ToleranceValue} |  | Задача |
| Метод+.Список объектов.Вставить |  | Задача |
| Метод+.Список объектов.Вырезать |  | Задача |
| Метод+.Список объектов.Импорт |  | Задача |
| Метод+.Список объектов.Копировать |  | Задача |
| Метод+.Список объектов.Переименовать |  | Задача |
| Метод+.Список объектов.Свойства |  | Задача |
| Метод+.Список объектов.Создать заполненный объект |  | Задача |
| Метод+.Список объектов.Создать новый объект |  | Задача |
| Метод+.Список объектов.Создать пустой объект |  | Задача |
| Метод+.Список объектов.Удалить |  | Задача |
| Метод+.Список объектов.Экспорт |  | Задача |
| Домен.Тип объекта.d14939a1-c979-3adc-abbf-bb11d900d585 | Adem.iRIS.Domain.Tools.Saw [Пила] | Операция |

1. Завершаем формирование задачи нажатием кнопки **OK**.
2. Повторяем пункты с 4 по 8, но для задачи **ТЕСТ. Домен.Остальные объекты**.



*Рис. 54. Определение новой задачи (****ТЕСТ. Домен.Остальные объекты****).*

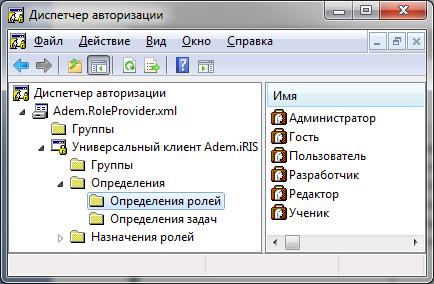
1. Переходим на вкладку **Задания** и добавляем задачу с именем **Домен.Все типы объектов.**

Обратите внимание на то, что в составе данной задачи перечислены все определения операций, ответственные за типы объектов прикладной области.

В таблице приведён перечень выбранных задач и операций:

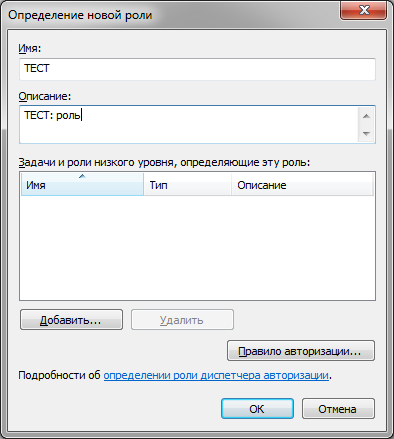
|  |
| --- |
| Имя задачи для **ТЕСТ. Домен.Остальные объекты** |
| Домен.Все типы объектов |

1. Завершаем формирование задачи нажатием кнопки **OK**.
2. В диспетчере авторизации переходим на **Определение ролей**.



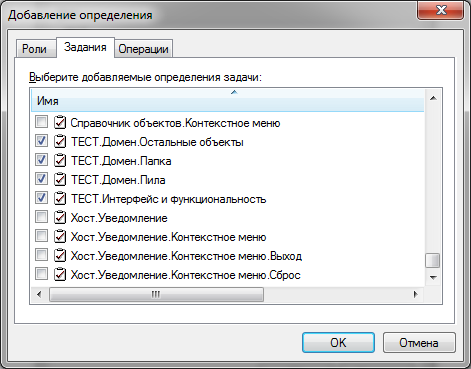
*Рис. 55. Определения ролей.*

1. Через контекстное меню выбираем пункт **Новое определение роли…**
2. В диалоге **Определение новой роли** заполняем поля **Имя** и **Описание**.



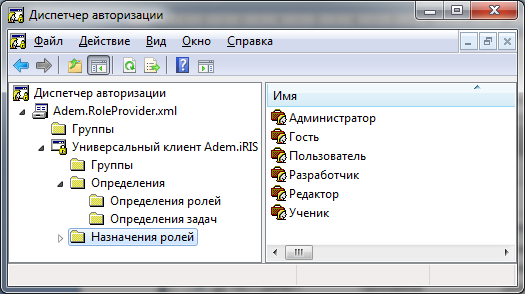
*Рис. 56. Определение новой роли (****ТЕСТ****).*

1. После этого нажимаем кнопку **Добавить…**
2. В диалоге **Добавление определения** переходим на вкладку **Задания**, сортируем задачи по имени и напротив наших новых задач с префиксом **ТЕСТ** в имени ставим “галочки”.



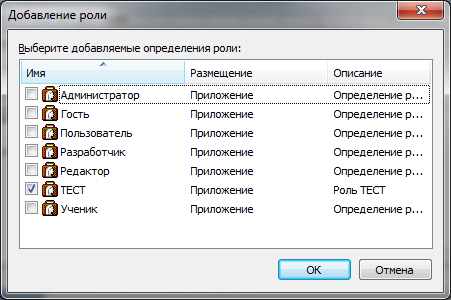
*Рис. 57. Добавление определения.*

1. Завершаем формирование роли нажатием кнопки **OK**.
2. В диспетчере авторизации переходим на **Назначение ролей**.



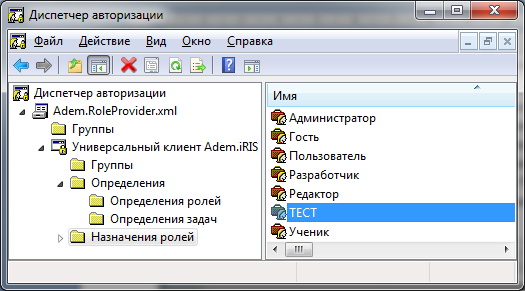
*Рис. 58. Назначение ролей.*

1. Через контекстное меню выбираем пункт **Назначить новую роль …**
2. В диалоге **Добавление роли** ставим “галочку” напротив роли **ТЕСТ**.



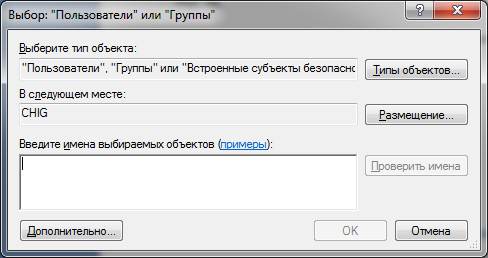
*Рис. 59. Добавление роли.*

1. Завершаем добавление роли нажатием кнопки **OK**.
2. В списке назначенных ролей выбираем **ТЕСТ**.



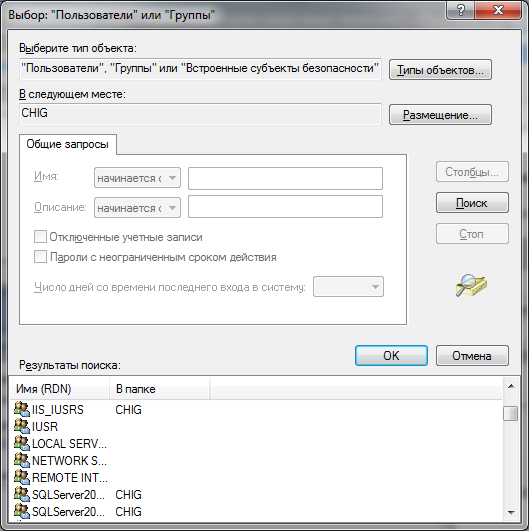
*Рис. 60.Назначение роли* ***ТЕСТ****.*

1. Через контекстное меню выбираем пункт **Назначить пользователей и группы** и далее пункт **Из Windows и Active Directory…**
2. В диалоге указываем необходимый нам список пользователей и Windows-групп путём нажатия кнопки **Размещение…** и выбора компьютера.



*Рис. 61. Выбор пользователей и групп.*

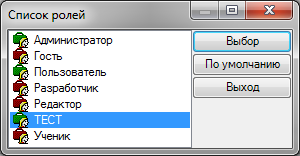
1. Нажимаем кнопки **Дополнительно…** и далее кнопку **Поиск.**
2. Из списка **Результаты поиска** выбираем пользователя либо Windows-группу.



*Рис. 62. Результат поиска.*

1. Завершаем работу нажатием кнопки **ОК** (дважды).
2. Если хост клиентской части **Adem iRIS** активен, то его надо снять через контекстное меню и пункт **Выход.**
3. Запускаем универсального клиента **Adem.iRIS.Client.exe**:

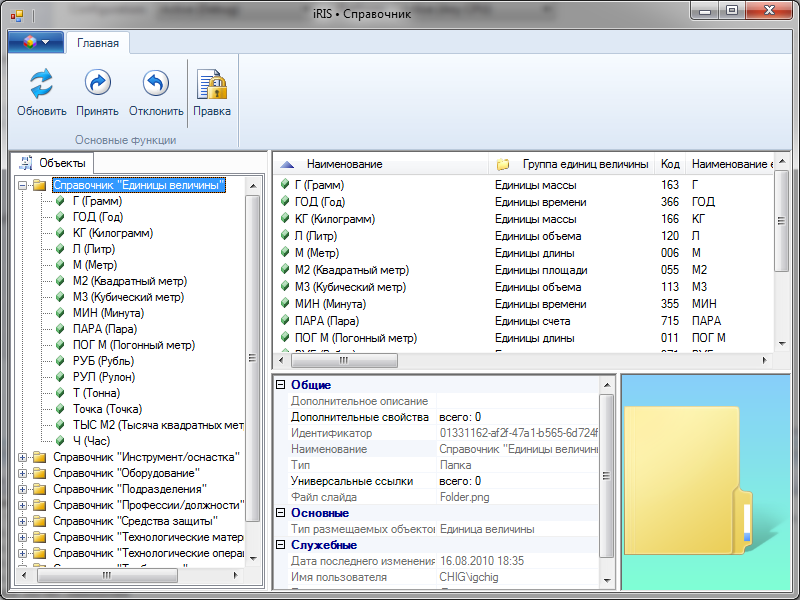
- с ключом **role** (находим роль **ТЕСТ** и нажимаем кнопку **Выбор**)



*Рис. 63. Список ролей*

- либо с ключом **role=ТЕСТ.**

1. Результат показан на рис. 64 (сравните с рис. 46)



Только одна вкладка

Отсутствуют дополнительные панели

Отсутствует строка состояния

Контекстное меню недоступно

Контекстное меню недоступно

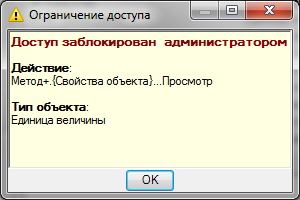
Отсутствует панель инструментов

Отсутствует дополнительное описание

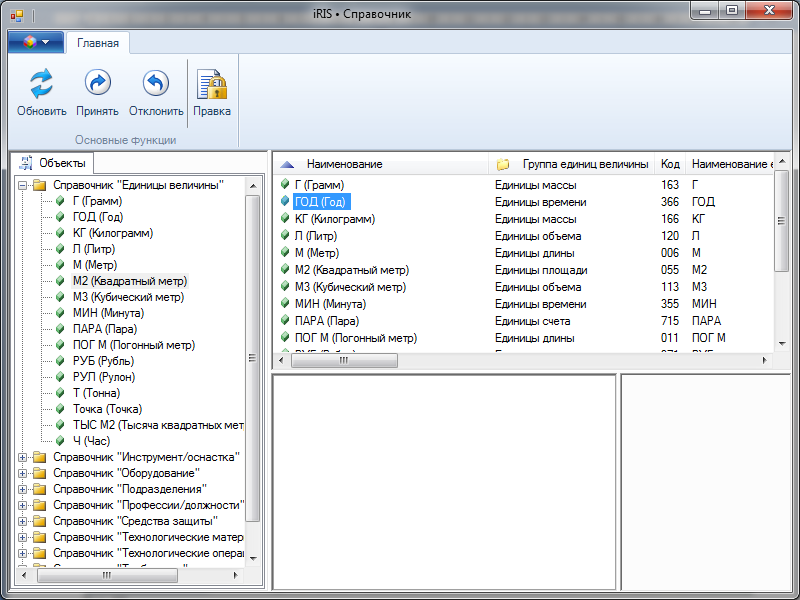
Только один пункт меню

*Рис. 64. Универсальный клиент (ролевой контент* ***ТЕСТ****).*

1. При попытке, допустим, просмотра свойств объекта типа **Единица величины** появляется соответствующее сообщение:



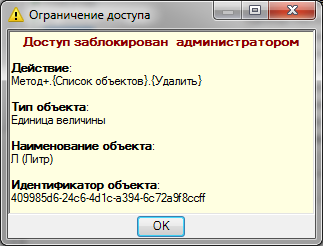
*Рис. 65. Сообщение об ограничении доступа.*

**

Просмотр свойств  
для данного объекта  
запрещён

*Рис. 66. Свойства объекта* ***ГОД*** *недоступны для просмотра.*

1. Появление сообщения при попытке удаления одного из объектов типа **Единица величины**:



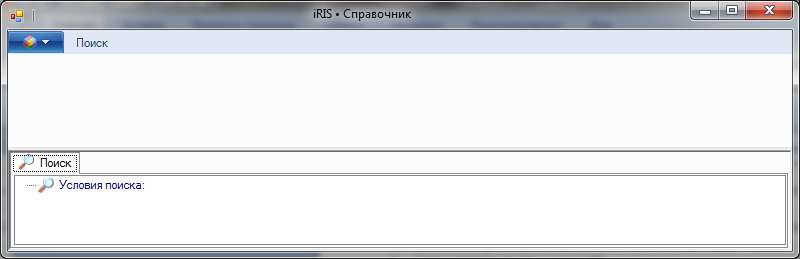
*Рис. 67. Сообщение об ограничении доступа.*

## Пример 2. Создание и назначение роли только для поиска

1. Запускаем оснастку провайдера ролей **azman.msc**.
2. Выполняем постановку новой задачи **ПОИСК.Интерфейс и функциональность**, включив в неё задачи:

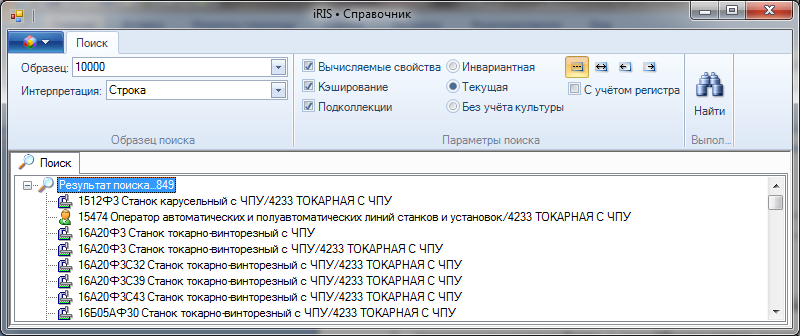
|  |
| --- |
| Имя задачи |
| Интерфейс |
| Интерфейс.Лента |
| Включаем также все задачи с префиксом **Интерфейс.Лента.Поиск** в имени |
| Включаем также все задачи с префиксом **Метод.Лента.Поиск** в имени |
| Интерфейс.Панель |
| Интерфейс.Панель.Иерархия |
| Интерфейс.Панель.Иерархия.Вкладки |
| Интерфейс.Панель...Вкладки.Поиск |
| Метод.Панель...Вкладки.Поиск |
| Результат поиска |
| Хост.Уведомление |
| Хост.Уведомление.Контекстное меню |
| Хост.Уведомление.Контекстное меню.Выход |
| Метод.Хост.Уведомление.Контекстное меню.Выход |
| Метод.Хост.Уведомление.Контекстное меню |
| Метод.Хост.Уведомление |

1. Выполняем новое определение роли **ПОИСК**, включив в неё задачу **ПОИСК.Интерфейс и функциональность**.
2. Выполняем назначение новой роли **ПОИСК**, указав текущего пользователя либо Windows-группу.
3. Запускаем универсального клиента с ключом **-role=ПОИСК**.
4. Результат приведён на рис. 68.



*Рис. 68. Универсальный клиент (ролевой контент* ***ПОИСК****).*

1. Нажимаем пункт меню **Поиск**, в поле **Образец поиска** вводим фрагмент текста и нажимаем кнопку **Найти**.



*Рис. 69. Результат поиска.*

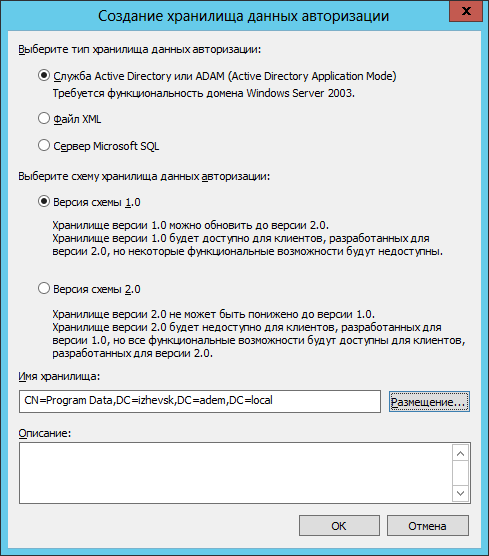
# Интеграция с Active Directory

Как было отмечено ранее, в поставку **Adem iRIS**  хранилище авторизации, предназначенное для использования в **Active Directory**, не входит. Поэтому его необходимо предварительно сгенерировать.

1. На сервере, где установлен **Active Directory**, регистрируемся как пользователь с правами администратора, позволяющими редактировать содержимое **Active Directory**.
2. Запускаем оснастку провайдера ролей (рис. 1 и 2).
3. Устанавливаем режим разработчика (рис. 29).
4. Далее выполняем команду:

*Меню Действие Новое хранилище авторизации…*

1. В качестве типа хранилища указываем службу **Active Directory** (рис. 70)



При наличии у пользователя достаточных прав сразу предлагается соответствующий контейнер для размещения хранилища авторизации

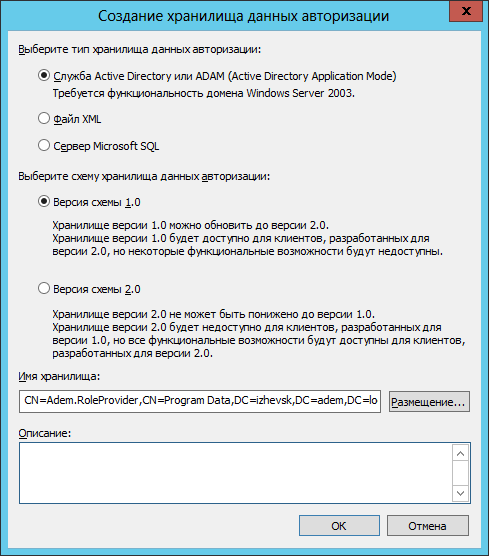
При наличии у пользователя достаточных прав кнопка становится доступной

*Рис.70. Определение контейнера для размещения хранилища авторизации в* ***Active Directory****.*

1. Редактируем поле **Имя хранилища** (рис. 71) с учётом синтаксиса запросов протокола LDAP, добавляя в начало строки фрагмент текста:

**CN=Adem.RoleProvider,**

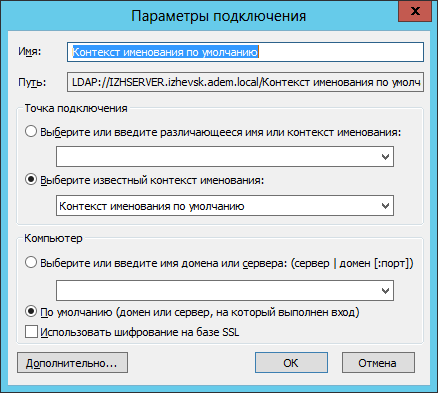
Таким образом, мы создаём свой контейнер с именем **Adem.RoleProvider** (используется по умолчанию в файле конфигурации провайдера) для размещения хранилища авторизации.

****

Имя хранилища авторизации по умолчанию

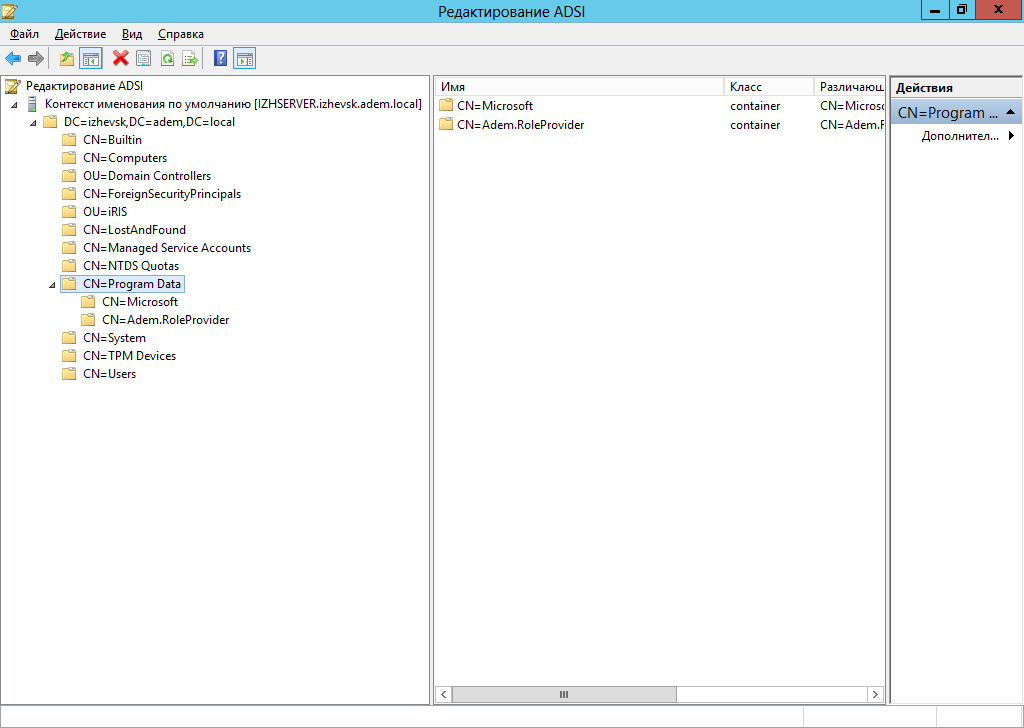
*Рис.71. Создание хранилища авторизации в* ***Active Directory****.*

1. Нажимаем кнопку OK и выходим из оснастки провайдера ролей.
2. Для проверки запускаем на сервере программу **Редактирование ADSI** (Active Directory Service Interface).
3. Если параметры подключения ранее не были выбраны, то соглашаемся с предлагаемым по умолчанию.



*Рис.72. Параметры подключения.*

1. Нажимаем кнопку **Обновить** (для обновления кэша) и находим созданный нами контейнер.

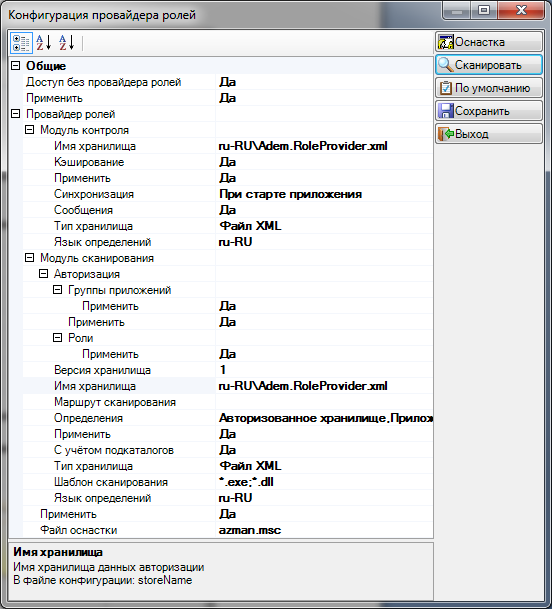


Созданный нами контейнер  
**Adem.RoleProvider**

Кнопка **Обновить**

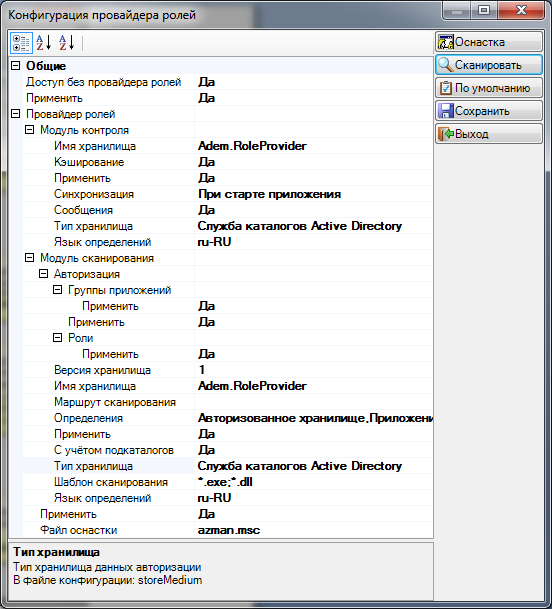
*Рис.73. Контейнер для размещения хранилища авторизации котов к работе.*

1. На сервере либо на любом клиентском компьютере, предварительно включённом в состав домена (!) администратором сети, регистрируемся в домене (!) как пользователь с правами администратора, позволяющими редактировать содержимое **Active Directory**. Пользователь также должен принадлежать к группе **Adem Administrators**, созданной на сервере (!) , поскольку нам надо будет задействовать ключ **azman**.
2. Запускаем сервер **Adem iRIS.**
3. Запускаем универсального клиента **Adem.iRIS**  с ключом **azman**



Перед созданием хранилища авторизации меняем тип хранилища на   
**Служба каталогов Active Directory**

*Рис.74. Конфигурация провайдера ролей (по умолчанию).*

**

Имя контейнера (по умолчанию)  
в **Active Directory**

Для дальнейшей работы   
с универсальным клиентом  
также выбираем

**Служба каталогов Active Directory**

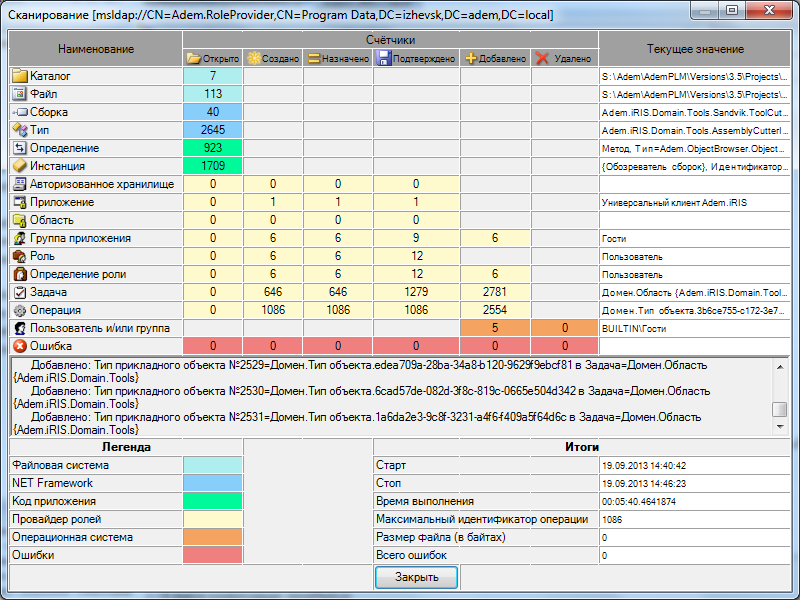
Перед формированием  
хранилища авторизации  
выбрана

**Служба каталогов Active Directory**

Перед формированием  
хранилища авторизации  
имя контейнера должно соответствовать  
созданному ранее в **Active Directory**без учёта синтаксиса LDAP  
(см. рис. 71)

*Рис.75. Конфигурация провайдера ролей, настроенная на работу с* ***Active Directory****.*

1. После внесения соответствующих изменений (см. рис. 75) можно сохранить файл конфигурации, если в дальнейшем предполагается работа именно с **Active Directory** (нажимаем кнопку **Сохранить**).
2. Теперь приступаем к формированию содержимого хранилища авторизации путём нажатия кнопки **Сканировать**.

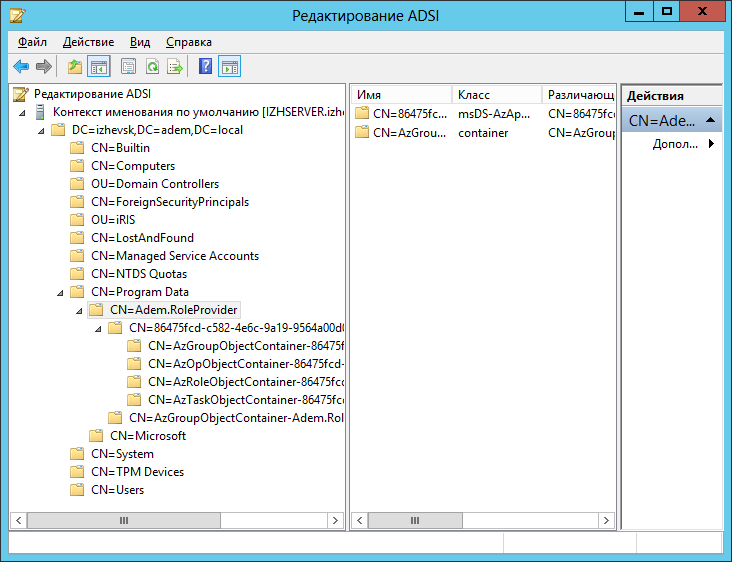


*Рис.76. Формирование хранилища завершено.*

1. Нажимаем кнопку **Закрыть**.
2. Теперь можно приступать к развёртыванию клиентских частей **Adem.iRIS**.

Если возникают проблемы, связанные с недостаточными правами у пользователя, то эту ситуацию можно проконтролировать следующим образом:

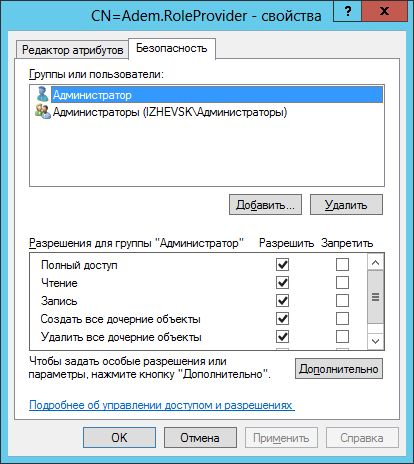
1. Запускаем на сервере (в качестве примера используется сервер Microsoft Windows Standard Server 2012) программу **Редактор ADSI** и выбираем контейнер **Adem.RoleProvider**.



Контейнер, содержащий  
хранилище авторизации

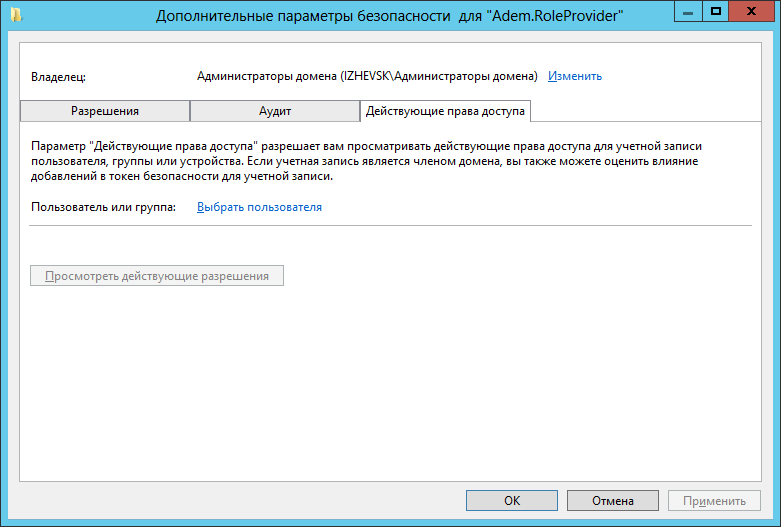
*Рис.77. Редактор ADSI.*

1. Через контекстное меню выбираем пункт **Свойства**, затем вкладку **Безопасность**.



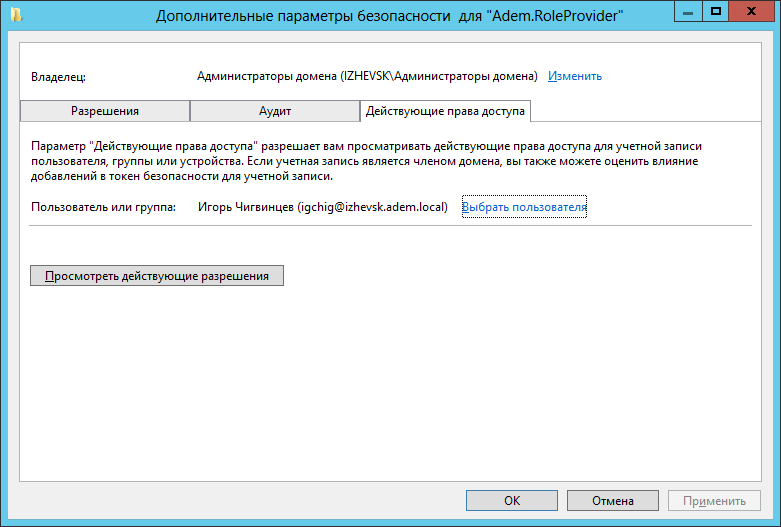
*Рис.78. Свойства контейнера.*

1. Нажимаем кнопку **Дополнительно**.



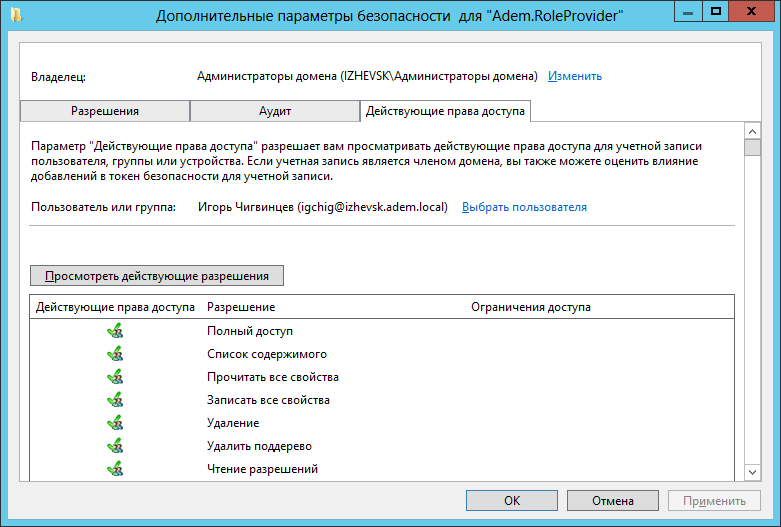
*Рис.79. Дополнительные параметры безопасности.*

1. Нажимаем ссылку **Выбрать пользователя**.



*Рис.80. Выполнен выбор пользователя.*

1. Нажимаем кнопку **Просмотреть действующие разрешения**.



*Рис.81.Просмотр действующих разрешений.*