ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
НАУЧНО - ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ «ЭКРА»

УТВЕРЖДЕН

ЭКРА.00010-02-ЛУ

DCOM для OPC

Инструкция по настройке

ЭКРА.00010-02 91 01-2

Листов 20

2023

Аннотация

Документ описывает последовательность действий по настройке DCOM (Distributed COM) в операционной системе «Windows 7» и новее для обеспечения взаимодействия клиента и сервера OPC. Если клиент и сервер OPC расположены на одном компьютере, то в результате настройки на компьютере будут созданы два пользователя, от имени одного из которых будет запускаться OPC-сервер, а от имени второго — OPC-клиент; подсистема DCOM на компьютере будет настроена так, чтобы OPC-клиент мог установить соединение с OPC-сервером. Если клиент и сервер OPC расположены на разных компьютерах, то в результате настройки на каждом компьютере будут созданы два пользователя, от имени одного из которых будет запускаться OPC-сервер, а от имени второго — OPC-клиент; подсистема DCOM на каждом компьютере будет настроена так, чтобы OPC-клиент мог установить соединение с OPC-сервером.

ОГЛАВЛЕНИЕ

1. ОБЩИЕ НАСТРОЙКИ

Нижеперечисленные операции должны быть выполнены как на стороне сервера, так и на стороне клиента. Они включают в себя создание учетных записей пользователей и определение общих настроек DCOM.

1.1. Настройка учетных записей

Для того чтобы OPC-клиент мог соединиться с OPC-сервером, в системе должны существовать пользователи, от лица которых будет выполняться это соединение. В зависимости от того, объединены ли компьютеры в один домен или нет, учетные записи этих пользователей могут быть созданы либо в домене, либо на локальных компьютерах. Можно использовать уже существующих пользователей. Следует учесть, что локальные учетные записи пользователей должны создаваться как на клиентском, так и на серверном компьютерах. Нельзя для одного пользователя использовать локальную учетную запись вместе с доменной.

В данном руководстве будет описан процесс создания локальных учетных записей пользователей. Настройка домена выходит за рамки данного руководства и описываться не будет. Следует отметить, что дальнейшие действия (после настройки учетных записей) будут одинаковы вне зависимости от того, используются ли локальные учетные записи либо доменные.

Редактирование списка пользователей и групп выполняется в окне оснастки «Локальные пользователи и группы» (Рис. 1), открываемое командой «lusrmgr.msc». Окно этой оснастки содержит список всех пользователей и групп на данной машине.

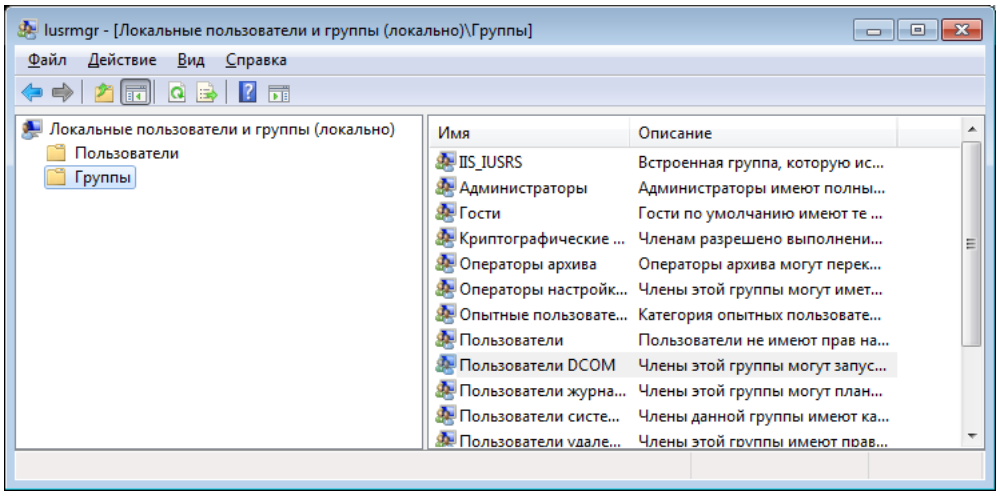

Рис. 1 Окно оснастки «Локальные пользователи и группы»

Для создания нового пользователя нужно выделить узел «Пользователи» и в меню «Действие» выбрать пункт «Новый пользователь...». В появившемся окне (Рис. 2) ввести имя пользователя и его пароль. Снять флаг «Требовать смены пароля...». Обратить внимание, что пароль не должен быть пустым (удаленный доступ для пользователя с пустым паролем по умолчанию запрещен). Затем нажать на кнопку «Создать». После создания пользователя

окно «Новый пользователь» не закрывается, а просто очищает свои поля, позволяя сразу же создать следующего пользователя.

Указанным образом создаем пользователей «OpcServer» и «OpcClient» (от имени этих пользователей будут работать соответственно OPC-сервер и OPC-клиент). Следует еще раз обратить внимание на то, что оба пользователя должны быть созданы как на серверном, так и на клиентском компьютерах, причем один и тот же пользователь на двух разных компьютерах должен иметь один и тот же пароль.

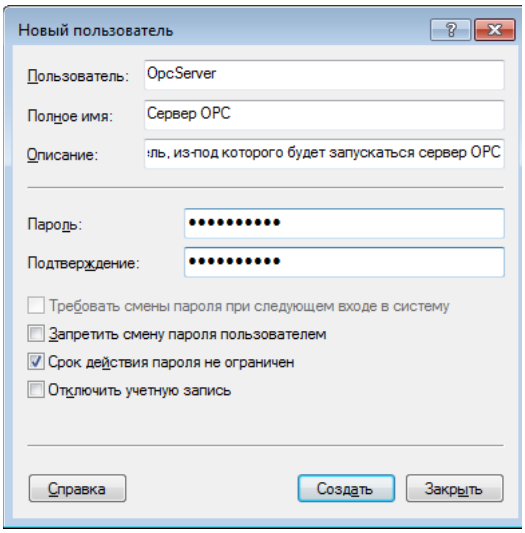

Рис. 2 Создание пользователя

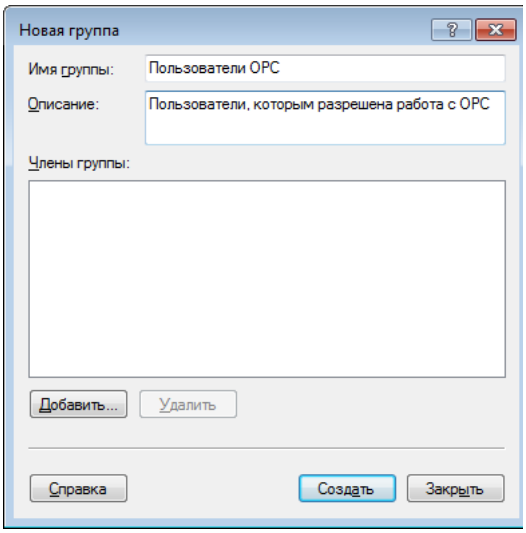

Рис. 3 Создание группы

Для того чтобы в дальнейшем не настраивать разрешения доступа в DCOM для отдельных пользователей, рекомендуется создать отдельную группу, в которую будут входить эти пользователи. Также можно использовать какую-либо уже существующую группу, если она не выполняет каких-либо служебных функций. Так, не следует использовать такие группы, как «Пользователи».

Для создания новой группы требуется выделить узел «Группы» в левой части окна (Рис. 1) и в меню «Действие» выбрать пункт «Создать группу...». В появившемся окне ввести имя и описание новой группы (Рис. 3). Нажать на кнопку «Создать».

Теперь нужно добавить ранее созданных пользователей в данную группу. Для этого в контекстном меню созданной группы нужно выбрать пункт «Добавить в группу...» и в появившемся окне нажать на кнопку «Добавить». В окне выбора пользователя (Рис. 4) ввести имена созданных пользователей (через точку с запятой), нажать на кнопку «Проверить имена» (для проверки правильности введенных имен), затем нажать на кнопку «ОК». Также можно выполнить поиск пользователей, нажав на кнопку «Дополнительно...». Обратить внимание, что если добавляются доменные пользователи, то нужно дополнительно указать их месторасположение, нажав на кнопку «Размещение...».

Таким же образом нужно добавить пользователей «OpcServer» и «OpcClient» в группу «Администраторы».

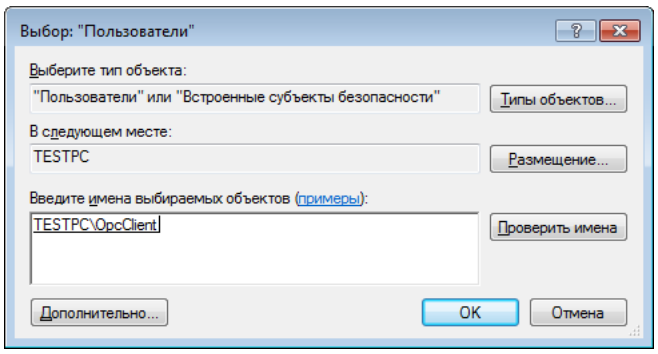

Рис. 4 Окно выбора пользователя (группы)

1.2. Настройка общих параметров DCOM

После создания группы пользователей требуется разрешить этой группе выполнять работу через DCOM. Настройка выполняется через оснастку «Службы компонентов». Чтобы открыть окно этой оснастки, нужно в окне «Выполнить» ввести команду «dcomcnfg».

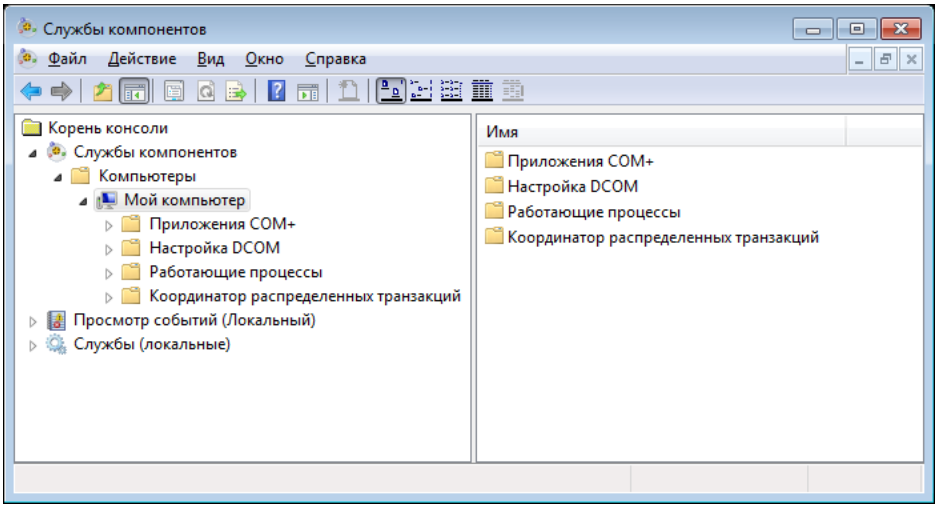

Рис. 5 Окно оснастки «Службы компонентов»

В левой части этого окна выбрать узел «Мой компьютер» и в контекстном меню узла выбрать пункт «Свойства». Откроется окно свойств, содержащее общие настройки DCOM для данного компьютера.

На вкладке «Свойства по умолчанию» (Рис. 6) нужно проверить, что:

- Флаг «Разрешить использование DCOM...» установлен.
- Уровень проверки подлинности выставлен в «Подключиться».
- Уровень олицетворения выставлен в «Определить».

На вкладке «Безопасность COM» (Рис. 7) нужно изменить ограничения на права доступа и на запуск и активацию. Эти ограничения применяются ко всем компонентам на данном компьютере в дополнение к их собственным настройкам. Права на запуск определяют,

какие пользователи могут запускать серверные процессы, а права на доступ — какие пользователи могут обращаться к объектам процесса, когда он уже запущен.

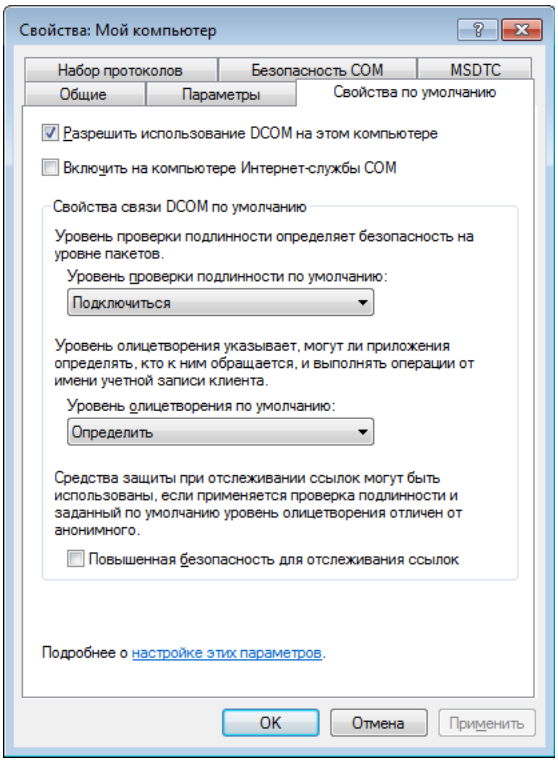

Рис. 6 Свойства по умолчанию

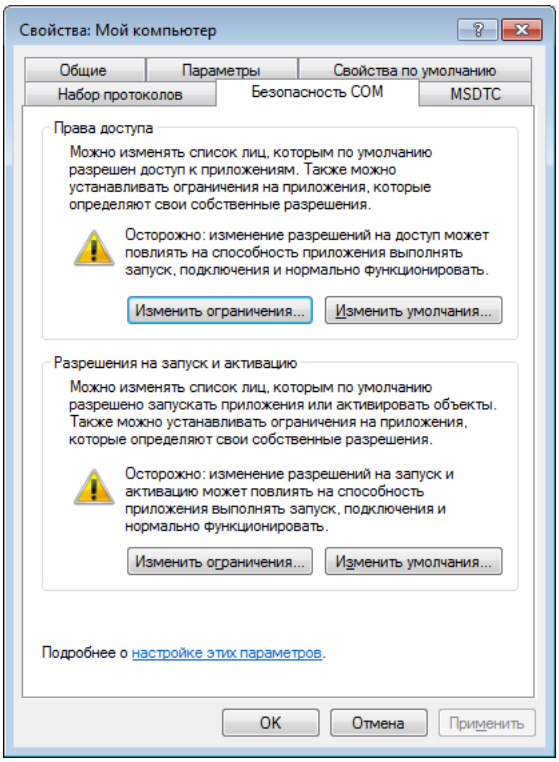

Рис. 7 Свойства безопасности COM

Для настройки прав доступа нужно нажать на кнопку «Изменить ограничения...» в группе «Права доступа». Будет отображено окно настройки прав доступа (Рис. 8).

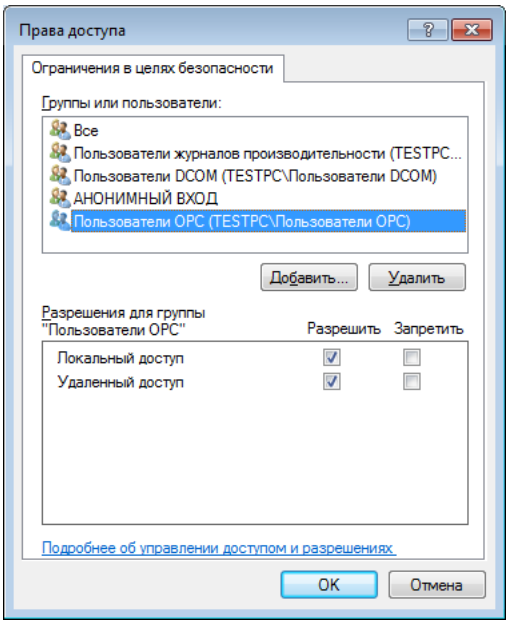

Рис. 8 Назначение прав доступа

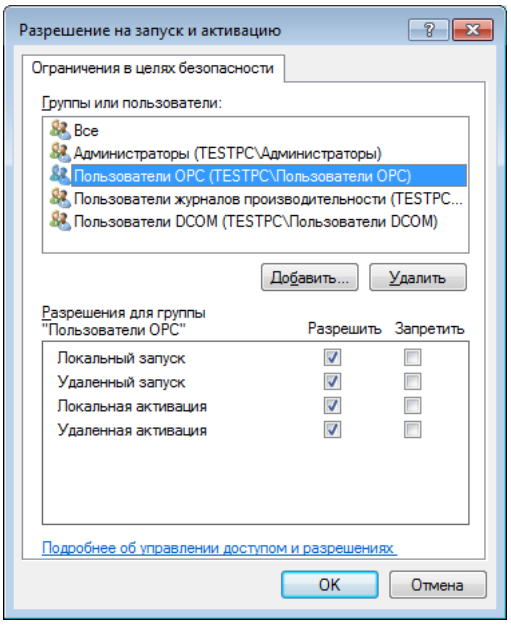

Рис. 9 Назначение прав на запуск

В верхней части окна размещен список пользователей и групп, которым разрешена работа через DCOM. Нужно добавить в этот список ранее созданную группу «Пользователи OPC». Для этого нужно нажать на кнопку «Добавить...», размещенную под этим списком. Откроется диалоговое окно (Рис. 10), идентичное окну добавления пользователей в группу (Рис. 4). В поле ввода нужно ввести имя группы, нажать на кнопку «Проверить имена», затем (если группа с таким именем была найдена), нажать на кнопку «OK».

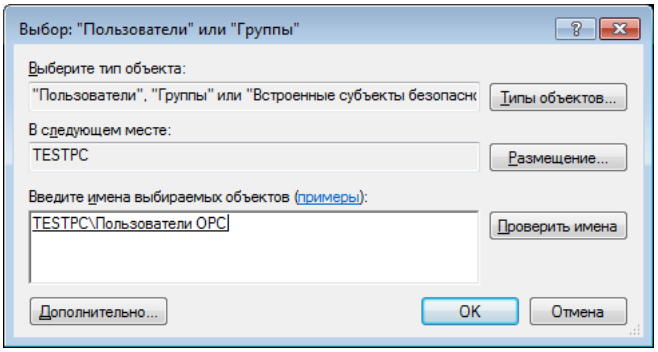

Рис. 10 Добавление группы

Выбранная группа будет добавлена в список пользователей и групп, которым разрешен доступ (Рис. 8). Далее нужно разрешить для этой группы удаленный доступ. Для этого нужно выделить ее (щелчком левой кнопки мыши) и установить флаг «Разрешить» в строке «Удаленный доступ» в таблице прав доступа в нижней части окна свойств. Затем закрыть окно настройки прав доступа, нажав на кнопку «OK».

Таким же образом нужно настроить разрешения на запуск и активацию. Окно настройки прав на запуск вызывается нажатием кнопки «Изменить ограничения...» в группе «Разрешения на запуск и активацию» в окне свойств DCOM (Рис. 7). Будет отображено окно настройки разрешений на запуск и активацию (Рис. 9). Вышеописанным образом нужно добавить в список пользователей и групп группу «Пользователи OPC» и разрешить для нее удаленный запуск и удаленную активацию, установив соответствующие флажки в нижней части окна. Затем закрыть окно нажатием на кнопку «OK».

Теперь окно свойств DCOM (Рис. 7) можно закрыть, подтвердив изменения нажатием на кнопку «OK».

1.3. Настройка системных политик

Если для доступа используются не доменные, а локальные пользователи, нужно проверить значение политики идентификации локальных пользователей при сетевом (удаленном) доступе. При использовании доменных пользователей выполнение нижеописанных настроек не требуется.

Редактирование политик выполняется в оснастке «Редактор локальной групповой политики» (Рис. 11), открываемой командой «gpedit.msc».

В дереве политик в левой части окна нужно найти узел «Параметры безопасности» (в соответствии с рисунком). В правой части окна при этом будет отображен список поли-

тик данного узла. Нужно проверить значение политики «Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей». Значением политики должно быть «Обычная – локальные пользователи удостоверяются как они сами» (Рис. 13).

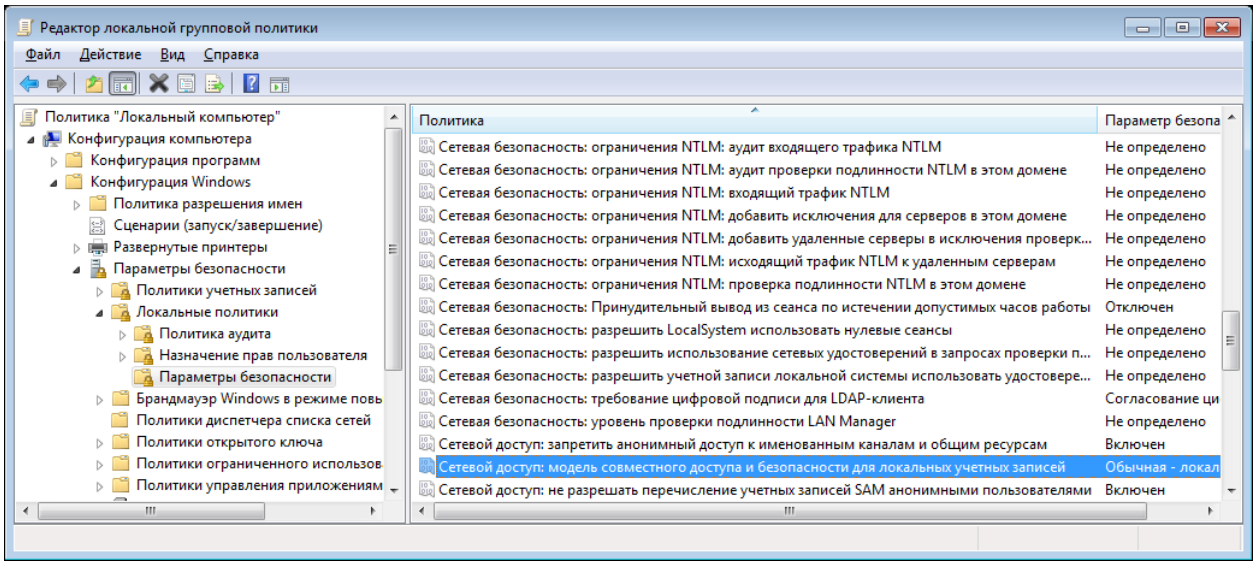

Рис. 11 Настройка политики безопасности

Также необходимо проверить значение политики «Сетевой доступ: разрешать применение разрешений «Для всех» к анонимным пользователям». Значением политики должно быть значение «Включено» (Рис. 12).

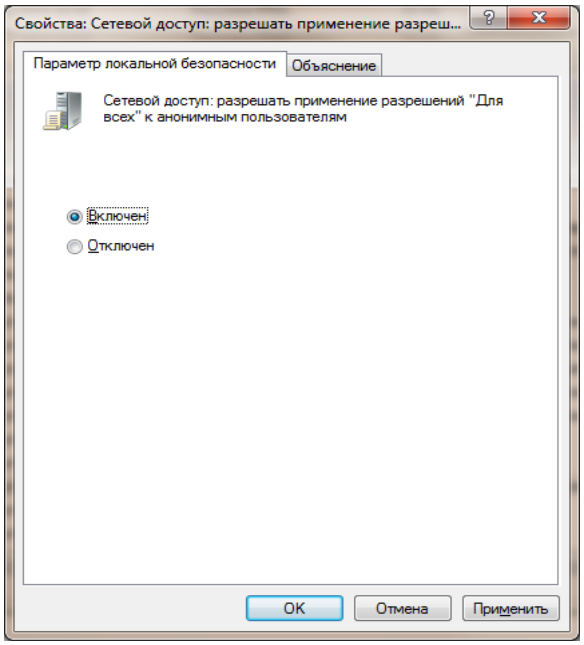

Рис. 12 Разрешать применение разрешений «Для всех» для анонимных пользователей

Дополнительно можно (не обязательно) запретить локальный вход для созданных пользователей «OpcServer» или «OpcClient». Для этого нужно открыть политику «Запретить локальный вход» в группе «Назначение прав пользователя» (Рис. 14), нажать на кнопку

«Добавить пользователя или группу...» и указать этих двух пользователей, после чего закрыть окно нажатием на кнопку «ОК».

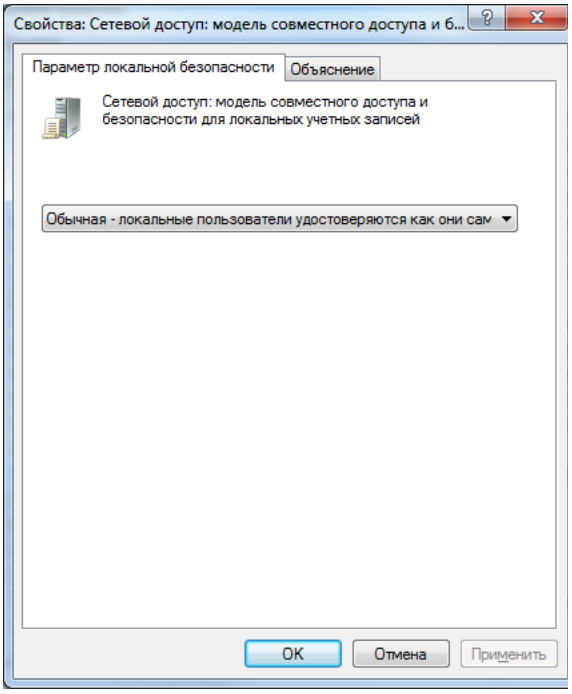

Рис. 13 Модель совместного доступа при сетевом входе

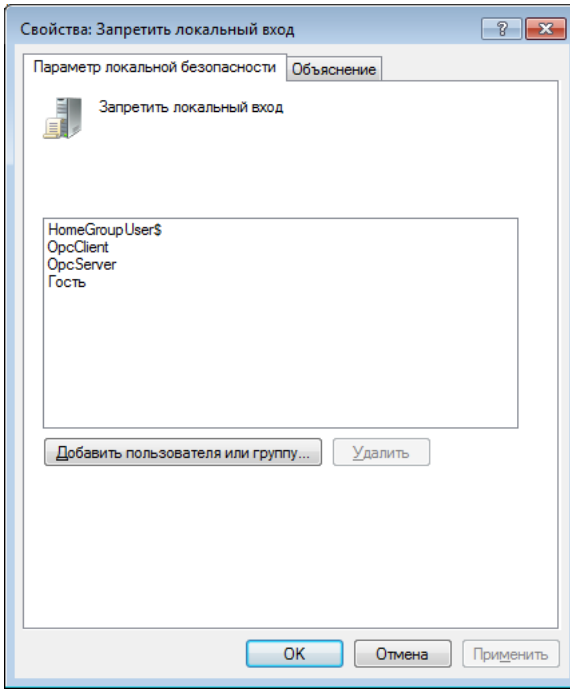

Рис. 14 Запрет локального входа для указанных пользователей

Следует учесть, что запрет локального входа для указанного пользователя делает невозможным запуск приложений от имени этого пользователя. Если OPC-сервер или OPC-клиент запускается как консольное либо оконное приложение (не как служба), то локальный вход для соответствующего пользователя обязательно должен быть разрешен.

1.4. Настройка брандмауэра

Модель DCOM использует TCP-соединение с динамическим назначением портов. Если клиентский либо серверный компьютер защищен брандмауэром, то требуется его настройка. Наиболее простым вариантом является добавление исключения для приложений OPC-сервера (на серверном компьютере) и OPC-клиента (на клиентском компьютере). Для встроенного брандмауэра Windows для этого требуется открыть окно «Панель управления» и в нем выбрать пункт «Брандмауэр Windows» (если в «Панели управления» включен просмотр по категориям, то требуется выбрать категорию «Система и безопасность»).

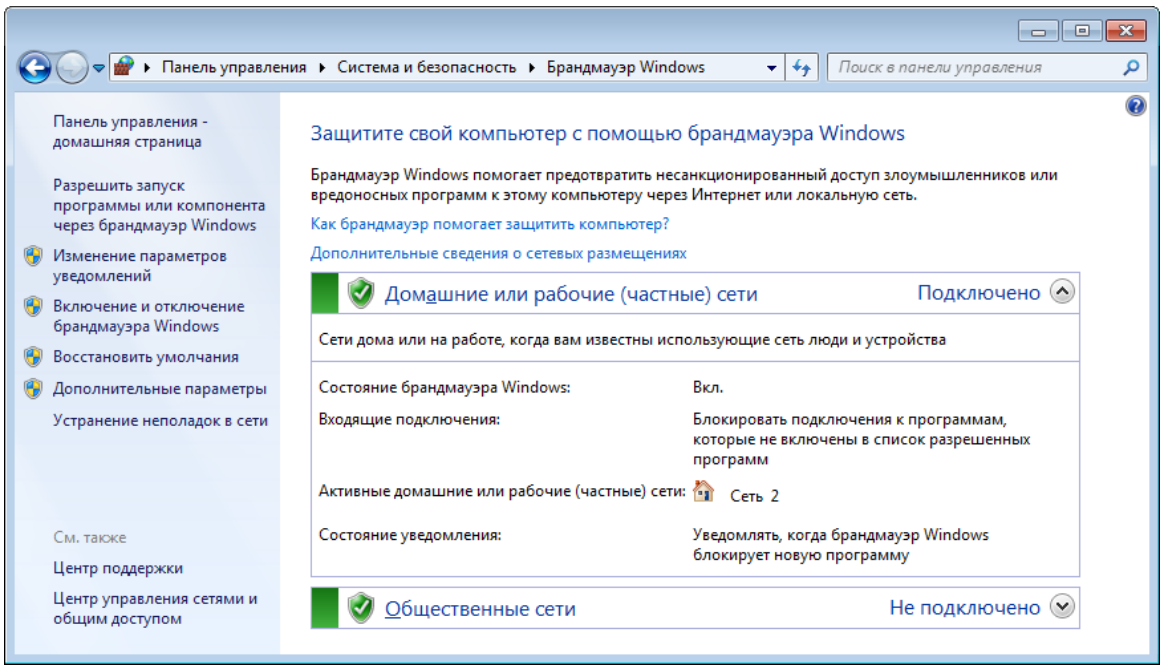

Рис. 15 Окно настройки брандмауэра Windows

В окне настройки брандмауэра (Рис. 15) в списке действий, расположенном в левой части окна, требуется выбрать пункт «Разрешить запуск программы или компонента через брандмауэр Windows». В открывшемся окне (Рис. 16) нажать на кнопку «Разрешить другую программу...» и выбрать исполняемый файл OPC-сервера (OPC-клиента). Затем закрыть окно разрешений нажатием на кнопку «OK».

При необходимости можно явно указать диапазон портов для работы DCOM и задать разрешения брандмауэра только для этого диапазона, но это может повлиять на работу других приложений, установленных в системе.

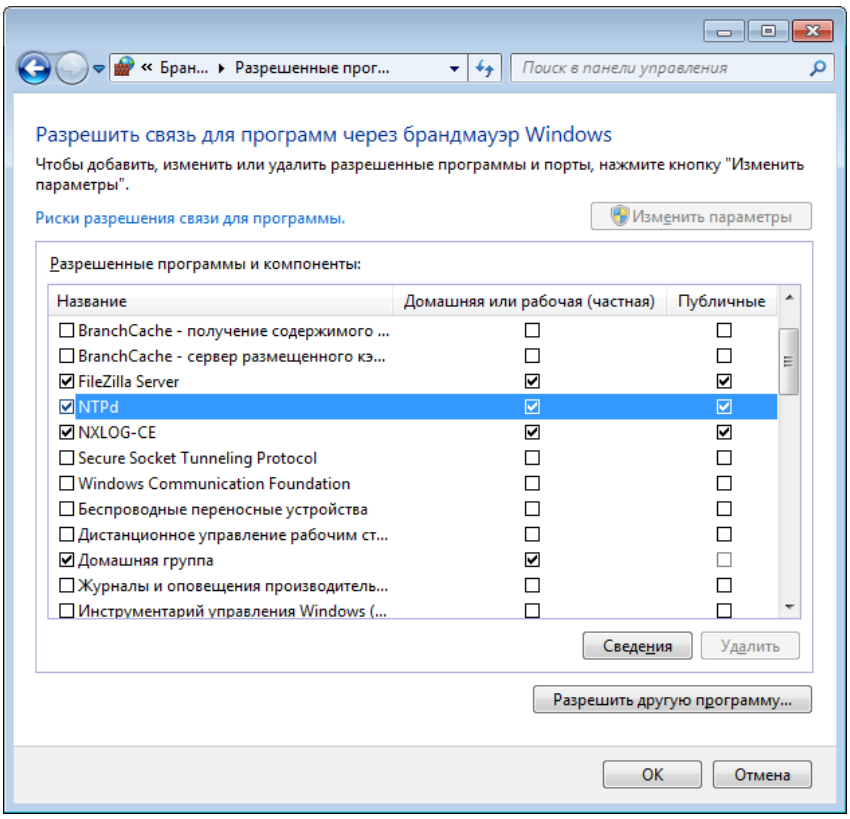

Рис. 16 Список разрешений брандмауэра

Если в системе установлены сторонние файерволы, они также должны быть настроены.

2. НАСТРОЙКА СЕРВЕРНОЙ ЧАСТИ

Предполагается, что на серверной стороне расположен (запущен) сервер OPC, для которого требуется настроить разрешения доступа. Действия, описанные в главе «Общие настройки», должны быть уже выполнены, и в системе должны существовать пользователи «OpcServer» и «OpcClient», объединенные в группу «Пользователи OPC». В данной главе настраивается доступ непосредственно к серверу OPC, а также определяются параметры его работы.

2.1. Настройка DCOM для сервера OPC

Для настройки DCOM непосредственно для сервера OPC нужно еще раз открыть окно оснастки «Службы компонентов» (команда «dcomcnfg») и выбрать узел «Настройка DCOM». В правой части окна появится список всех COM-компонентов, зарегистрированных на данном компьютере (Рис. 17).

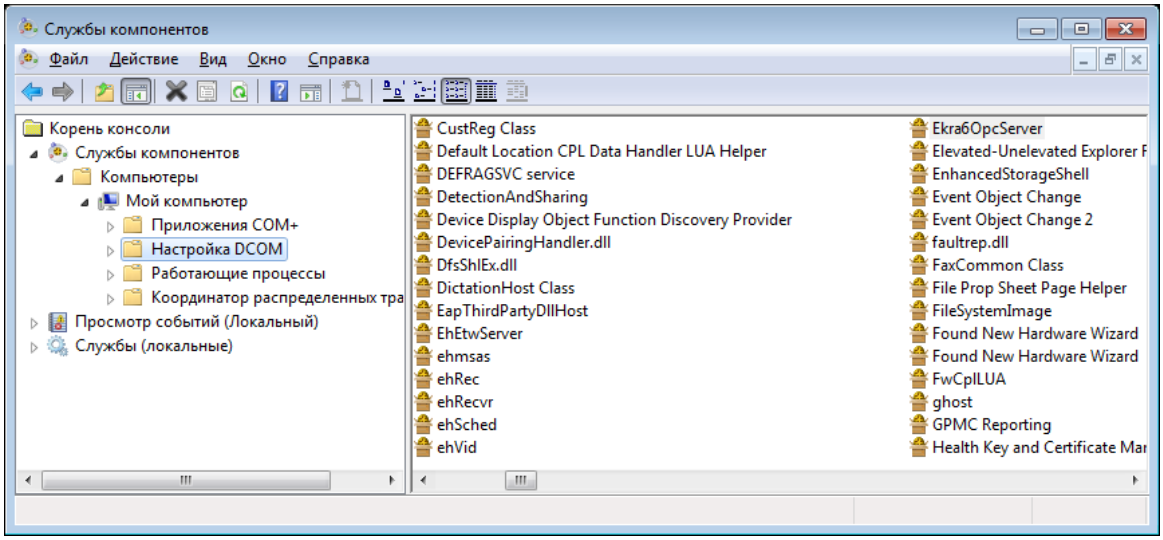

Рис. 17 Список COM-компонентов в системе

В этом списке нужно найти компонент сервера (в нашем случае это элемент с именем «Ekra6OpcServer») и из его контекстного меню вызвать пункт «Свойства». Откроется диалоговое окно свойств этого компонента (Рис. 18). В нем нужно открыть вкладку «Безопасность» (Рис. 19), на которой настраиваются права доступа к данному компоненту. В группе «Разрешения на запуск и активацию» нужно установить переключатель из положения «По умолчанию» в положение «Настроить». При этом станет активной кнопка «Изменить...». При нажатии на эту кнопку будет отображено диалоговое окно настроек «Разрешение на запуск и активацию» (Рис. 9). В этом диалоге в список пользователей и групп нужно добавить группу «Пользователи OPC» и выставить для нее все флаги разрешений, после чего закрыть диалог нажатием на кнопку «OK». Точно также настроить разрешения на доступ: выставить соответствующий переключатель в положение «Настроить», нажать на кнопку «Изменить...», в открывшемся диалоге добавить группу «Пользователи OPC» и выставить для нее все флаги разрешений.

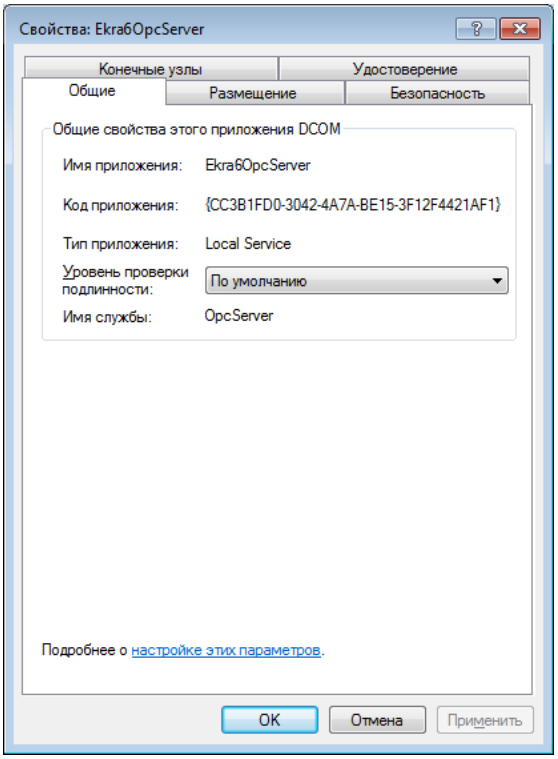

Рис. 18 Общие свойства компонента сервера

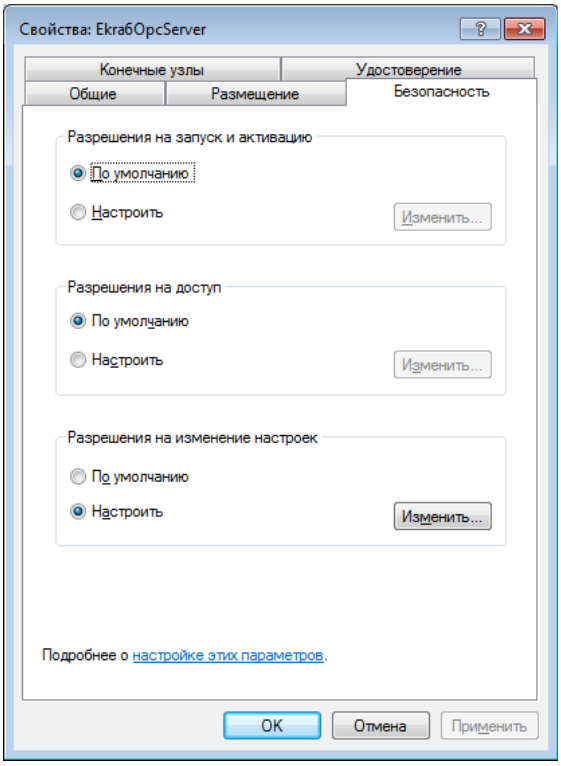

Рис. 19 Настройки безопасности компонента сервера

Затем перейти на вкладку «Удостоверение» (Рис. 20). Здесь задается пользователь, от имени которого будет выполняться приложение OPC-сервера.

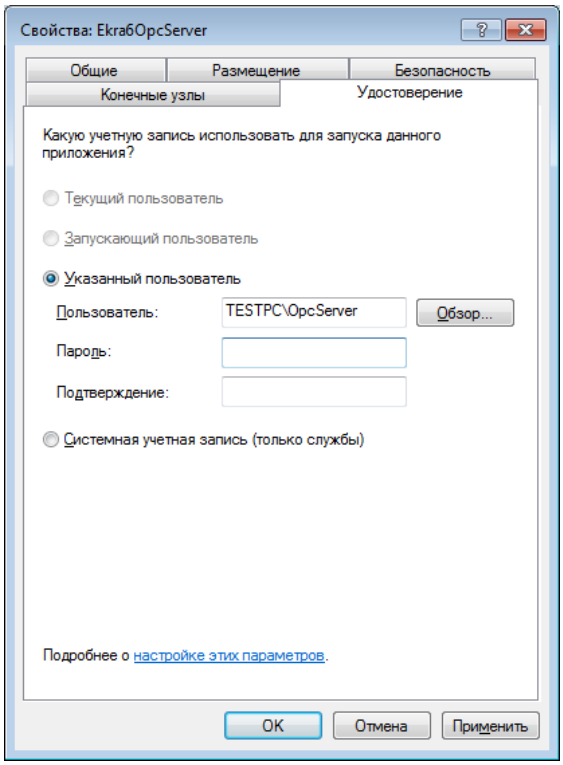

Рис. 20 Выбор учетной записи для запуска OPC-сервера

Нужно выставить переключатель в значение «Указанный пользователь». Станут активными поля ввода «Пользователь», «Пароль» и «Подтверждение». В поле ввода «Пользователь» нужно ввести имя учетной записи, от имени которой будет запускаться сервер: в нашем случае это пользователь «OpcServer», добавленный при выполнении действий из главы «Настройка учетных записей». В поля ввода «Пароль» и «Подтверждение» нужно ввести пароль этого пользователя, указанный при его создании.

После этого можно закрыть диалог свойств, нажав на кнопку «ОК».

В качестве побочного эффекта этих действий пользователь «OpcServer» получит право на вход в качестве службы.

2.2. Дополнительные настройки пользователя

После выполнения действий из пункта «Настройка DCOM для сервера OPC» сервер OPC будет запускаться от имени пользователя «OpcServer». Требуется убедиться, что прав этого пользователя достаточно для работы приложения сервера. Возможно, потребуется предоставить доступ этому пользователю к каким-то каталогам, в которых лежат файлы, необходимые для работы сервера. Набор требуемых прав и действий для их предоставления может быть различен для разных приложений, и поэтому в данном документе не указывается.

2.3. Компонент «OpcEnum»

Этот компонент предоставляет клиентам информацию об установленных на данной системе OPC-серверах. Если для работы клиента необходима эта информация, то следует установить этот компонент на компьютер сервера и настроить для него разрешения доступа. При этом придется разрешить удаленный доступ для анонимного пользователя, что может быть нежелательно с точки зрения безопасности.

Для настройки DCOM требуется командой «dcomcnfg» открыть окно оснастки «Службы компонентов» (Рис. 5). В дереве в левой части окна выбрать узел «Мой компьютер» и открыть его свойства (Рис. 7). Перейти на вкладку «Безопасность COM», нажать на кнопку «Изменить ограничения» в группе «Права доступа» (Рис. 8). В открывшемся окне в списке пользователей найти пользователя «АНОНИМНЫЙ ВХОД» и выставить для него разрешение «Удаленный доступ». После этого последовательно закрыть окно настройки прав доступа и окно свойств нажатием на кнопку «ОК».

Теперь нужно настроить права доступа непосредственно для компонента «OpcEnum». Процесс настройки аналогичен настройке OPC-сервера из пункта «Настройка DCOM для сервера OPC». В окне оснастки «Службы компонентов» нужно выбрать узел «Настройка DCOM» (Рис. 17). В открывшемся списке найти компонент «OpcEnum» и открыть его свойства. Перейти на вкладку «Безопасность» (Рис. 19). В группе «Разрешения на запуск и активацию» выставить переключатель в положение «Настроить», нажать на кнопку «Изменить...». В появившемся окне (Рис. 9) нажать на кнопку «Добавить...». В открывшемся окне выбора пользователя ввести имя группы «Пользователи OPC», нажать на кнопку «Проверить имена», за-

тем закрыть окно нажатием на кнопку «ОК». В результате в списке пользователей в окне разрешений должна появиться соответствующая группа. Нужно выделить ее и в таблице разрешений (в нижней части окна) выставить все флаги в «Разрешить». Затем закрыть окно разрешений нажатием на кнопку «ОК». Таким же образом настроить разрешения на доступ, после чего закрыть окно свойств компонента нажатием на кнопку «ОК».

По аналогии с пунктом «Настройка брандмауэра» настроить разрешения для исполняемого файла приложения «OpcEnum.exe».

После выполнения этих действий компонент «OpcEnum» должен оказаться доступен для OPC-клиента, который сможет получить список серверов и их идентификаторы («AppID» и «CLSID»). По завершении настройки клиента рекомендуется снова запретить удаленный доступ для пользователя «АНОНИМНЫЙ ВХОД» в настройках DCOM. При этом следует отметить, что нельзя удалять самого пользователя из списка прав доступа: локальный доступ для пользователя «АНОНИМНЫЙ ВХОД» должен быть разрешен. В противном случае могут возникнуть проблемы при работе операционной системы.

3. НАСТРОЙКА КЛИЕНТСКОЙ ЧАСТИ

Предполагается, что на клиентской стороне расположен OPC-клиент, который должен подключаться к серверу и запрашивать с него данные. Действия, описанные в главе «Общие настройки», должны быть уже выполнены, и в системе должны существовать пользователи «OpcServer» и «OpcClient», объединенные в группу «Пользователи OPC».

3.1. Настройка DCOM

Если клиент использует подписку для получения данных с сервера (обратные вызовы), желательно настроить DCOM на разрешение вызовов со стороны сервера. Для этого нужно открыть окно оснастки «Службы компонентов» (Рис. 5) и открыть свойства узла «Мой компьютер» на вкладке «Безопасность COM» (Рис. 7). В группе «Права доступа» нажать на кнопку «Изменить умолчания...». Откроется окно «Права доступа» (Рис. 8). Добавить в список пользователей группу «Пользователи OPC» (с помощью кнопки «Добавить...») и разрешить для нее удаленный доступ. Последовательно закрыть окно прав доступа и окно свойств узла «Мой компьютер» нажатием на кнопки «OK».

Вообще данная настройка не вполне безопасна, так как влияет на все запущенные в системе процессы. Рекомендуется сначала проверить работу клиента без выполнения данной настройки, и выполнять ее только в том случае, если иначе работа клиента невозможна.

3.2. Настройка запуска OPC-клиента

На последнем этапе настройки требуется обеспечить запуск OPC-клиента от имени соответствующего пользователя.

Если клиент установлен в виде службы, то для ее настройки требуется выполнить следующие действия. Сначала нужно открыть оснастку управления службами (это можно сделать командой «services.msc»). В появившемся окне (Рис. 21) найти нужную службу и в ее контекстном меню выбрать пункт «Свойства». В окне свойств открыть вкладку «Вход в систему», выставить переключатель на значение «С учетной записью» и указать имя учетной записи «OpcClient». В полях «Пароль» и «Подтверждение» указать пароль этого пользователя. После этого закрыть окно свойств нажатием на кнопку «OK».

Требуется учесть, что после этих действий служба (OPC-клиент) будет выполняться от имени указанного пользователя, и прав этого пользователя должно хватать для ее корректной работы. Например, если OPC-клиент использует какие-то файлы конфигурации, то указанный пользователь должен иметь доступ к этим файлам.

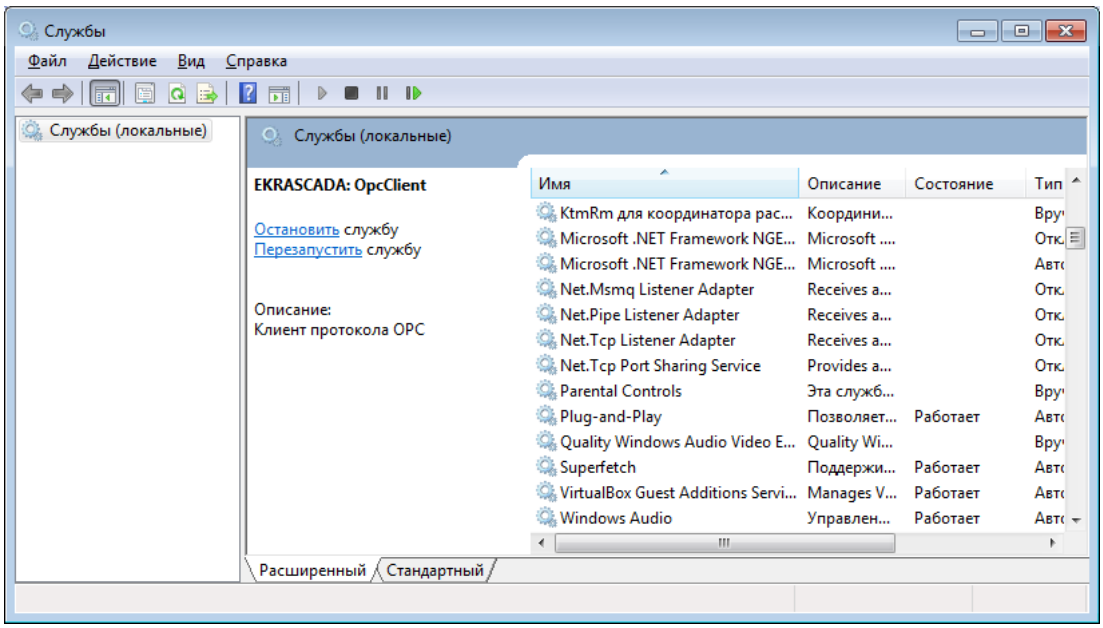

Рис. 21 Окно оснастки настройки служб

Если клиент запускается в виде консольного либо оконного приложения, для запуска его от имени указанного пользователя можно воспользоваться командой «runas». Пример использования: «runas /user:OpcClient opcclient.exe», где «opcclient.exe» – имя исполняемого файла OPC-клиента.

4. ПРИЛОЖЕНИЯ

4.1. Настройка прав доступа пользователя к каталогам

Пусть некоторое приложение (OPC-сервер) запускается от имени пользователя «OpcServer» и в процессе работы обращается к файлам в каталоге (директории) «C:\Data». Для того, чтобы обеспечить корректную работу приложения, требуется предоставить указанному пользователю права доступа к данному каталогу.

В контекстном меню указанного каталога нужно выбрать пункт свойства (Рис. 22). В открывшемся окне свойств открыть вкладку «Безопасность» (Рис. 23). Нажать на кнопку «Изменить...». Будет открыто окно «Разрешения для группы...». В нем нажать на кнопку «Добавить...». В открывшемся окне (Рис. 24) указать нужного пользователя, затем закрыть это окно нажатием на кнопку «OK». В результате список пользователей в окне «Разрешения...» будет изменен: в него будет добавлен выбранный пользователь. Нужно выделить этого пользователя и в таблице «Разрешения для группы...» выставить необходимые права. Затем последовательно закрыть окна «Разрешения для группы...» и «Свойства...» нажатиями на кнопки «OK».

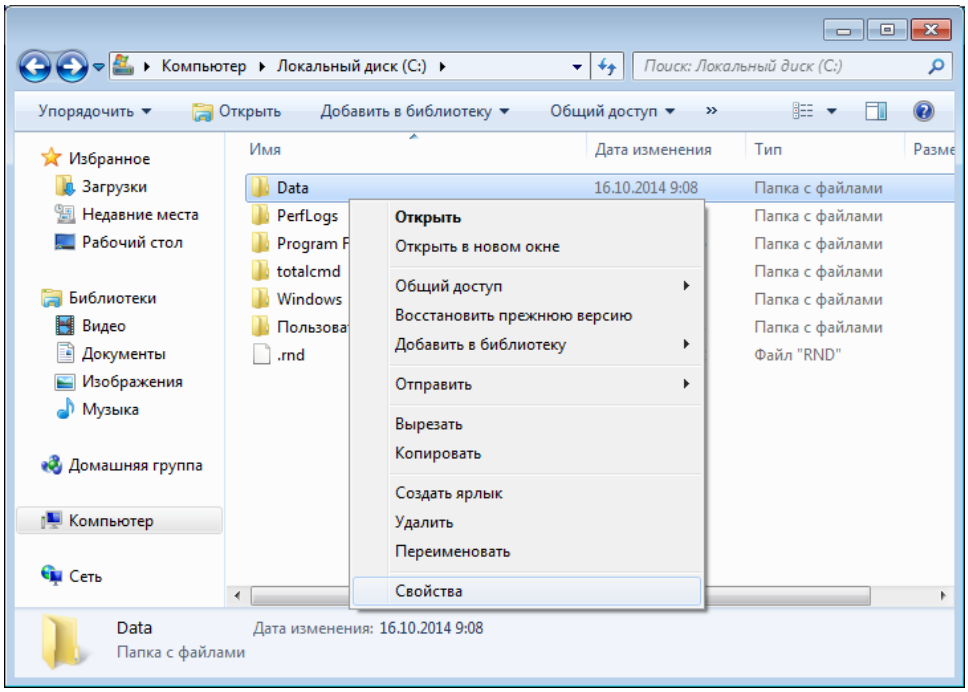

Рис. 22 Контекстное меню каталога

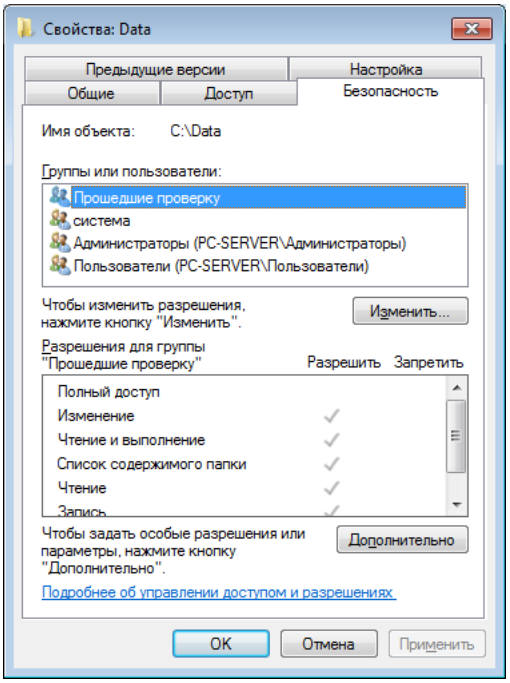

Рис. 23 Окно свойств каталога

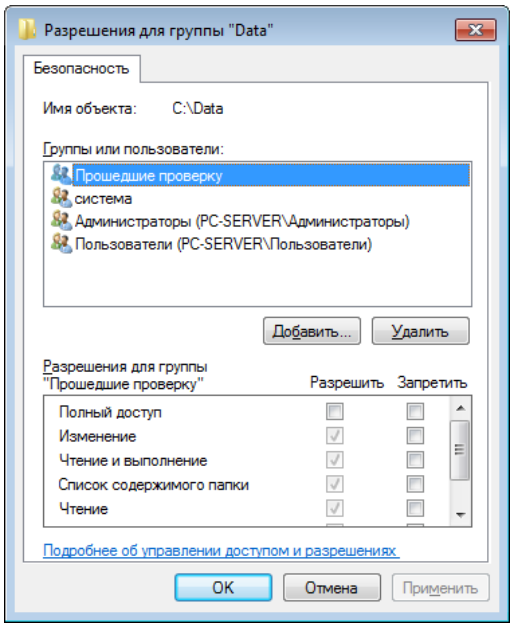

Рис. 24 Редактирование прав доступа к каталогу

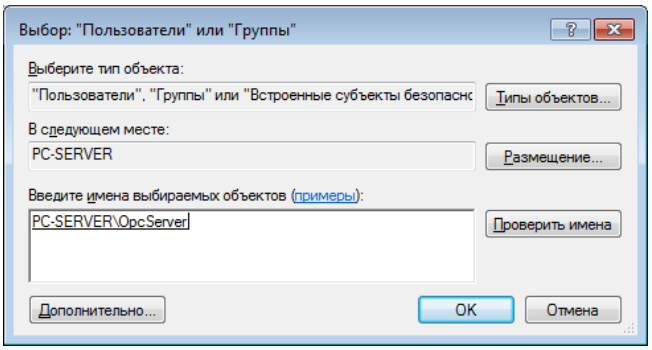

Рис. 25 Выбор пользователя