Настройка DCOM для работы с удаленными OPC-серверами

Руководство Пользователя

2014

Настройка DCOM для работы с удаленными OPC-серверами.
Руководство Пользователя/1-е изд.

Настоящее руководство предназначено для обучения настройке DCOM для разных ОС.

Документ содержит описание процедуры настройки компонентов DCOM для операционных систем Windows XP, Windows 7, Windows 2008 Server.

ООО «КРУГ-Софт»

440028, г. Пенза, ул. Титова, 1

Телефоны: (841-2) 49-97-75; 55-64-97; 49-94-14; 48-34-80; 55-64-95

Факс: (841-2) 55-64-96

e-mail – **krug@krug2000.ru**

e-mail – **support@opcserver.ru**

http://www.krugsoft.ru

http://opcserver.ru

📖 СОДЕРЖАНИЕ

Стр.

1 ОБЩИЕ СВЕДЕНИЯ

Технология OPC (OLE for Process Control) основана на технологиях Microsoft COM/DCOM.
В рамках спецификации OPC существуют 2 понятия: OPC-сервер и OPC-клиент.
Чтобы OPC-клиент мог подключиться к OPC-серверу на другом компьютере (в рамках одной сети) необходимо корректно сконфигурировать службу DCOM. В основном данная настройка сводится к конфигурированию соответствующих прав доступа и осуществляется стандартными средствами ОС Windows.

Работа с удаленным OPC-сервером проиллюстрирована на рисунке 1.1.
Синхронное подключение OPC-клиента (рисунок 1), создаёт только соединение 1. Соединение 2 устанавливается только в случаях выполнения асинхронных вызовов для доставки клиенту запрошенных данных.

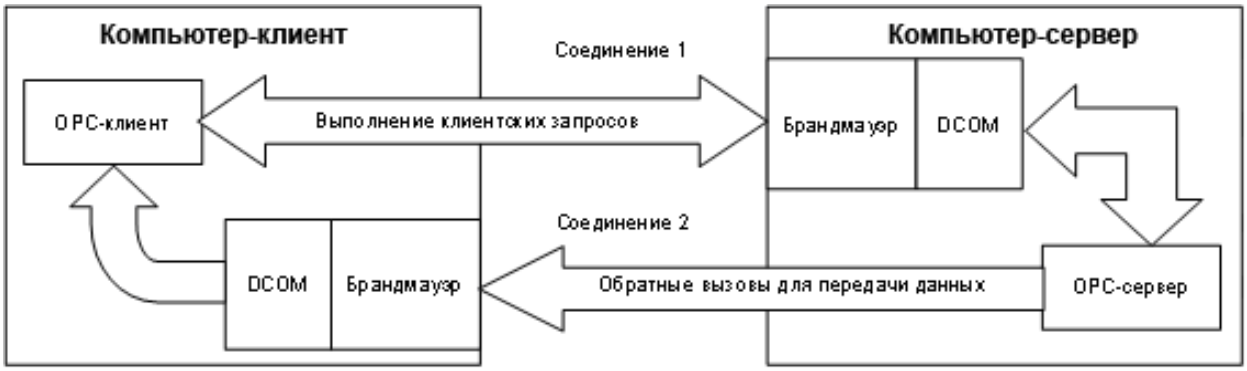

Рисунок 1.1 — Схема взаимодействия с OPC-сервером

В данном документе содержатся сведения о конфигурировании клиентского компьютера и о конфигурировании компьютера с OPC-сервером. Для настройки выполните последовательно все пункты данного руководства. В зависимости от того, находятся ли компьютеры в домене или в рабочей группе, нужно выполнить только один из следующих пунктов.

2 СОЗДАНИЕ И НАСТРОЙКА УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ

2.1 Настройка учетных записей для Windows XP

2.1.1 Настройка компьютеров, находящихся в домене

☝**ВНИМАНИЕ!!!**

Если есть возможность использовать доменную подсистему Windows, то нужно обязательно это сделать. Вы получите выигрыш в скорости работы и сделаете настраиваемою систему более надежной.

При настройке компьютеров нужно убедиться в том, что оба компьютера находятся в одном домене, или что домены, к которым они относятся, соединены доверительными отношениями. При этом нужно использовать именно учетные записи пользователей домена, а не локальные.

При настройке компьютеров, входящих в домен, выполните следующие шаги:

1. На компьютере, где установлен OPC-сервер, или на контроллере домена рекомендуем создать учетную запись группы пользователей. Для этого необходимо запустить проводник (**Win+E**) и выполнить последовательность действий, изображенную на рисунке 2.1. Имя группы может быть любым (например, «**Users OPC**»). В дальнейшем созданная группа будет использоваться в настройках OPC-серверов.

   Шаг создания группы можно пропустить и использовать при настройках OPC-серверов учетные записи пользователей домена. Но мы рекомендуем использовать для настройки OPC группу пользователей. В случаях, когда предполагается, что к OPC-серверу будет обращаться несколько разных пользователей, их учетные записи достаточно включить в созданную группу («**Users OPC**»). При таком подходе настроенную систему проще сопровождать. Например, если изменится имя пользователя, запускающего OPC-клиент, нужно будет добавить нового пользователя в группу. Настройки DCOM при этом изменять не нужно.

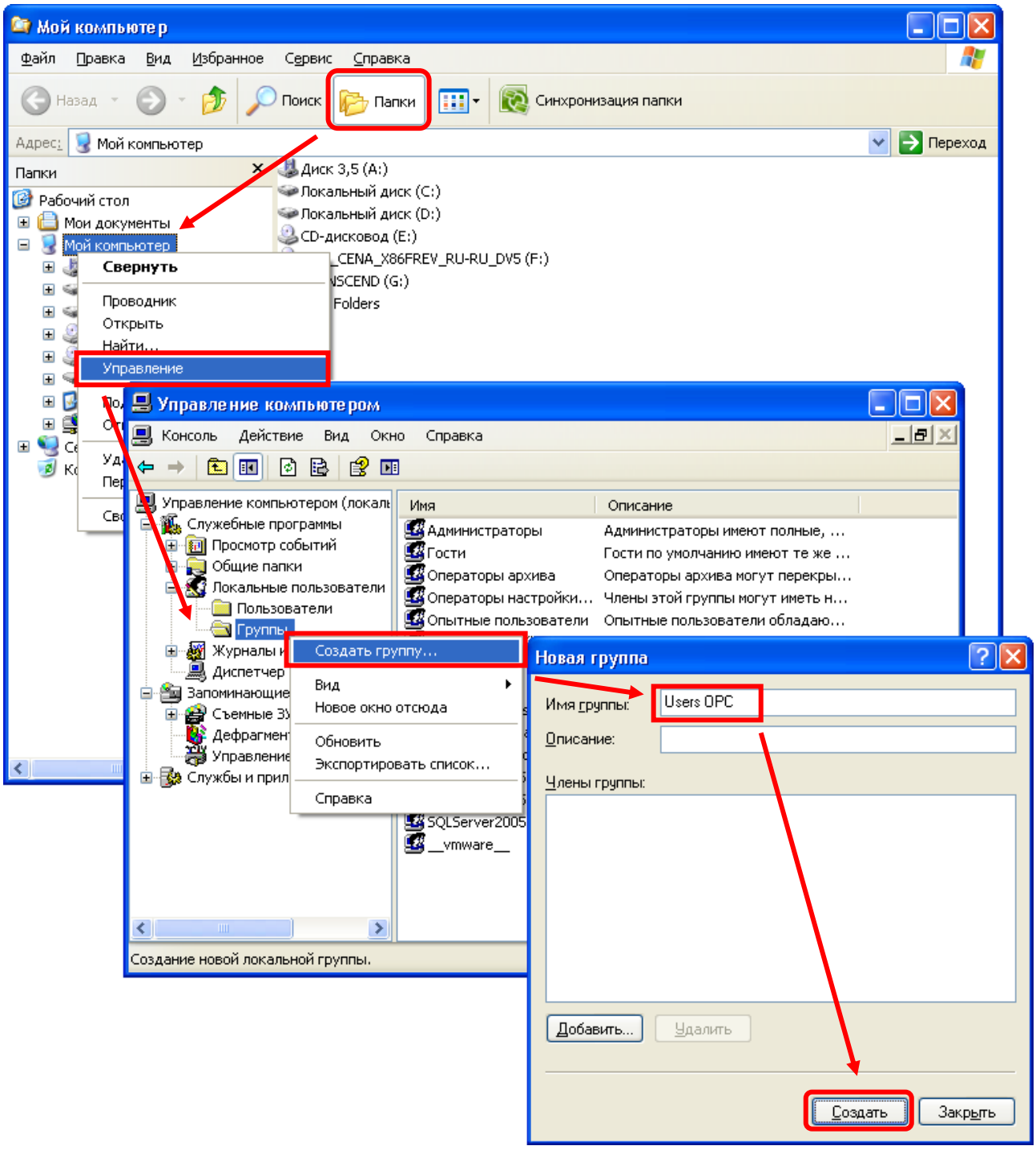

Рисунок 2.1 — Создание группы пользователей

Если будет использована группа, созданная на контроллере домена, ее можно использовать при настройке OPC-серверов на всех компьютерах, включенных в домен. Таким образом, список пользователей, имеющих доступ к OPC-серверам, будет глобальный для всего домена. И может редактироваться централизованно на

контроллере домена. Если для каждого компьютера с OPC-сервером нужны индивидуальные права доступа пользователей, можно использовать локальную учетную запись группы.

Начиная с версии Windows Server 2003, в операционной системе уже имеется группа по работе с DCOM – «Пользователи DCOM». Можно использовать ее для настройки OPC-серверов.

2 В группу, созданную на шаге 1 («**Users OPC**» или «**Пользователи DCOM**»), добавьте учетные записи пользователей домена, которым будет разрешен доступ к OPC-серверу (рисунок 2.2). Если шаг 1 был пропущен, в дальнейших настройках вместо учетной записи группы используйте учетные записи пользователей домена.

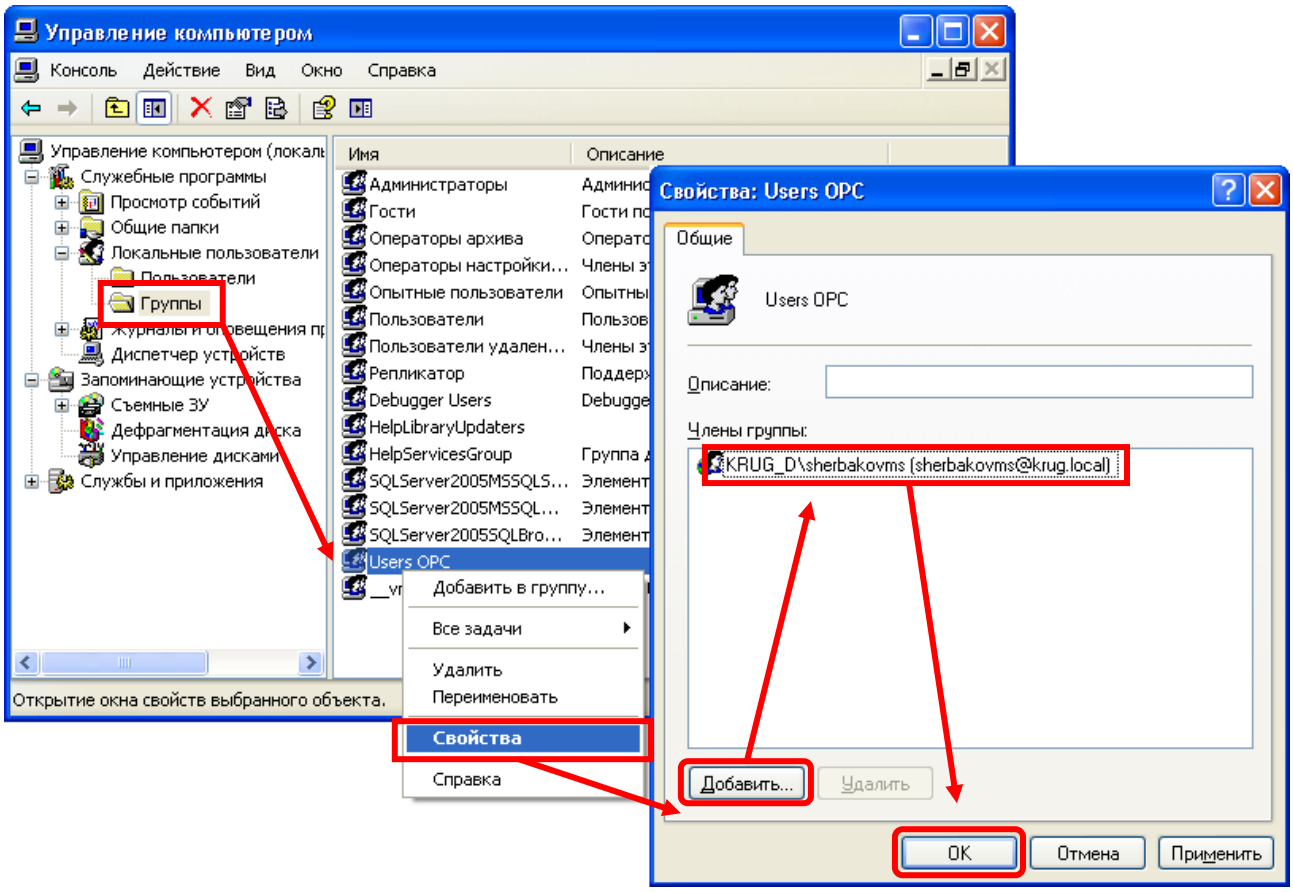

Рисунок 2.2 — Добавление учетной записи пользователя в группу

☝**ВНИМАНИЕ!!!**

Если клиент и сервер являются членами одного домена или разных доменов, имеющих между собой доверительные отношения, то в этом случае локальные учётные записи пользователей при выполнении вызовов DCOM игнорируются и настройки, сделанные для них, будут не действительны. Нужно использовать учетные записи пользователей домена!

Если планируется использовать несколько OPC-клиентов для подключения к OPC-серверу, и клиенты будут запущены под разными пользователями, нужно повторить шаг 2 для каждого пользователя.

2.1.2 Настройка компьютеров, находящихся в рабочей группе

Для настройки компьютеров, находящихся в рабочей группе, выполните следующие шаги:

1. На компьютере сервера рекомендуем создать локальную учетную запись группы пользователей (рисунок 2.1). Имя группы может быть любым (например, «**Users OPC**»).

   В дальнейшем созданная группа будет использоваться в настройках OPC-серверов. Шаг создания группы можно пропустить и использовать при настройках OPC-серверов учетные записи пользователей. Но мы рекомендуем использовать для настройки OPC учетную запись группы. В случаях, когда предполагается, что к OPC-серверу будет обращаться несколько разных пользователей, их учетные записи достаточно включить в созданную группу («**Users OPC**»). При таком подходе настроенную систему проще сопровождать. Например, если изменится имя пользователя, запускающего OPC-клиент, нужно будет создать нового пользователя и добавить его в группу. Настройки DCOM при этом изменять не нужно.

   Начиная с версии Windows Server 2003, в операционной системе уже существует группа по работе с DCOM – «**Пользователи DCOM**». Можно использовать ее для настройки OPC-серверов.

2 На компьютере сервера создайте учетную запись того пользователя, от имени которого запускается OPC-клиент (рисунок 2.3). То есть, имя и пароль в новой учётной записи должны совпадать с именем и паролем пользователя, запускающего OPC-клиент на клиентском компьютере.

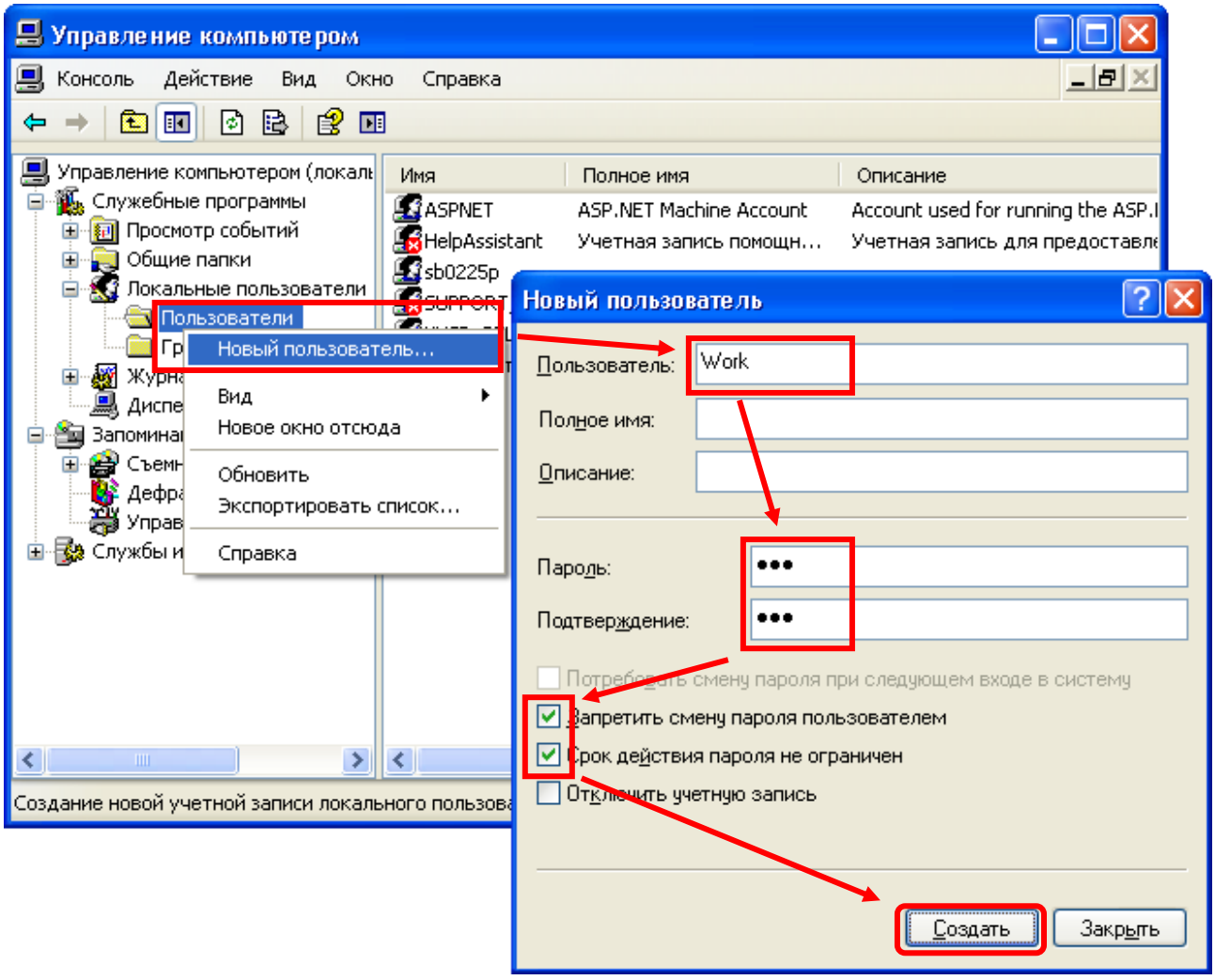

Рисунок 2.3 — Создание учетной записи пользователя

ВНИМАНИЕ!!!

Имя и пароль пользователя, запускающего OPC-клиент, и пользователя, которому предоставлен доступ к удаленному OPC-серверу, должны обязательно совпадать.

Созданную учетную запись пользователя нужно добавить в группу, созданную на шаге 1 («**Users OPC**» или «**Пользователи DCOM**», смотрите рисунок 2.4). Если шаг 1 был пропущен, учетная запись созданного пользователя должна использоваться в дальнейших настройках вместо учетной записи группы.

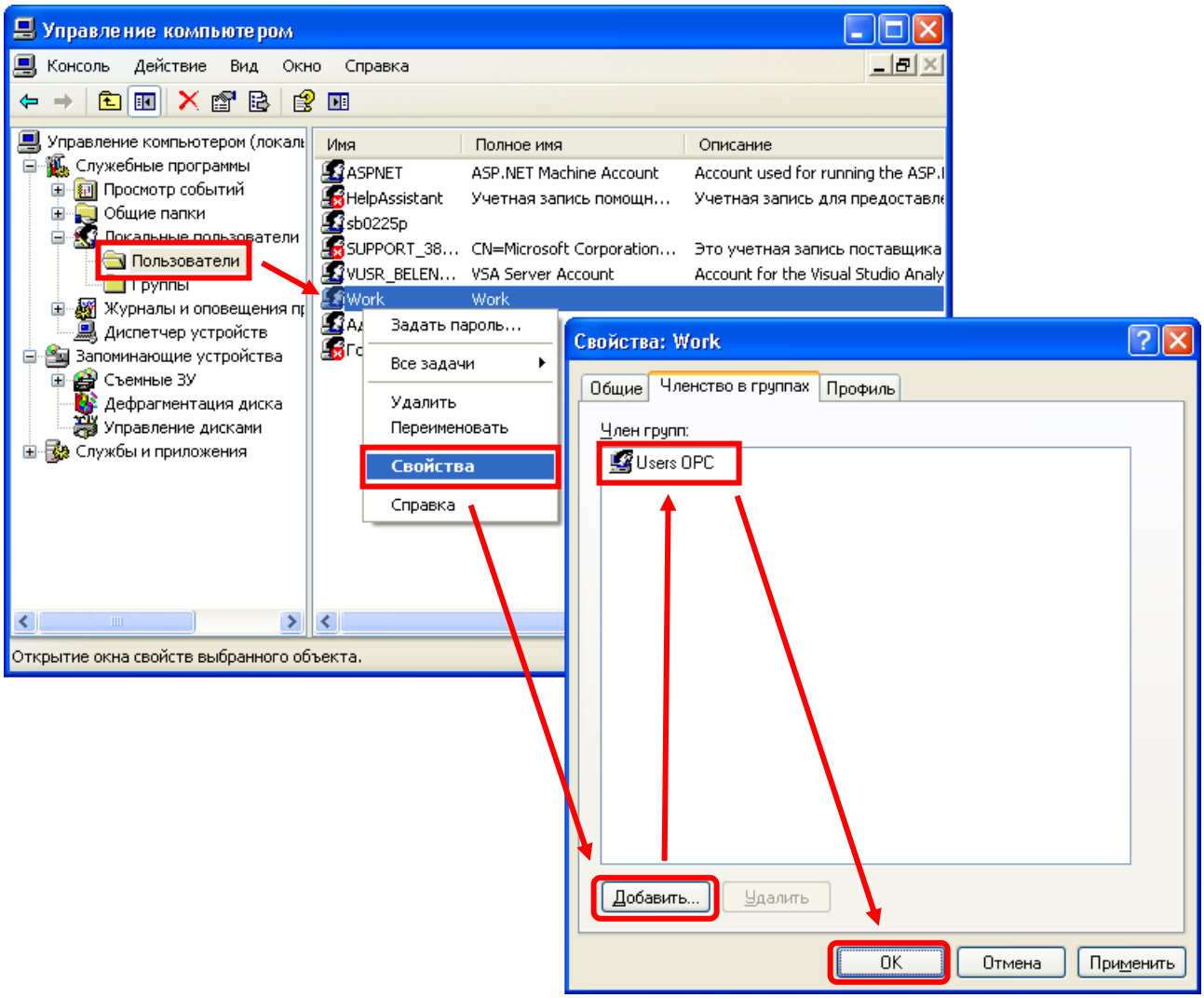

Рисунок 2.4 — Добавление созданного пользователя в группу

Если планируется использовать несколько OPC-клиентов для подключения к OPC-серверу, и клиенты будут запущены под разными пользователями, нужно повторить шаг 2 для каждого пользователя.

3 На компьютере клиента должна существовать учетная запись пользователя, под которой будет запущен OPC-сервер.

Если такая учетная запись будет отсутствовать, асинхронный опрос OPC-сервера станет не возможен. После завершения настроек OPC-сервера и выбора запускающего пользователя, нужно вернуться к этому пункту и, при необходимости, добавить нового пользователя на компьютере клиента.

☝**ВНИМАНИЕ!!!**

Имя и пароль пользователя, под учетной записью которого работает OPC-сервер, и пользователя на компьютере клиента, должны обязательно совпадать.

При настройке OPC-серверов права доступа вновь добавленного пользователя не всегда имеют значение, и их можно ограничить.

2.1.3 Настройка компьютеров, находящихся в смешанной сети

Можно настроить соединение через DCOM между одним компьютером, находящимся в домене, и другим, находящимся в рабочей группе. Подобную конфигурацию сети применять не рекомендуется. Желательно, чтобы оба компьютера были расположены в рабочей группе или являлись членами одного домена или разных доменов, имеющих между собой доверительные отношения.

В данном случае настройка компьютеров производится аналогично настройке компьютеров, расположенных в рабочей группе. Для этого выполните следующие шаги:

1. На компьютере клиента создайте локальную учетную запись пользователя, с помощью которой будет происходить подключение к серверу. И обязательно установите пользователю пароль (рисунок 2.3). Имя пользователя и пароль могут быть любыми, например, «**Work**» с паролем «**999**».

2. На компьютере сервера рекомендуем создать учетную запись локальной группы пользователей (рисунок 2.1). Имя группы может быть любым (например, «**Users OPC**»).

В дальнейшем созданная группа будет использоваться в настройках OPC-серверов. Шаг создания группы можно пропустить и использовать при настройках OPC-серверов учетные записи пользователей. Но мы рекомендуем использовать для настройки OPC учетную запись группы. В случаях, когда предполагается, что к OPC-серверу будет обращаться несколько разных пользователей, их учетные записи достаточно включить в созданную группу («**Users OPC**»). При таком подходе настроенную систему проще сопровождать. Например, если изменится имя пользователя, запускающего OPC-клиент, нужно будет создать нового пользователя и добавить его в группу. Настройки DCOM при этом изменять не нужно.

Начиная с версии Windows Server 2003, в операционной системе уже имеется группа по работе с DCOM – «**Пользователи DCOM**». Можно использовать ее для настройки OPC-серверов.

3 На компьютере сервера необходимо создать локальную учетную запись пользователя с таким же именем и паролем как у пользователя, созданного на шаге 1 («**Work**» с паролем «**999**», рисунок 2.3).

☝**ВНИМАНИЕ!!!**

Учетная запись пользователя домена и локальная учетная запись с таким же именем и паролем считаются различными! Поэтому в смешанной сети необходимо использовать локальные учетные записи, созданные на шаге 1 и 3.

В группу, созданную на шаге 2 («**Users OPC**» или «**Пользователи DCOM**»), нужно добавить учетную запись созданного пользователя («**Work**» с паролем «**999**», рисунок 2.4). Если шаг 2 был пропущен, в дальнейших настройках вместо учетной записи группы нужно использовать созданную учетную запись пользователя.

4 На компьютере клиента настройте сетевое подключение к серверу через учетную запись созданного пользователя.

Для этого откройте «**Пуск / Панель управления / Учетные записи пользователей**».

Если открывшееся окно имеет вид, как на рисунке 2.5, перейдите на вкладку «**Дополнительно**» и в разделе «**Пароли и паспорта .NET**» нажмите кнопку «**Управление паролями**».

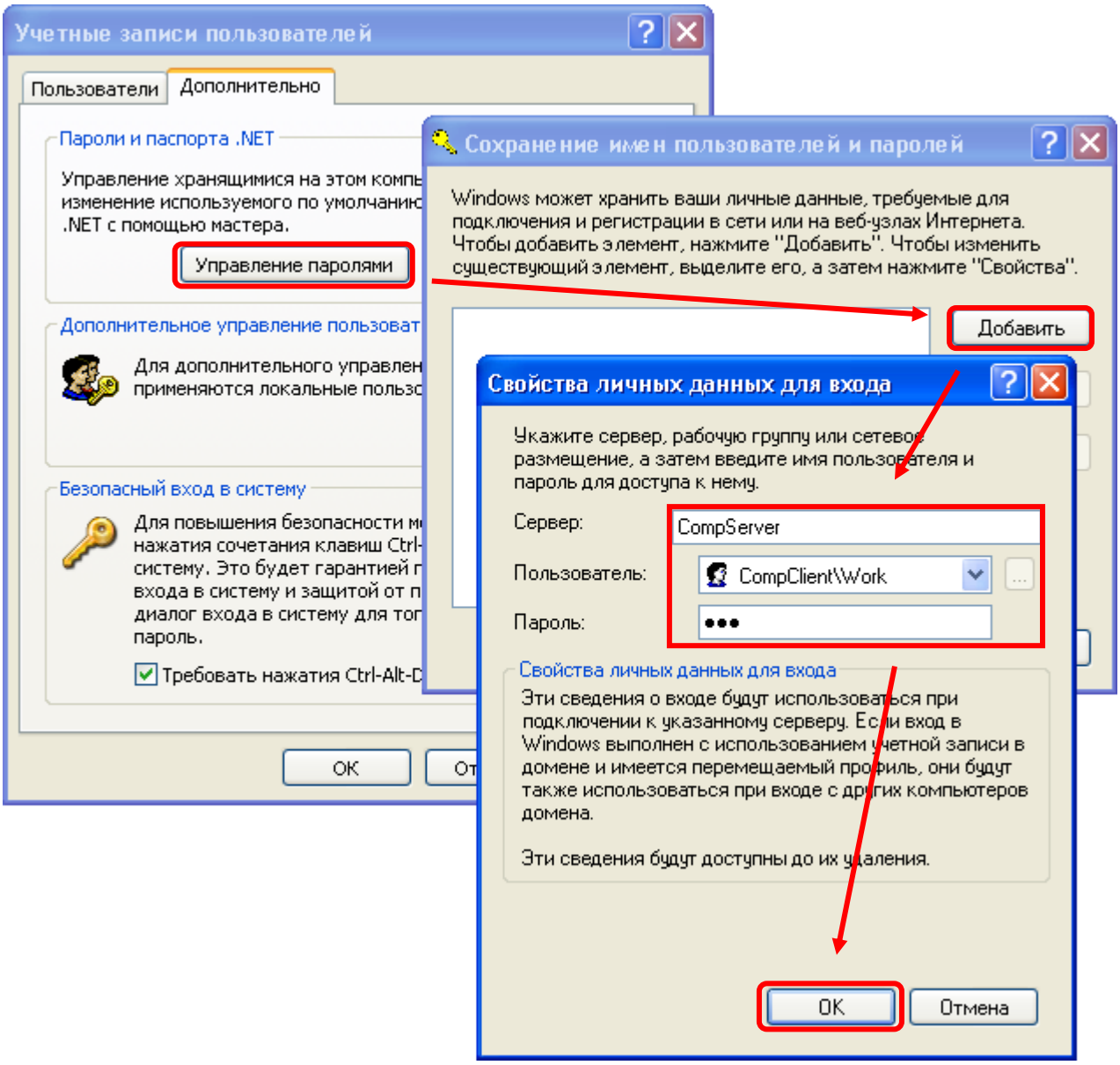

Рисунок 2.5 — Настройка сетевого подключения

В окне «**Сохранение имен пользователей и паролей**» нажмите кнопку «**Добавить**».

В окне «**Свойства личных данных для входа**» введите:

- В поле «**Сервер**» – имя компьютера, на котором установлен OPC-сервер.
- В поле «**Пользователь**» – имя пользователя, созданного на шаге 1. Имя должно быть в форме <имя компьютера клиента>\<имя пользователя>.

- В поле «**Пароль**» – пароль пользователя, созданного на шаге 1.

Нажмите на «**OK**» и закройте окна, чтобы сохранить сделанные изменения.

При настройке OPC-серверов права доступа вновь добавленного пользователя не всегда имеют значение, и их можно ограничить.

☝**Внимание!!!**

После сделанных настроек любые подключения к серверу от клиента (например, подключение к общим папкам на сервере) будут проходить в соответствии с назначенными правами доступа пользователя на компьютере сервере. Поэтому ограничение прав доступа пользователя нужно выполнять осторожно или не производить вообще.

2.2 Настройка учетных записей для Windows 7, Windows 8

2.2.1 Настройка компьютеров, находящихся в домене

☝**ВНИМАНИЕ!!!**

Если есть возможность использовать доменную подсистему Windows, то нужно обязательно это сделать. Вы получите выигрыш в скорости работы и сделаете настраиваемою систему более надежной.

При настройке компьютеров нужно убедиться в том, что оба компьютера находятся в одном домене, или что домены, к которым они относятся, соединены доверительными отношениями. При этом нужно использовать именно учетные записи пользователей домена, а не локальные.

При настройке компьютеров, входящих в домен, выполните следующие шаги:

1 На компьютере, где установлен OPC-сервер, или на контроллере домена рекомендуем создать учетную запись группы пользователей. Для этого необходимо запустить проводник (**Win+E**) и выполнить последовательность действий, изображенную на рисунке 2.6. Имя группы может быть любым (например, «**Users**

OPC»). В дальнейшем созданная группа будет использоваться в настройках OPC-серверов.

Шаг создания группы можно пропустить и использовать при настройках OPC-серверов учетные записи пользователей домена. Но мы рекомендуем использовать для настройки OPC группу пользователей. В случаях, когда предполагается, что к OPC-серверу будет обращаться несколько разных пользователей, их учетные записи достаточно включить в созданную группу («**Users OPC**»). При таком подходе настроенную систему проще сопровождать. Например, если изменится имя пользователя, запускающего OPC-клиент, нужно будет добавить нового пользователя в группу. Настройки DCOM при этом изменять не нужно.

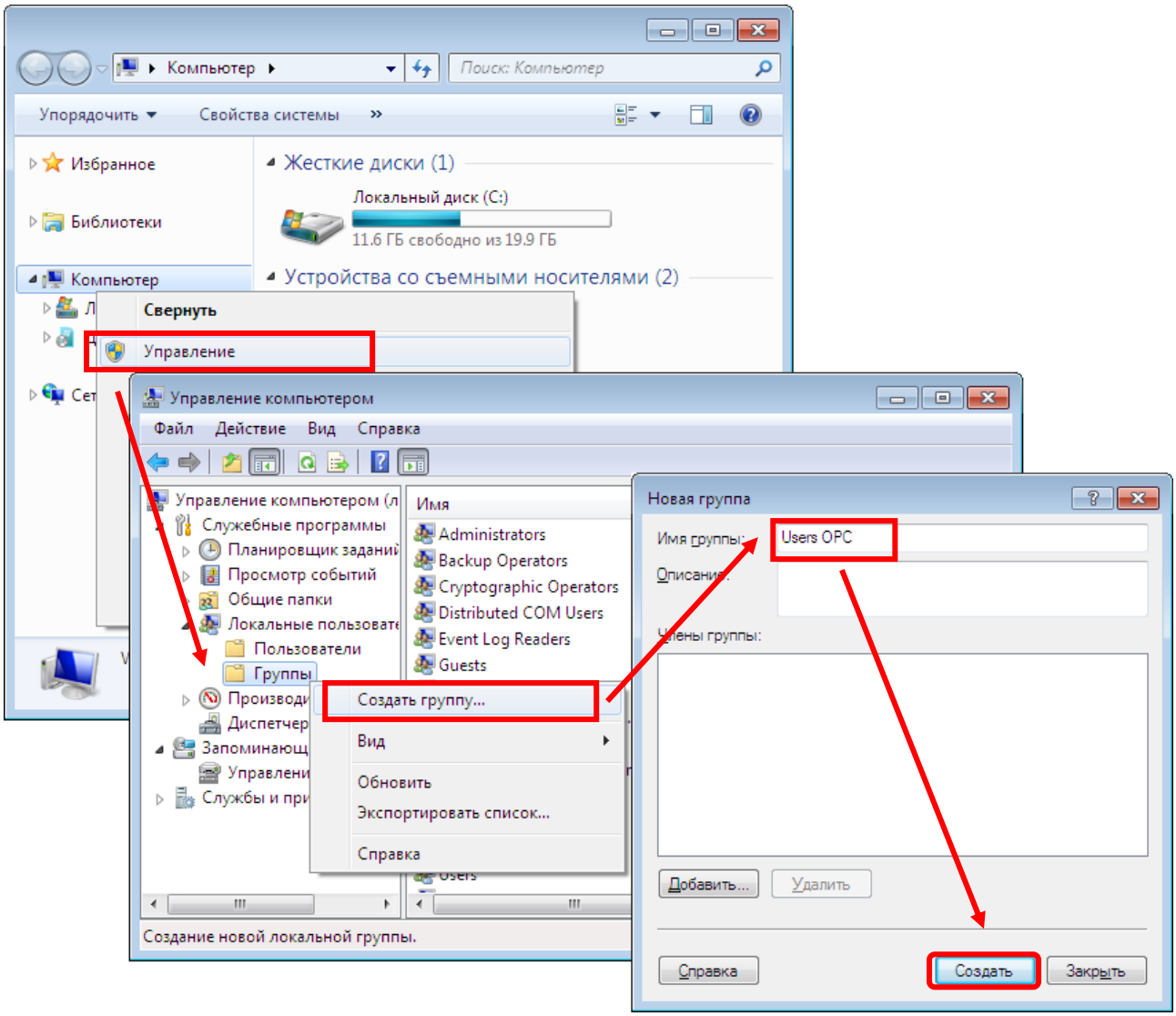

Рисунок 2.6 — Создание группы пользователей

Если будет использована группа, созданная на контроллере домена, ее можно использовать при настройке OPC-серверов на всех компьютерах, включенных в домен. Таким образом, список пользователей, имеющих доступ к OPC-серверам, будет глобальный для всего домена. И может редактироваться централизованно на контроллере домена. Если для каждого компьютера с OPC-сервером нужны индивидуальные права доступа пользователей, можно использовать локальную учетную запись группы.

Начиная с версии Windows Server 2003, в операционной системе уже имеется группа по работе с DCOM – «**Пользователи DCOM**». Можно использовать ее для настройки OPC-серверов.

2 В группу, созданную на шаге 1 («**Users OPC**» или «**Пользователи DCOM**»), добавьте учетные записи пользователей домена, которым будет разрешен доступ к OPC-серверу (рисунок 2.7). Если шаг 1 был пропущен, в дальнейших настройках вместо учетной записи группы используйте учетные записи пользователей домена.

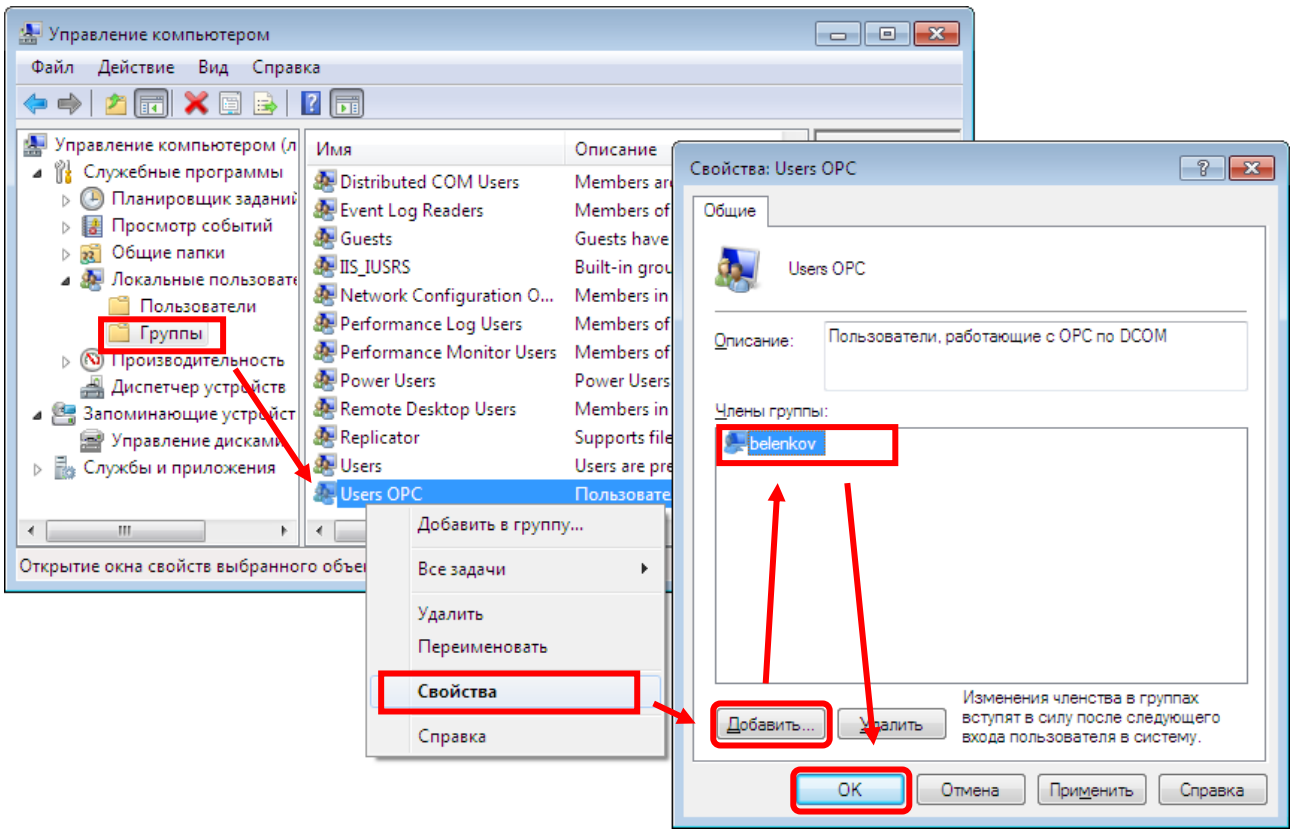

Рисунок 2.7 — Добавление учетной записи пользователя в группу

☝**ВНИМАНИЕ!!!**

Если клиент и сервер являются членами одного домена или разных доменов, имеющих между собой доверительные отношения, то в этом случае локальные учётные записи пользователей при выполнении вызовов DCOM игнорируются и настройки, сделанные для них, будут не действительны. Нужно использовать учетные записи пользователей домена!

Если планируется использовать несколько OPC-клиентов для подключения к OPC-серверу, и клиенты будут запущены под разными пользователями, нужно повторить шаг 2 для каждого пользователя.

2.2.2 Настройка компьютеров, находящихся в рабочей группе

Для настройки компьютеров, находящихся в рабочей группе, выполните следующие шаги:

1 На компьютере сервера рекомендуем создать локальную учетную запись группы пользователей (рисунок 2.6). Имя группы может быть любым (например, «**Users OPC**»).

В дальнейшем созданная группа будет использоваться в настройках OPC-серверов. Шаг создания группы можно пропустить и использовать при настройках OPC-серверов учетные записи пользователей. Но мы рекомендуем использовать для настройки OPC учетную запись группы. В случаях, когда предполагается, что к OPC-серверу будет обращаться несколько разных пользователей, их учетные записи достаточно включить в созданную группу («**Users OPC**»). При таком подходе настроенную систему проще сопровождать. Например, если изменится имя пользователя, запускающего OPC-клиент, нужно будет создать нового пользователя и добавить его в группу. Настройки DCOM при этом изменять не нужно.

Начиная с версии Windows Server 2003, в операционной системе уже существует группа по работе с DCOM – «**Пользователи DCOM**». Можно использовать ее для настройки OPC-серверов.

2 На компьютере сервера создайте учетную запись того пользователя, от имени которого запускается OPC-клиент (рисунок 2.8). То есть, имя и пароль в новой учётной записи должны совпадать с именем и паролем пользователя, запускающего OPC-клиент на клиентском компьютере.

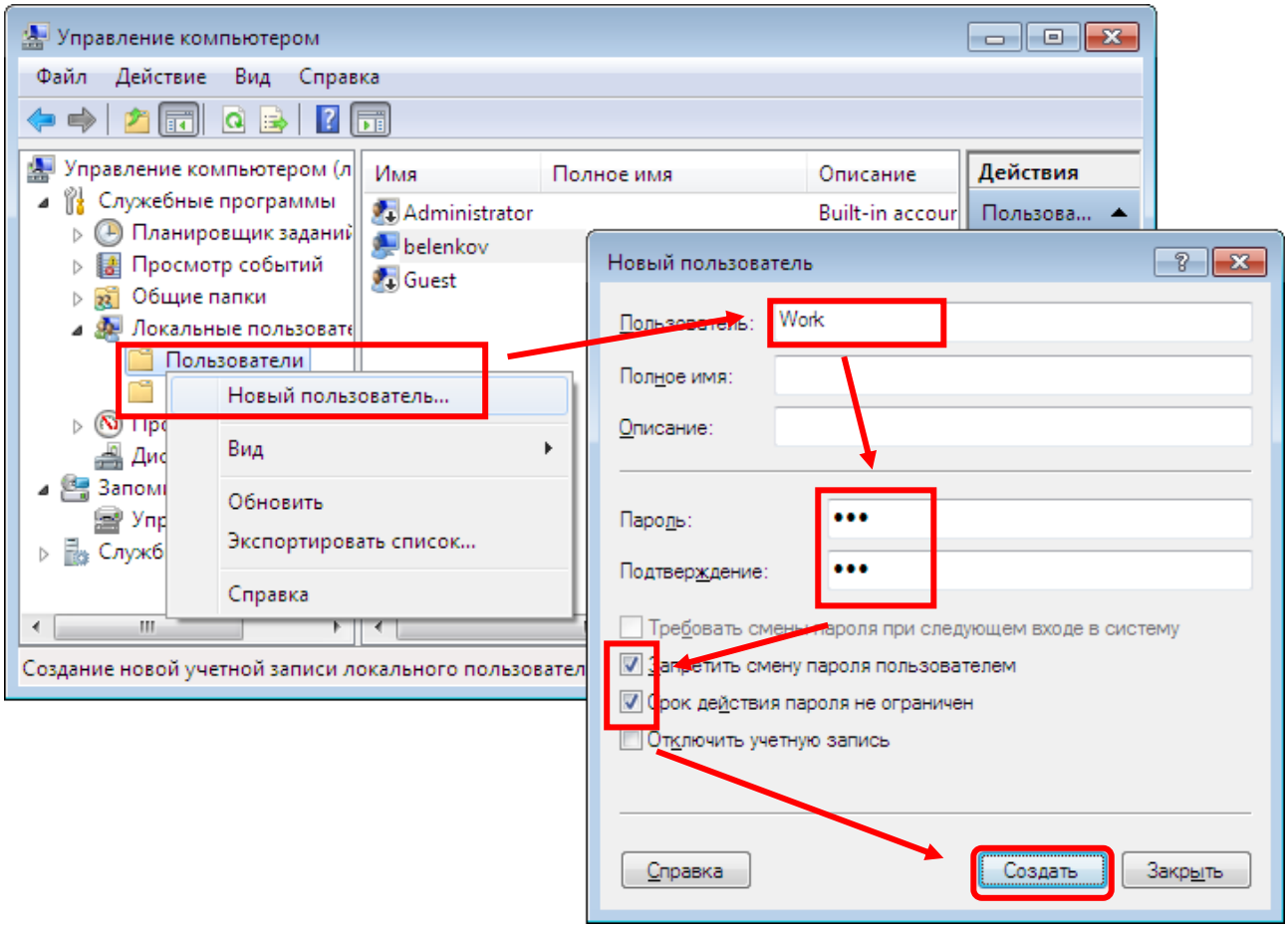

Рисунок 2.8 — Создание учетной записи пользователя

ВНИМАНИЕ!!!

Имя и пароль пользователя, запускающего OPC-клиент, и пользователя, которому предоставлен доступ к удаленному OPC-серверу, должны обязательно совпадать.

Созданную учетную запись пользователя нужно добавить в группу, созданную на шаге 1 («**Users OPC**» или «**Пользователи DCOM**», рисунок 2.9). Если шаг 1 был пропущен, учетная запись созданного пользователя должна использоваться в дальнейших настройках вместо учетной записи группы.

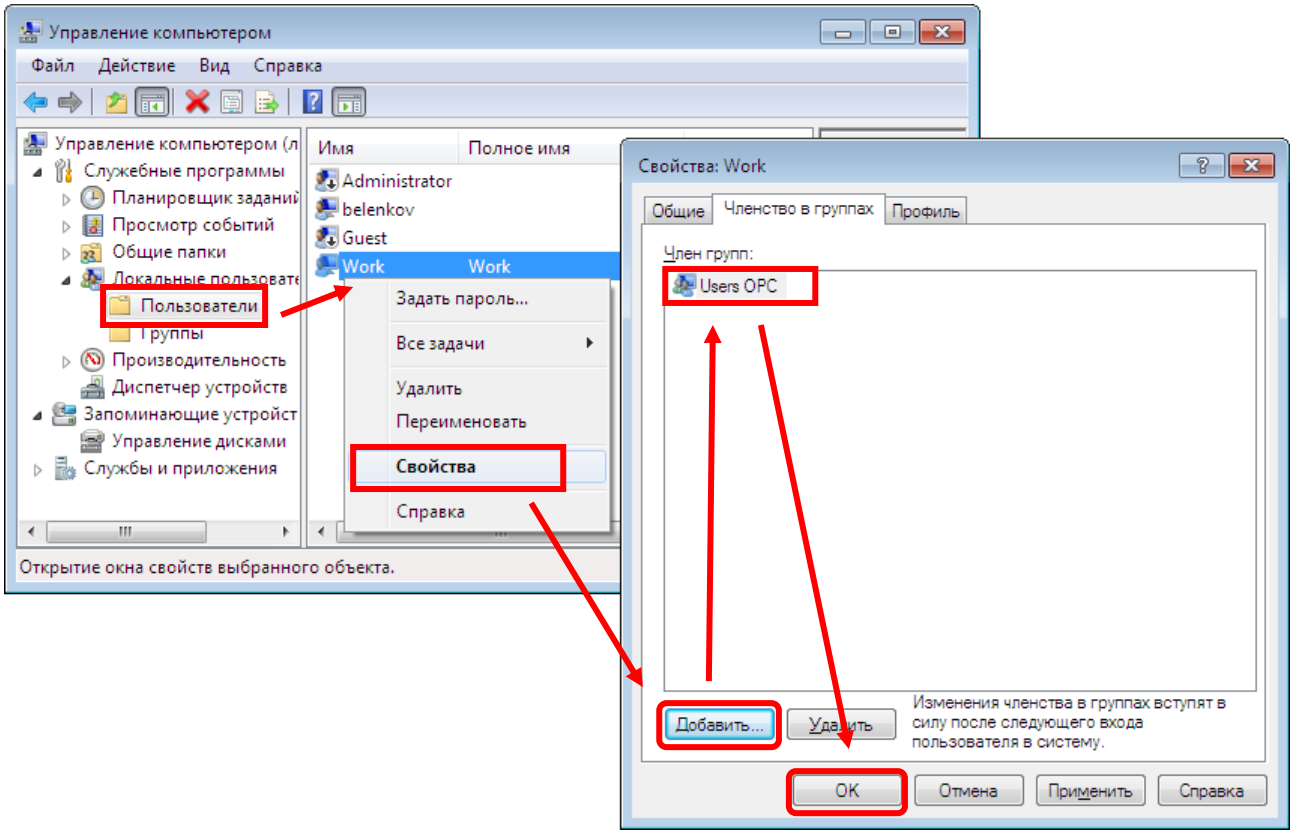

Рисунок 2.9 — Добавление созданного пользователя в группу

Если планируется использовать несколько OPC-клиентов для подключения к OPC-серверу, и клиенты будут запущены под разными пользователями, нужно повторить шаг 2 для каждого пользователя.

3 На компьютере клиента должна существовать учетная запись пользователя, под которой будет запущен OPC-сервер.

Если такая учетная запись будет отсутствовать, асинхронный опрос OPC-сервера станет не возможен. После завершения настроек OPC-сервера и выбора запускающего пользователя, нужно вернуться к этому пункту и, при необходимости, добавить нового пользователя на компьютере клиента.

ВНИМАНИЕ!!!

Имя и пароль пользователя, под учетной записью которого работает OPC-сервер, и пользователя на компьютере клиента, должны обязательно совпадать.

При настройке OPC-серверов права доступа вновь добавленного пользователя не всегда имеют значение, и их можно ограничить.

2.2.3 Настройка компьютеров, находящихся в смешанной сети

Можно настроить соединение через DCOM между одним компьютером, находящимся в домене, и другим, находящимся в рабочей группе. Подобную конфигурацию сети применять не рекомендуется. Желательно, чтобы оба компьютера были расположены в рабочей группе или являлись членами одного домена или разных доменов, имеющих между собой доверительные отношения.

В данном случае настройка компьютеров производится аналогично настройке компьютеров, расположенных в рабочей группе. Для этого выполните следующие шаги:

1. На компьютере клиента создайте локальную учетную запись пользователя, с помощью которой будет происходить подключение к серверу. И обязательно установите пользователю пароль (рисунок 2.8). Имя пользователя и пароль могут быть любыми, например, «**Work**» с паролем «**999**».

2. На компьютере сервера рекомендуем создать учетную запись локальной группы пользователей (рисунок 2.6). Имя группы может быть любым (например, «**Users OPC**»).

   В дальнейшем созданная группа будет использоваться в настройках OPC-серверов. Шаг создания группы можно пропустить и использовать при настройках OPC-серверов учетные записи пользователей. Но мы рекомендуем использовать для настройки OPC учетную запись группы. В случаях, когда предполагается, что к OPC-серверу будет обращаться несколько разных пользователей, их учетные записи достаточно включить в созданную группу («**Users OPC**»). При таком подходе настроенную систему проще сопровождать. Например, если изменится имя

пользователя, запускающего OPC-клиент, нужно будет создать нового пользователя и добавить его в группу. Настройки DCOM при этом изменять не нужно.

Начиная с версии Windows Server 2003, в операционной системе уже имеется группа по работе с DCOM – «**Пользователи DCOM**». Можно использовать ее для настройки OPC-серверов.

3 На компьютере сервера необходимо создать локальную учетную запись пользователя с таким же именем и паролем как у пользователя, созданного на шаге 1 («**Work**» с паролем «**999**», рисунок 2.8).

☝**ВНИМАНИЕ!!!**

Учетная запись пользователя домена и локальная учетная запись с таким же именем и паролем считаются различными! Поэтому в смешанной сети необходимо использовать локальные учетные записи, созданные на шаге 1 и 3.

В группу, созданную на шаге 2 («**Users OPC**» или «**Пользователи DCOM**»), нужно добавить учетную запись созданного пользователя («**Work**» с паролем «**999**», рисунок 2.9). Если шаг 2 был пропущен, в дальнейших настройках вместо учетной записи группы нужно использовать созданную учетную запись пользователя.

4 На компьютере клиента настройте сетевое подключение к серверу через учетную запись созданного пользователя.

Для этого откройте «**Пуск / Панель управления / Учетные записи пользователей / Диспетчер учетных данных / Добавить учетные данные Windows**» (рисунок 2.10).

В открывшемся окне введите следующие данные (рисунок 2.10):

- В поле «**Адрес в интернете или в сети**» – имя компьютера, на котором установлен OPC-сервер.
- В поле «**Имя пользователя**» – имя пользователя, созданного на шаге 1. Имя должно быть в форме <имя компьютера клиента>\<имя пользователя>.
- В поле «**Пароль**» – пароль пользователя, созданного на шаге 1.

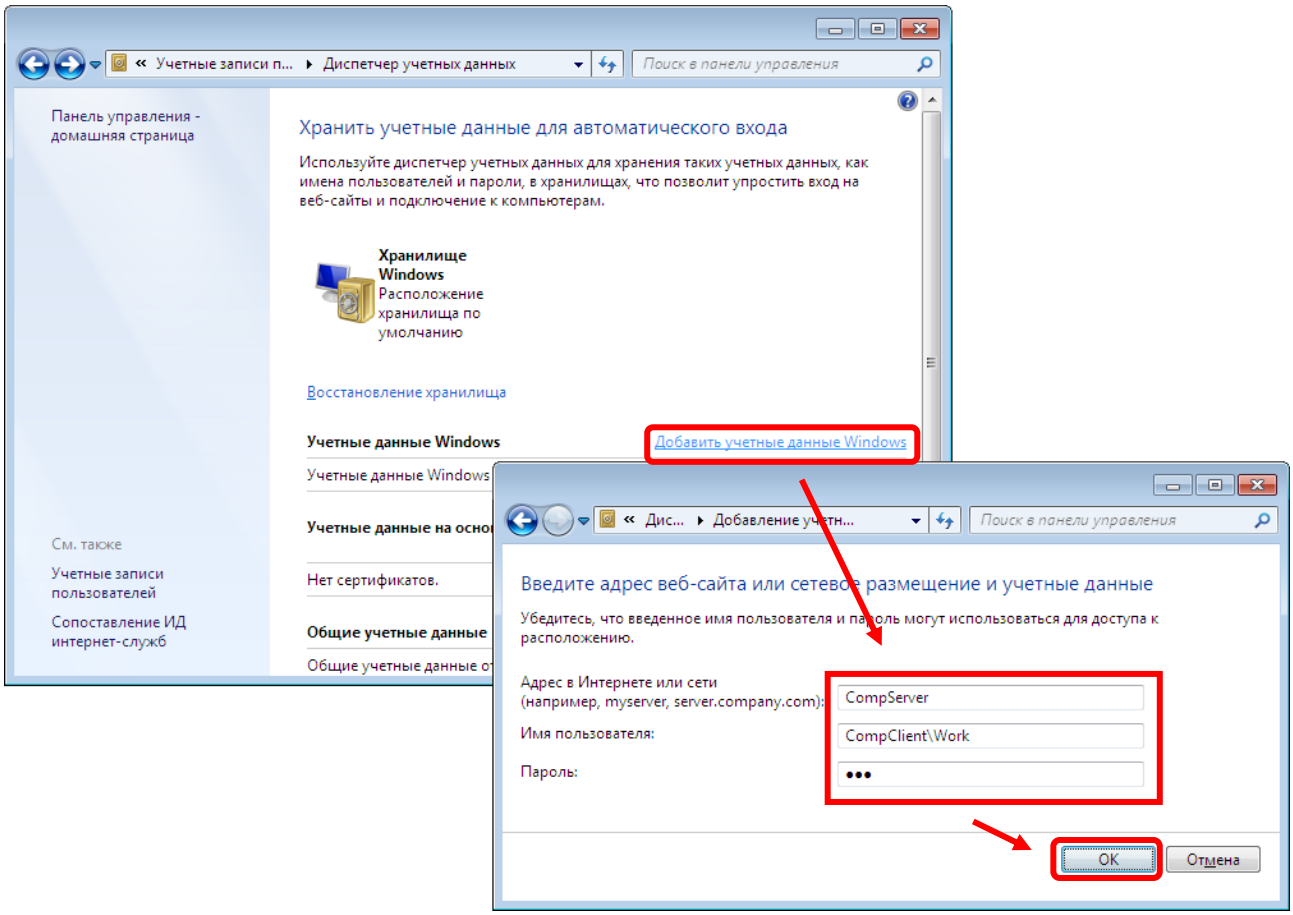

Рисунок 2.10 — Настройка сетевого подключения

Нажмите на «**OK**» и закройте окна, чтобы сохранить сделанные изменения.

При настройке OPC-серверов права доступа вновь добавленного пользователя не всегда имеют значение, и их можно ограничить.

ВНИМАНИЕ!!!

После сделанных настроек любые подключения к серверу от клиента (например, подключение к общим папкам на сервере) будут проходить в соответствии с назначенными правами доступа пользователя на компьютере сервере. Поэтому ограничение прав доступа пользователя нужно выполнять осторожно или не производить вообще.

2.3 Настройка учетных записей для Windows Server 2008, Windows Server 2012

2.3.1 Настройка компьютеров, находящихся в домене

☝**ВНИМАНИЕ!!!**

Если есть возможность использовать доменную подсистему Windows, то нужно обязательно это сделать. Вы получите выигрыш в скорости работы и сделаете настраиваемую систему более надежной.

При настройке компьютеров нужно убедиться в том, что оба компьютера находятся в одном домене, или что домены, к которым они относятся, соединены доверительными отношениями. При этом нужно использовать именно учетные записи пользователей домена, а не локальные.

При настройке компьютеров, входящих в домен, выполните следующие шаги:

1. На компьютере, где установлен OPC-сервер, или на контроллере домена рекомендуем создать учетную запись группы пользователей. Для этого необходимо открыть «**Пуск / Панель управления / Администрирование / Управление компьютером**» и выполнить последовательность действий, изображенную на рисунке 2.11. Имя группы может быть любым (например, «**Users OPC**»). В дальнейшем созданная группа будет использоваться в настройках OPC-серверов.
   Шаг создания группы можно пропустить и использовать при настройках OPC-серверов учетные записи пользователей домена. Но мы рекомендуем использовать для настройки OPC группу пользователей. В случаях, когда предполагается, что к OPC-серверу будет обращаться несколько разных пользователей, их учетные записи достаточно включить в созданную группу («**Users OPC**»). При таком подходе настроенную систему проще сопровождать. Например, если изменится имя пользователя, запускающего OPC-клиент, нужно будет добавить нового пользователя в группу. Настройки DCOM при этом изменять не нужно.

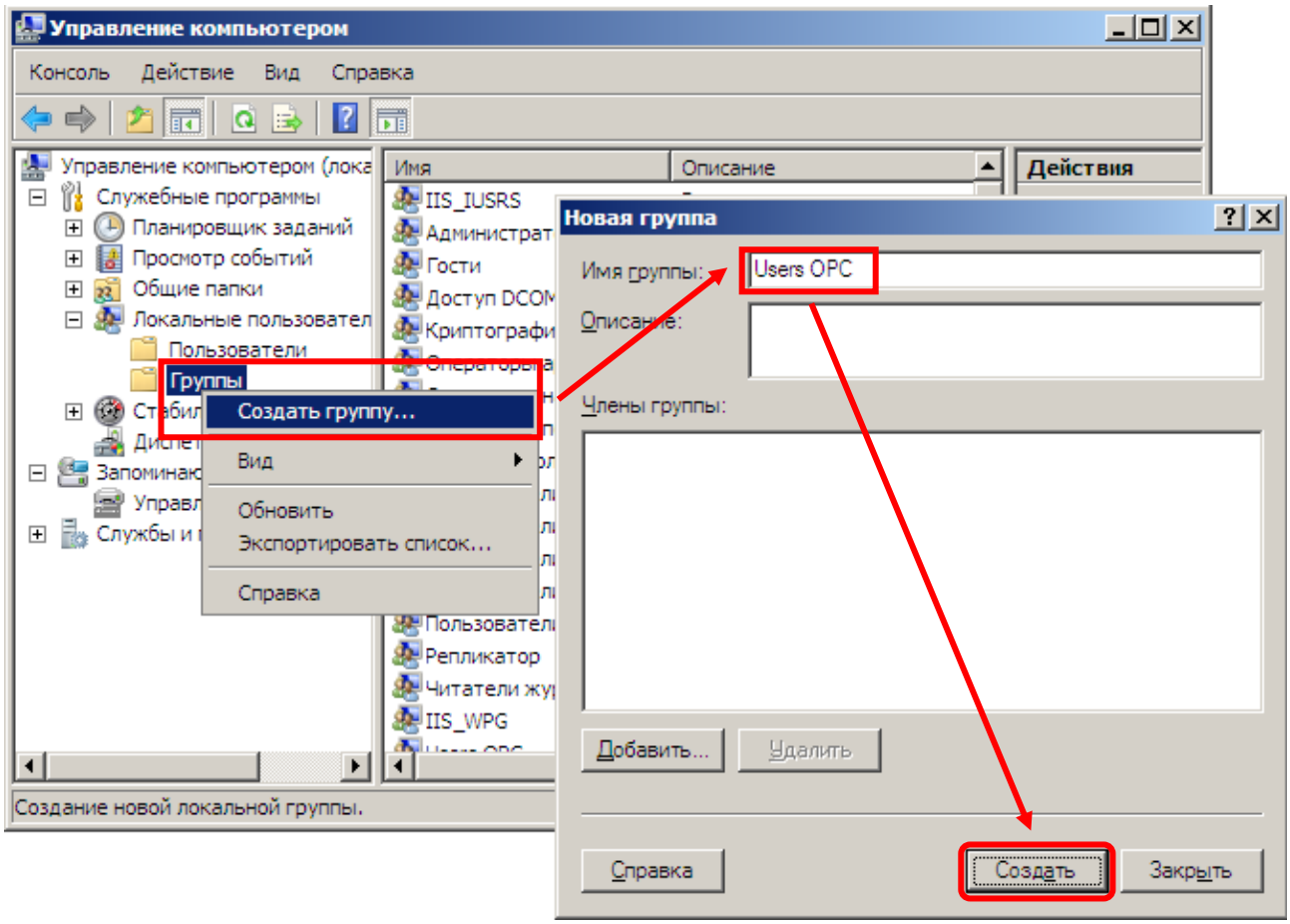

Рисунок 2.11 — Создание группы пользователей

Если будет использована группа, созданная на контроллере домена, ее можно использовать при настройке OPC-серверов на всех компьютерах, включенных в домен. Таким образом, список пользователей, имеющих доступ к OPC-серверам, будет глобальный для всего домена. И может редактироваться централизованно на контроллере домена. Если для каждого компьютера с OPC-сервером нужны индивидуальные права доступа пользователей, можно использовать локальную учетную запись группы.

Начиная с версии Windows Server 2003, в операционной системе уже имеется группа по работе с DCOM – «**Пользователи DCOM**». Можно использовать ее для настройки OPC-серверов.

2 В группу, созданную на шаге 1 («**Users OPC**» или «**Пользователи DCOM**»), добавьте учетные записи пользователей домена, которым будет разрешен доступ к OPC-

серверу (рисунок 2.12). Если шаг 1 был пропущен, в дальнейших настройках вместо учетной записи группы используйте учетные записи пользователей домена.

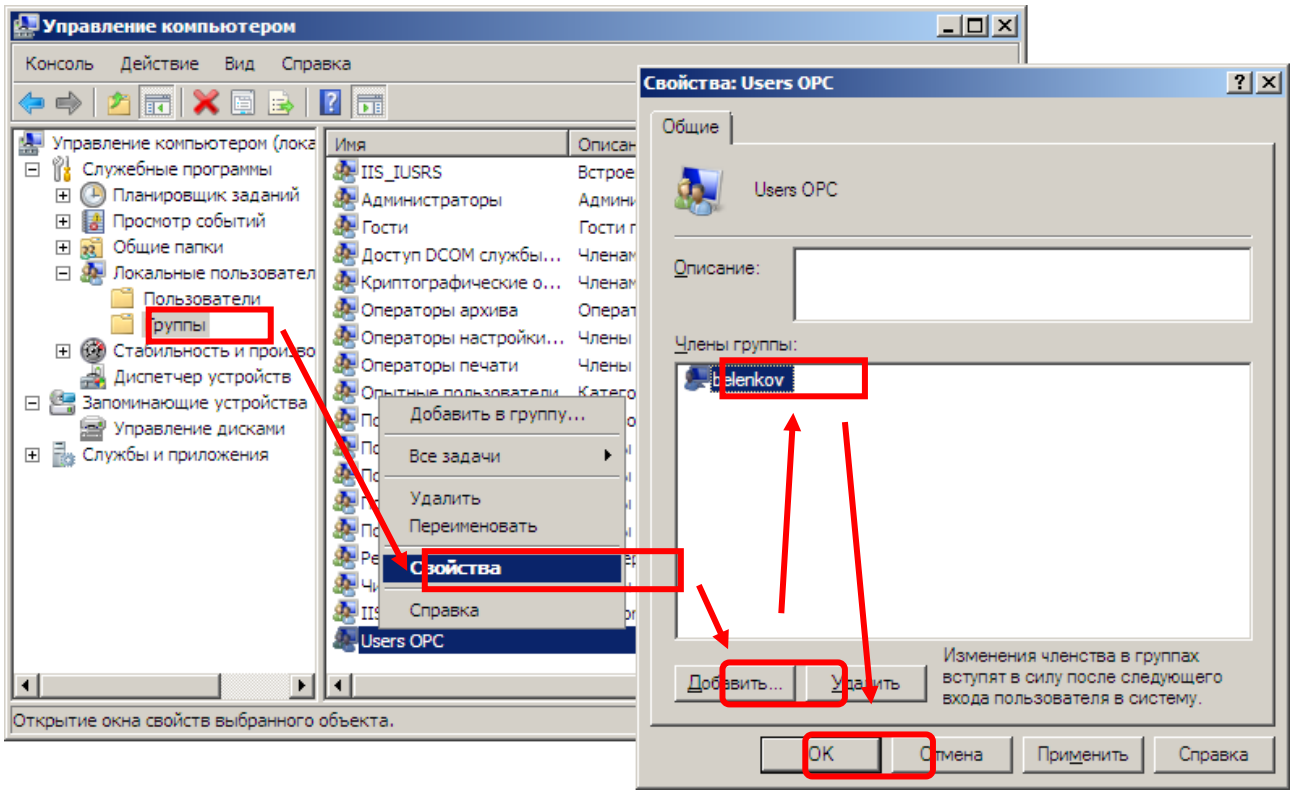

Рисунок 2.12 — Добавление учетной записи пользователя в группу

ВНИМАНИЕ!!!

Если клиент и сервер являются членами одного домена или разных доменов, имеющих между собой доверительные отношения, то в этом случае локальные учётные записи пользователей при выполнении вызовов DCOM игнорируются и настройки, сделанные для них, будут не действительны. Нужно использовать учетные записи пользователей домена!

Если планируется использовать несколько OPC-клиентов для подключения к OPC-серверу, и клиенты будут запущены под разными пользователями, нужно повторить шаг 2 для каждого пользователя.

2.3.2 Настройка компьютеров, находящихся в рабочей группе

Для настройки компьютеров, находящихся в рабочей группе, выполните следующие шаги:

1. На компьютере сервера рекомендуем создать локальную учетную запись группы пользователей (рисунок 2.11). Имя группы может быть любым (например, «**Users OPC**»).

   В дальнейшем созданная группа будет использоваться в настройках OPC-серверов. Шаг создания группы можно пропустить и использовать при настройках OPC-серверов учетные записи пользователей. Но мы рекомендуем использовать для настройки OPC учетную запись группы. В случаях, когда предполагается, что к OPC-серверу будет обращаться несколько разных пользователей, их учетные записи достаточно включить в созданную группу («**Users OPC**»). При таком подходе настроенную систему проще сопровождать. Например, если изменится имя пользователя, запускающего OPC-клиент, нужно будет создать нового пользователя и добавить его в группу. Настройки DCOM при этом изменять не нужно.

   Начиная с версии Windows Server 2003, в операционной системе уже существует группа по работе с DCOM – «**Пользователи DCOM**». Можно использовать ее для настройки OPC-серверов.

2. На компьютере сервера создайте учетную запись того пользователя, от имени которого запускается OPC-клиент (рисунок 2.13). То есть, имя и пароль в новой учётной записи должны совпадать с именем и паролем пользователя, запускающего OPC-клиент на клиентском компьютере.

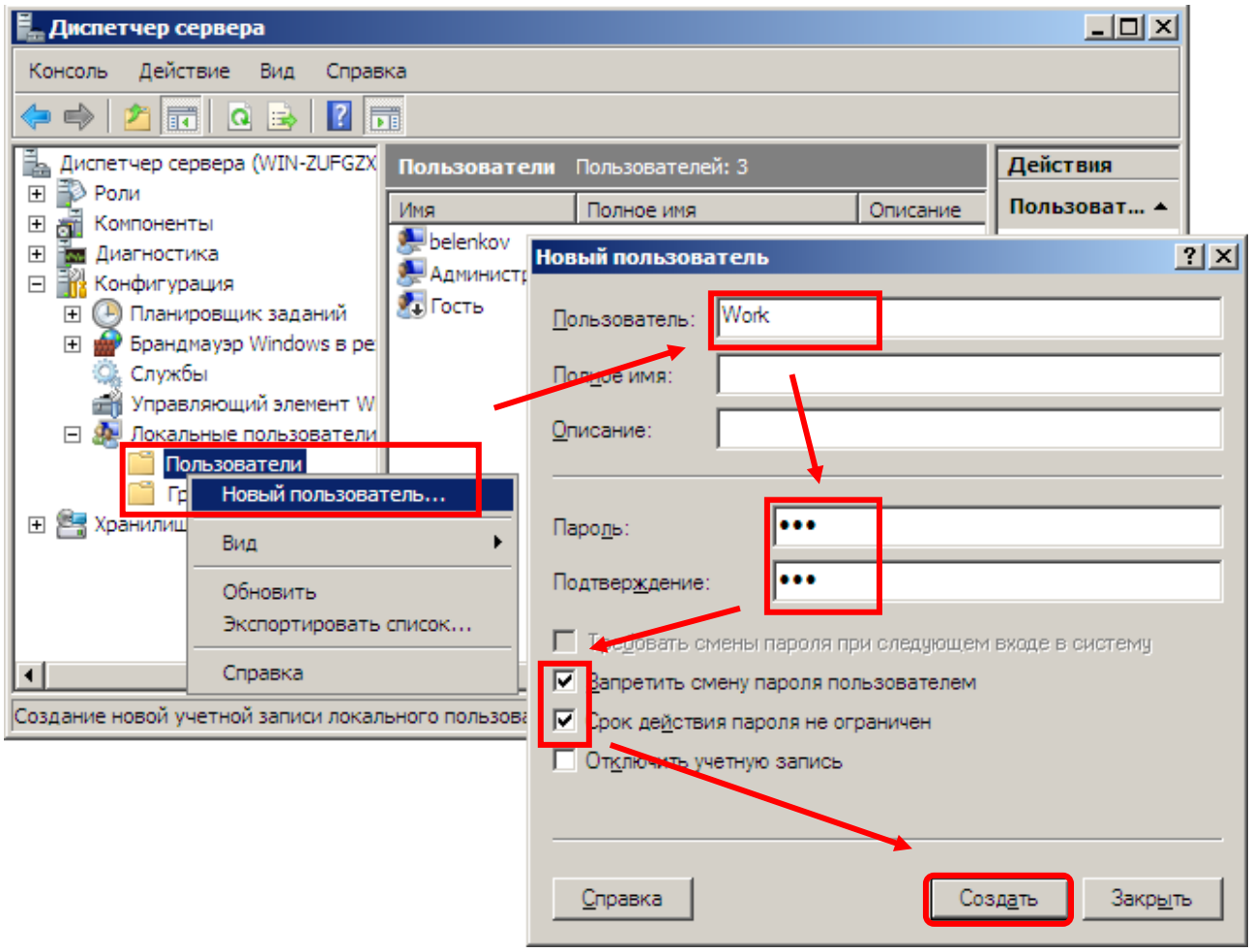

Рисунок 2.13 — Создание учетной записи пользователя

ВНИМАНИЕ!!!

Имя и пароль пользователя, запускающего OPC-клиент, и пользователя, которому предоставлен доступ к удаленному OPC-серверу, должны обязательно совпадать.

Созданную учетную запись пользователя нужно добавить в группу, созданную на шаге 1 («**Users OPC**» или «**Пользователи DCOM**», рисунок 2.14). Если шаг 1 был пропущен, учетная запись созданного пользователя должна использоваться в дальнейших настройках вместо учетной записи группы.

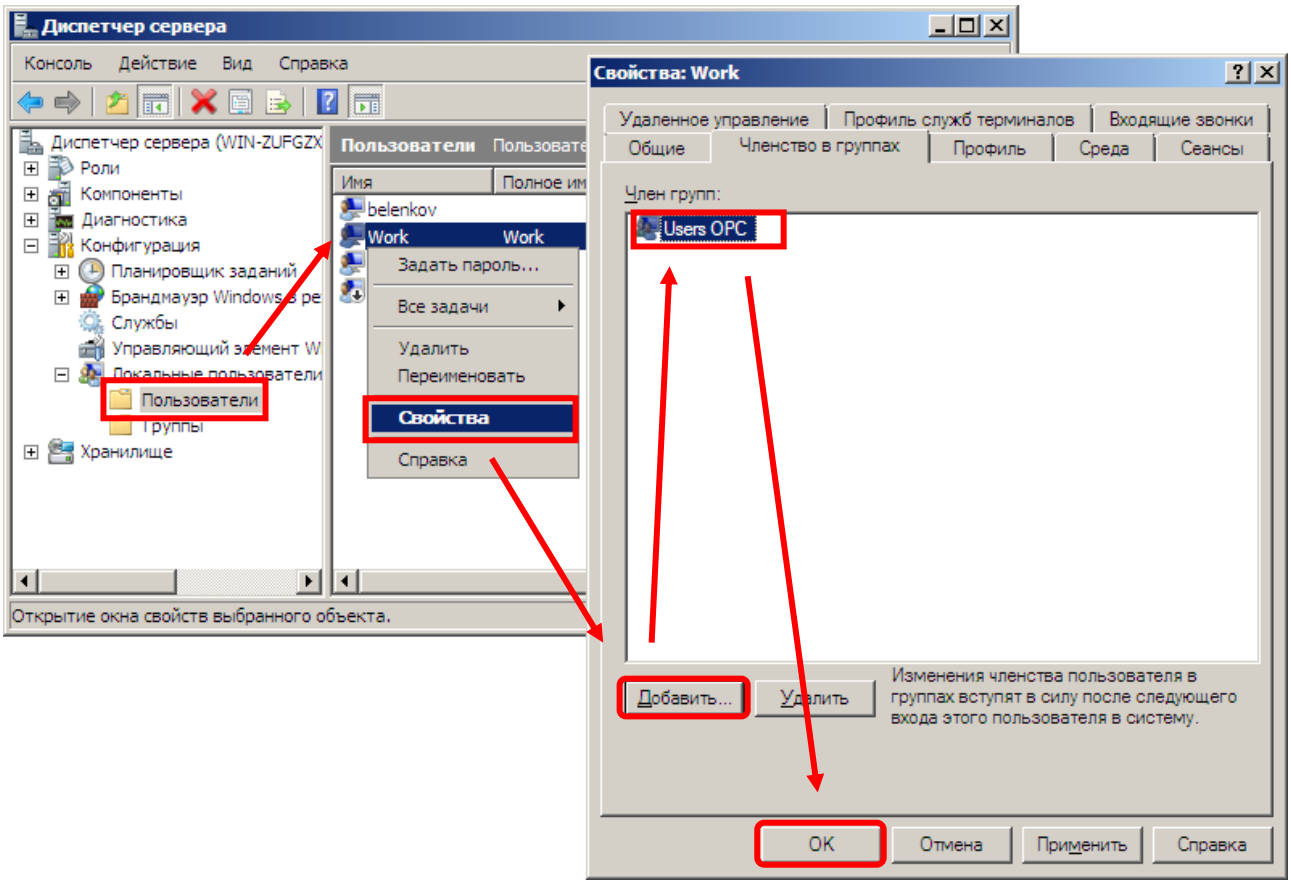

Рисунок 2.14 — Добавление созданного пользователя в группу

Если планируется использовать несколько OPC-клиентов для подключения к OPC-серверу, и клиенты будут запущены под разными пользователями, нужно повторить шаг 2 для каждого пользователя.

3 На компьютере клиента должна существовать учетная запись пользователя, под которой будет запущен OPC-сервер.

Если такая учетная запись будет отсутствовать, асинхронный опрос OPC-сервера станет не возможен. После завершения настроек OPC-сервера и выбора запускающего пользователя, нужно вернуться к этому пункту и, при необходимости, добавить нового пользователя на компьютере клиента.

ВНИМАНИЕ!!!

Имя и пароль пользователя, под учетной записью которого работает OPC-сервер, и пользователя на компьютере клиента, должны обязательно совпадать.

При настройке OPC-серверов права доступа вновь добавленного пользователя не всегда имеют значение, и их можно ограничить.

2.3.3 Настройка компьютеров, находящихся в смешанной сети

Можно настроить соединение через DCOM между одним компьютером, находящимся в домене, и другим, находящимся в рабочей группе. Подобную конфигурацию сети применять не рекомендуется. Желательно, чтобы оба компьютера были расположены в рабочей группе или являлись членами одного домена или разных доменов, имеющих между собой доверительные отношения.

В данном случае настройка компьютеров производится аналогично настройке компьютеров, расположенных в рабочей группе. Для этого выполните следующие шаги:

1. На компьютере клиента создайте локальную учетную запись пользователя, с помощью которой будет происходить подключение к серверу. И обязательно установите пользователю пароль (рисунок 2.13). Имя пользователя и пароль могут быть любыми, например, «**Work**» с паролем «**999**».

2. На компьютере сервера рекомендуем создать учетную запись локальной группы пользователей (рисунок 2.11). Имя группы может быть любым (например, «**Users OPC**»).

   В дальнейшем созданная группа будет использоваться в настройках OPC-серверов. Шаг создания группы можно пропустить и использовать при настройках OPC-серверов учетные записи пользователей. Но мы рекомендуем использовать для настройки OPC учетную запись группы. В случаях, когда предполагается, что к OPC-серверу будет обращаться несколько разных пользователей, их учетные записи достаточно включить в созданную группу («**Users OPC**»). При таком подходе настроенную систему проще сопровождать. Например, если изменится имя пользователя, запускающего OPC-клиент, нужно будет создать нового пользователя и добавить его в группу. Настройки DCOM при этом изменять не нужно.

Начиная с версии Windows Server 2003, в операционной системе уже имеется группа по работе с DCOM – «**Пользователи DCOM**». Можно использовать ее для настройки OPC-серверов.

3 На компьютере сервера необходимо создать локальную учетную запись пользователя с таким же именем и паролем как у пользователя, созданного на шаге 1 («**Work**» с паролем «**999**», рисунок 2.13).

☝**ВНИМАНИЕ!!!**

Учетная запись пользователя домена и локальная учетная запись с таким же именем и паролем считаются различными! Поэтому в смешанной сети необходимо использовать локальные учетные записи, созданные на шаге 1 и 3.

В группу, созданную на шаге 2 («**Users OPC**» или «**Пользователи DCOM**»), нужно добавить учетную запись созданного пользователя («**Work**» с паролем «**999**», рисунок 2.14). Если шаг 2 был пропущен, в дальнейших настройках вместо учетной записи группы нужно использовать созданную учетную запись пользователя.

4 На компьютере клиента настройте сетевое подключение к серверу через учетную запись созданного пользователя.

Для этого откройте «**Пуск / Панель управления / Учетные записи пользователей**». В открывшемся окне перейдите по ссылке «**Управление сетевыми паролями**» (рисунок 2.15).
В окне «**Сохранение имен пользователей и паролей**» нажмите кнопку «**Добавить**».
В окне «**Свойства сохраненных учетных данных**» введите:

- В поле «**Вход в**» - имя компьютера, на котором установлен OPC-сервер.
- В поле «**Пользователь**» - имя пользователя, созданного на шаге 1. Имя должно быть в форме <имя компьютера клиента>\<имя пользователя>.
- В поле «**Пароль**» - пароль пользователя, созданного на шаге 1.

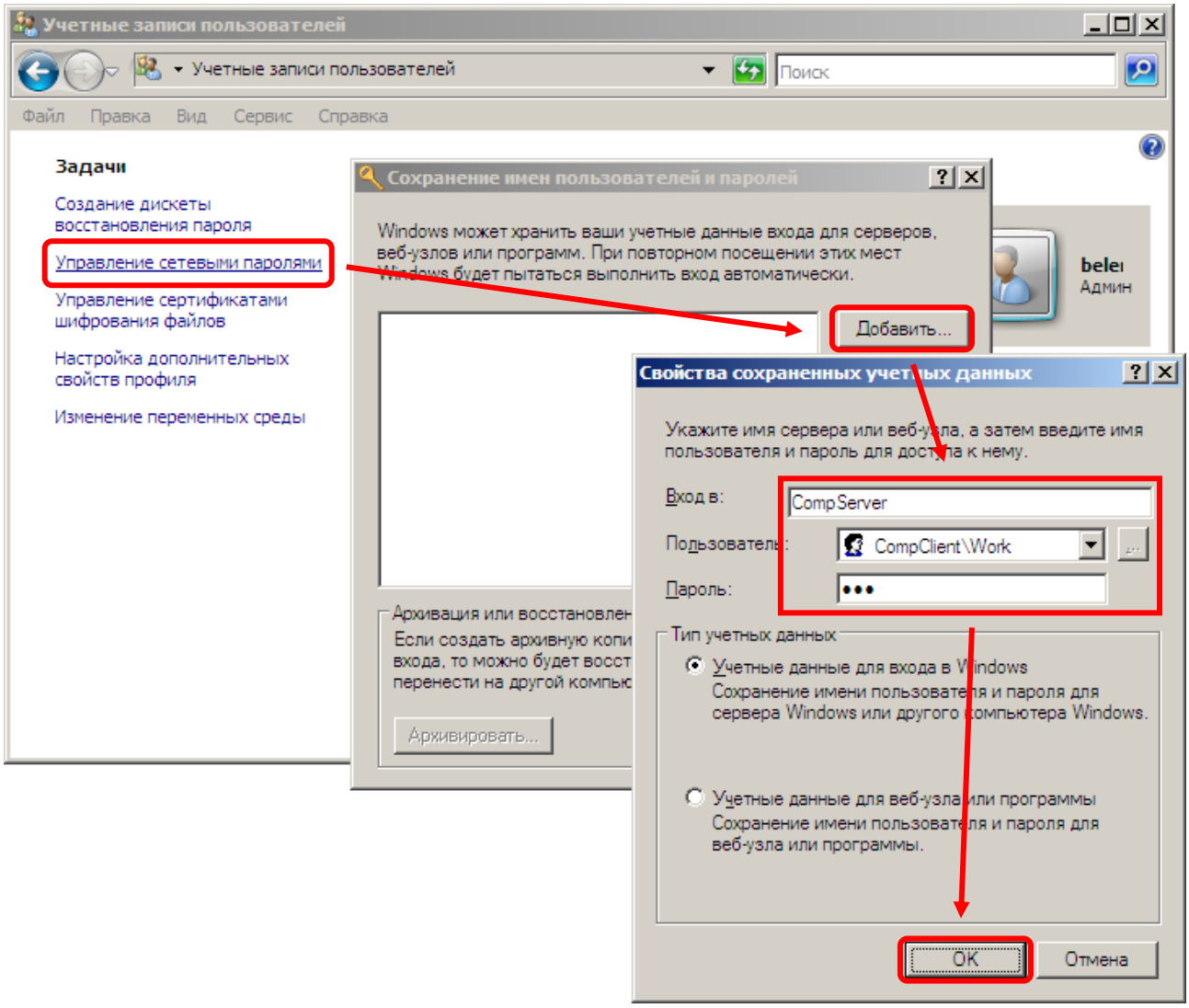

Рисунок 2.15 — Настройка сетевого подключения

Нажмите на «**OK**» и закройте окна, чтобы сохранить сделанные изменения.

При настройке OPC-серверов права доступа вновь добавленного пользователя не всегда имеют значение, и их можно ограничить.

ВНИМАНИЕ!!!

После сделанных настроек любые подключения к серверу от клиента (например, подключение к общим папкам на сервере) будут проходить в соответствии с назначенными правами доступа пользователя на компьютере сервере. Поэтому ограничение прав доступа пользователя нужно выполнять осторожно или не производить вообще.

3 НАСТРОЙКА БРАНДМАУЭРА

Для успешной установки DCOM соединения от компьютера-клиента к компьютеру-серверу, при функционирующем брандмауэре на одном или на обоих компьютерах, необходимо настроить брандмауэр.

3.1 Настройка брандмауэра для Windows XP

3.1.1 Настройка с помощью командной строки

Прежде всего, необходимо запустить командную строку. Для этого нужно открыть меню «**Пуск / Все программы / Стандартные / Командная строка**» (рисунок 3.1).
Далее следует выполнить последовательно следующие шаги:

1 На компьютере клиента и сервера введите в командной строке следующую команду:
netsh firewall add portopening protocol=tcp port=135 name=DCOM

После выполнения этой команды в настройках встроенного брандмауэра добавится правило «DCOM», разрешающее входящие вызовы для 135-го TCP порта (порт используется DCOM).

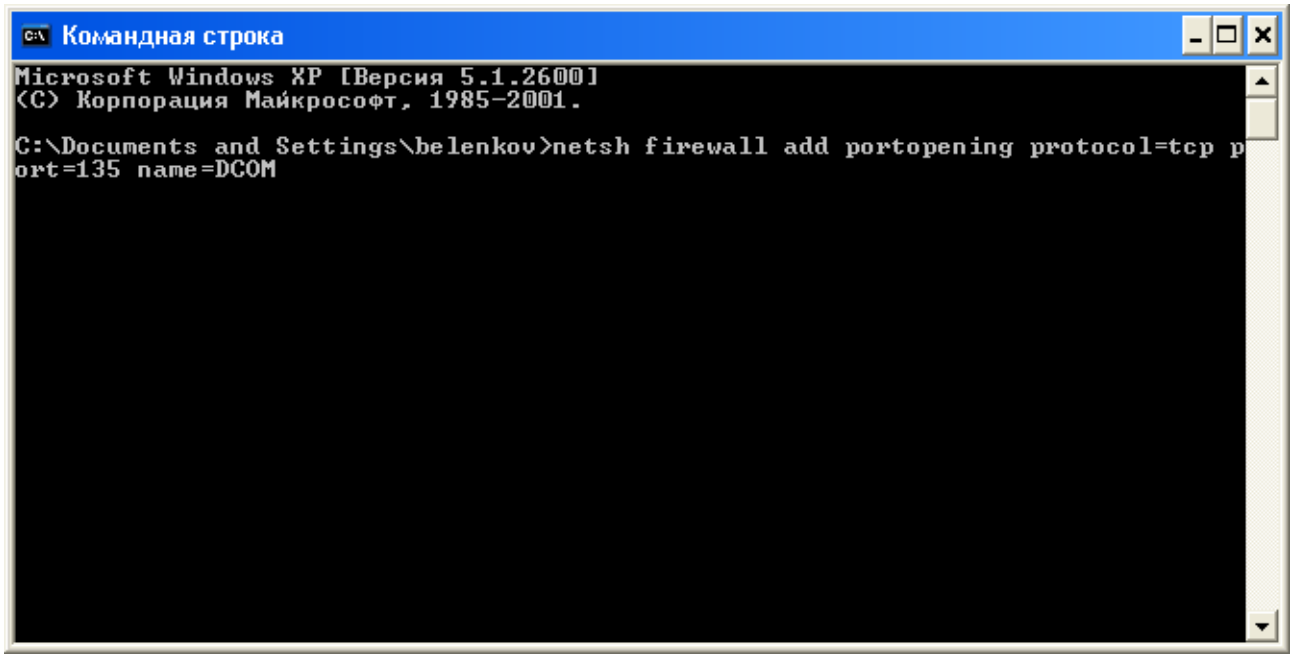

Рисунок 3.1 – Командная строка

2 На компьютере клиента введите в командной строке следующую команду:
netsh firewall add allowedprogram program=<ClientName> name=<RuleName>
где ClientName — полное имя исполняемого файла программы OPC-клиента,
RuleName — имя правила брандмауэра.

После выполнения этой команды в настройках встроенного брандмауэра добавится правило «RuleName», разрешающее входящие вызовы для программы OPC-клиента «ClientName».

3 На компьютере сервера добавьте исключение для утилиты перечисления OPC-серверов OPCEnum.exe. Для этого введите в командной строке следующую команду:
netsh firewall add allowedprogram program=<system32>\OPCEnum.exe name=OPCEnum
где <system32> – путь к системной папке ОС Windows system32, по умолчанию «C:\Windows\system32». В некоторых случаях OPCEnum может быть установлен в другую папку, тогда вместо <system32> нужно прописать путь к этой папке.

4 На компьютере сервера добавьте исключение для настраиваемых OPC-серверов. Для этого введите в командной строке следующую команду:
netsh firewall add allowedprogram program=<ServerName> name=<RuleName>
где ServerName – полное имя исполняемого файла программы OPC-сервера,
RuleName – имя правила брандмауэра.

Для систем, в составе которых используется брандмауэр стороннего производителя, при выполнении соответствующей настройки необходимо обратиться к документации установленного брандмауэра.

Даже если в системе не установлен брандмауэр стороннего производителя, а встроенный отключен, то выше описанные настройки желательно выполнить, чтобы уменьшить количество посторонних сообщений в журнале безопасности, при включённом аудите событий отказа в доступе.

3.1.2 Настройка через пользовательский интерфейс

Чтобы запустить консоль управления брандмауэром, необходимо открыть системное меню «**Пуск/ Панель управления/ Брандмауэр Windows**» или выполнить из командной строки (**Win+R**) инструкцию «***firewal.cpl***».

По умолчанию подключения с других компьютеров заблокированы в брандмауэре Windows. Для того чтобы OPC-клиенты могли подсоединяться к OPC-серверам на данном компьютере, необходимо создать правила для входящих соединений DCOM. Для этого на компьютерах клиента и сервера необходимо в консоли управления брандмауэром перейти на вкладку «**Исключения**» и нажать на кнопку «**Добавить порт**» (рисунок 3.2).

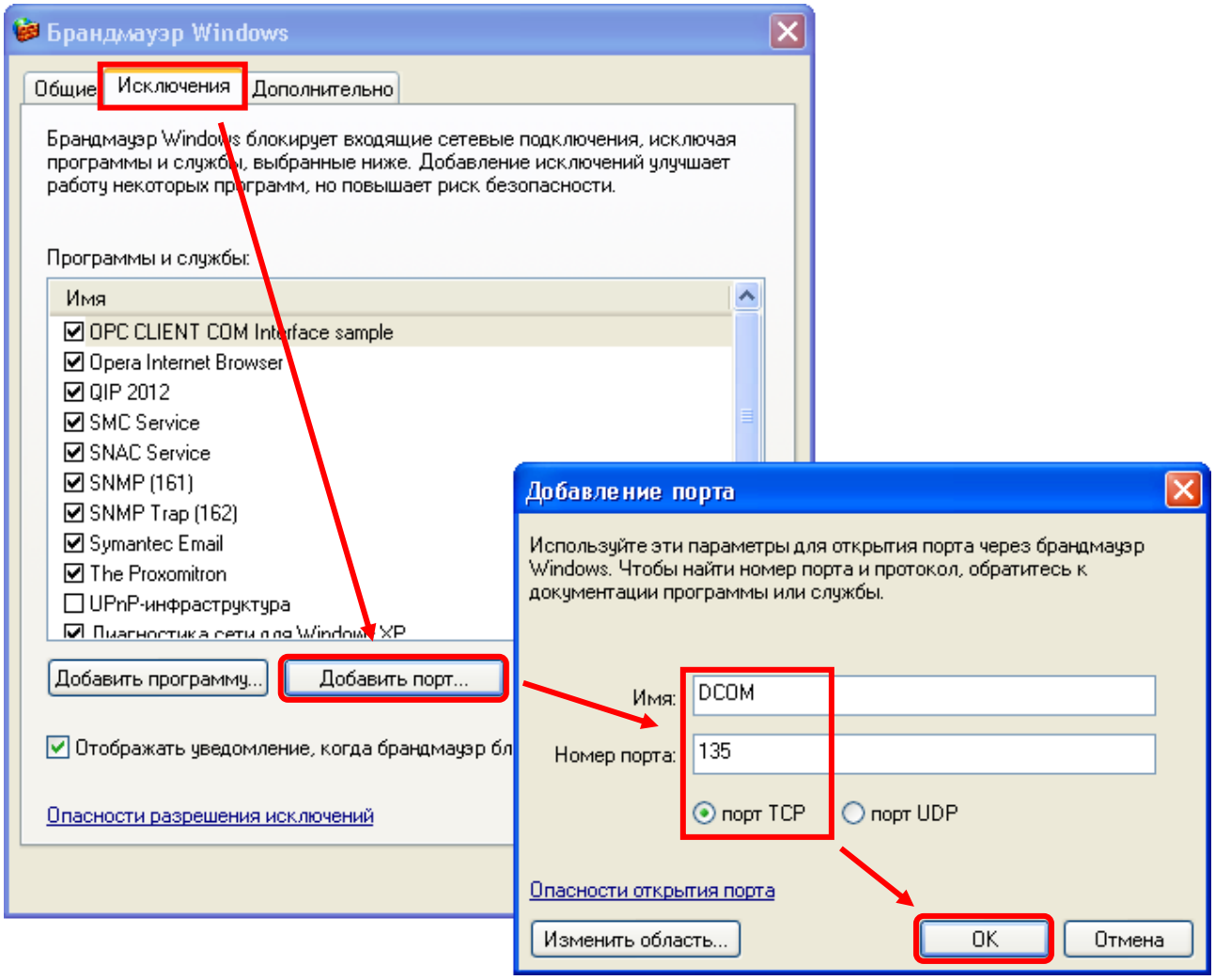

Рисунок 3.2 – Добавление порта DCOM в исключения брандмауэра

В окне «**Добавление порта**» в поле «**Имя**» задается название для исключения (например «**DCOM**») и номер порта (**135**). В качестве протокола указывается «**порт TCP**». Кнопкой «**ОК**» производится сохранение созданного исключения для порта 135.

Следующим шагом будет добавление исключений, разрешающих работу в сети, для каждого OPC-сервера, а так же для системной службы ***OpcEnum***, которая позволяет получить клиенту список OPC-серверов на удаленном компьютере. Чтобы добавить в исключения программу, нужно на вкладке «**Исключения**» консоли управления брандмауэром нажать кнопку «**Добавить программу**». Далее с помощью кнопки «**Обзор**» найти и добавить исполняемый файл приложения. При добавлении службы OpcEnum это будет файл **OpcEnum.exe**, расположенный по адресу «**C:\Windows\system32**» (рисунок 3.3). Кнопка «**ОК**» сохраняет изменения.

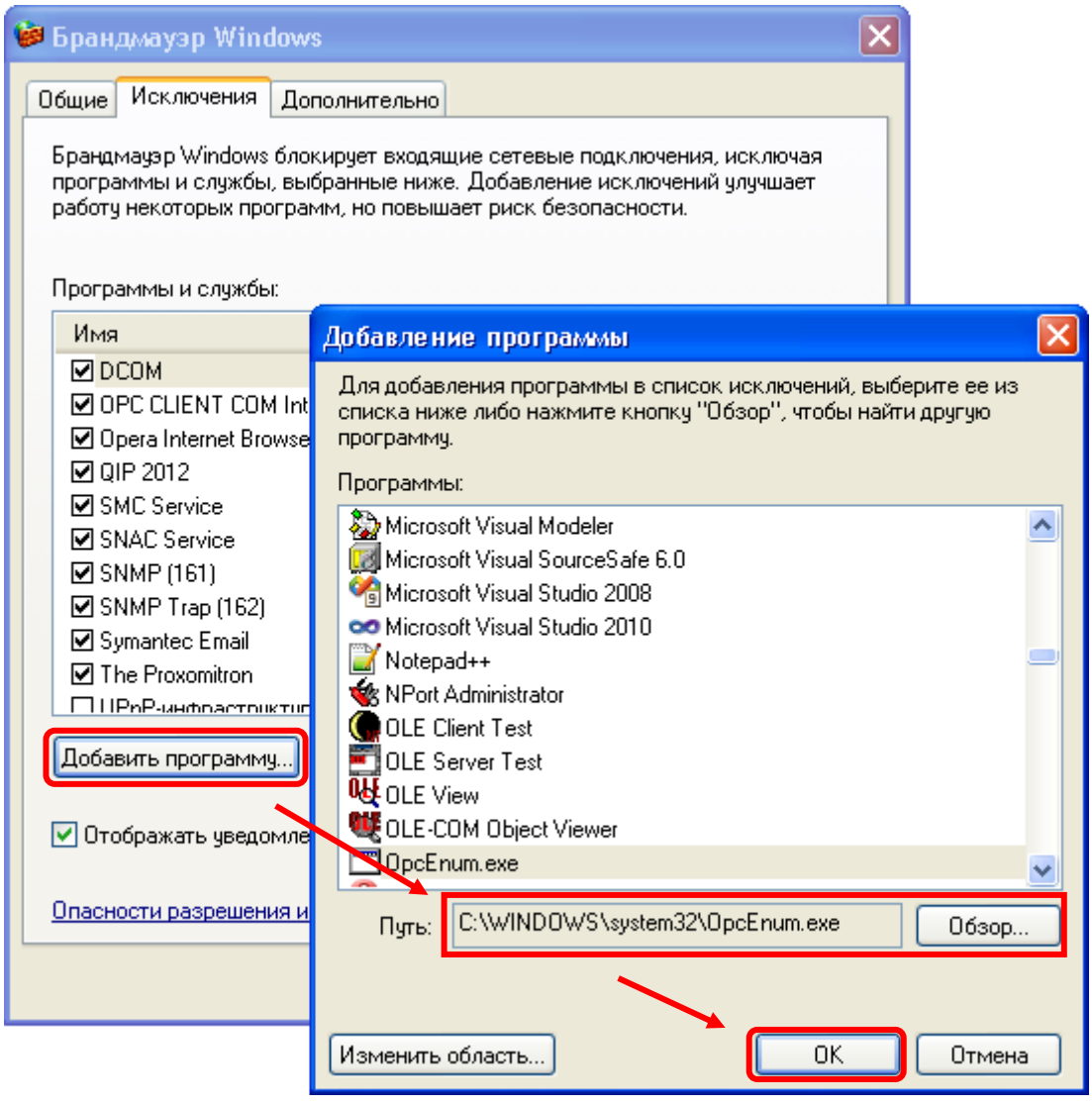

Рисунок 3.3 – Добавление программы в исключения брандмауэра

То же самое нужно проделать для каждого OPC-сервера, к которому предполагается удаленное подключение, а так же для каждого OPC-клиента.

3.2 Настройка брандмауэра для Windows 7, Windows 8

3.2.1 Настройка через пользовательский интерфейс

Чтобы запустить консоль управления брандмауэром, необходимо открыть системное меню «**Пуск / Панель управления / Система и безопасность / Брандмауэр Windows**» или выполнить из командной строки (**Win+R**) инструкцию «***firewal.cpl***». В открывшемся окне выбрать опцию «**Дополнительные параметры**» (рисунок 3.4). Для создания нового правила, нужно вызвать контекстное меню раздела «**Правила для входящих подключений**» и выбрать пункт «**Создать правило...**», чтобы запустить «**Мастер создания правила для нового входящего подключения**» (рисунок 3.4).

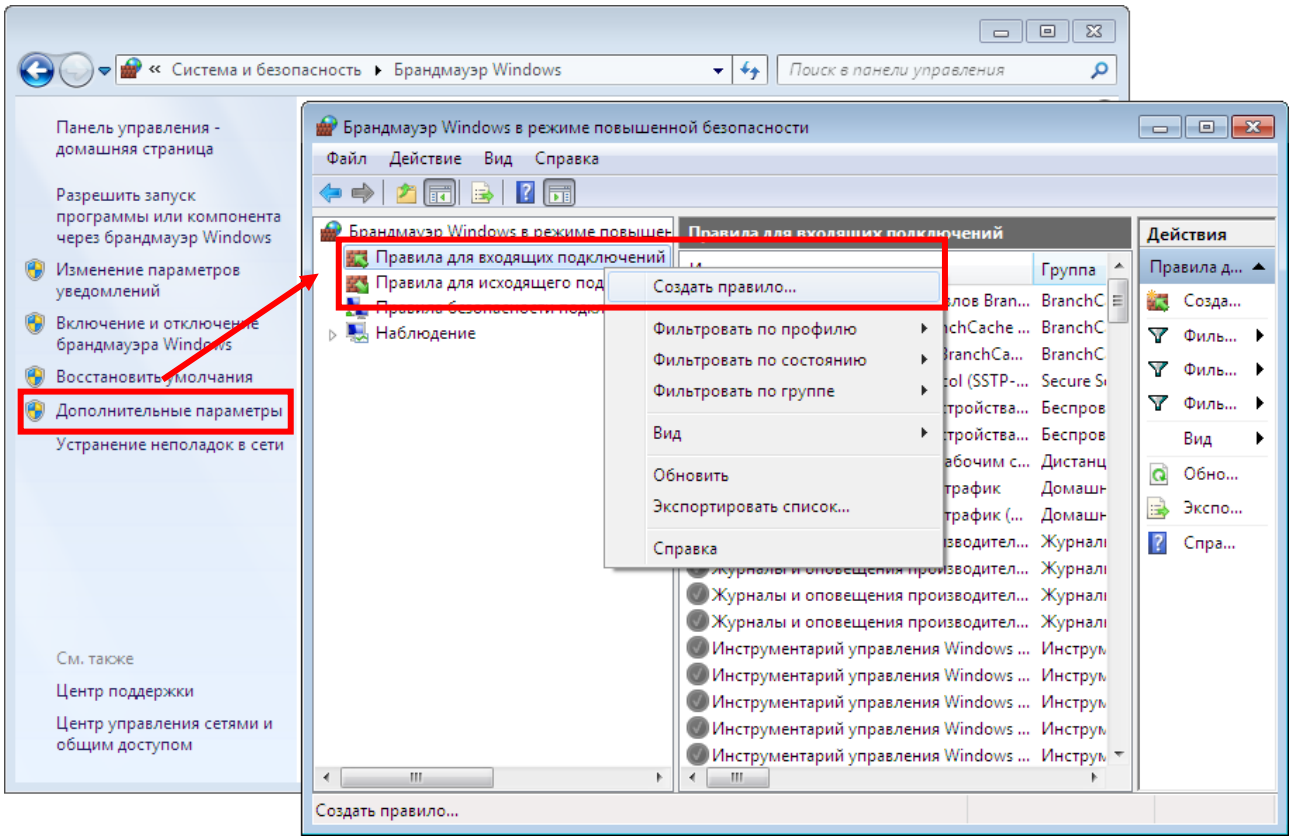

Рисунок 3.4 – Создание нового правила для входящих подключений

По умолчанию подключения с других компьютеров заблокированы в брандмауэре Windows. Для того чтобы OPC-клиенты могли подсоединяться к OPC-серверам на компьютере,

необходимо создать правила для входящих соединений DCOM. Для этого на компьютерах клиента и сервера необходимо выполнить следующие шаги:

1 Вызвать «**Мастер создания правила...**» и выбрать тип правила «**Для порта**» (рисунок 3.5).

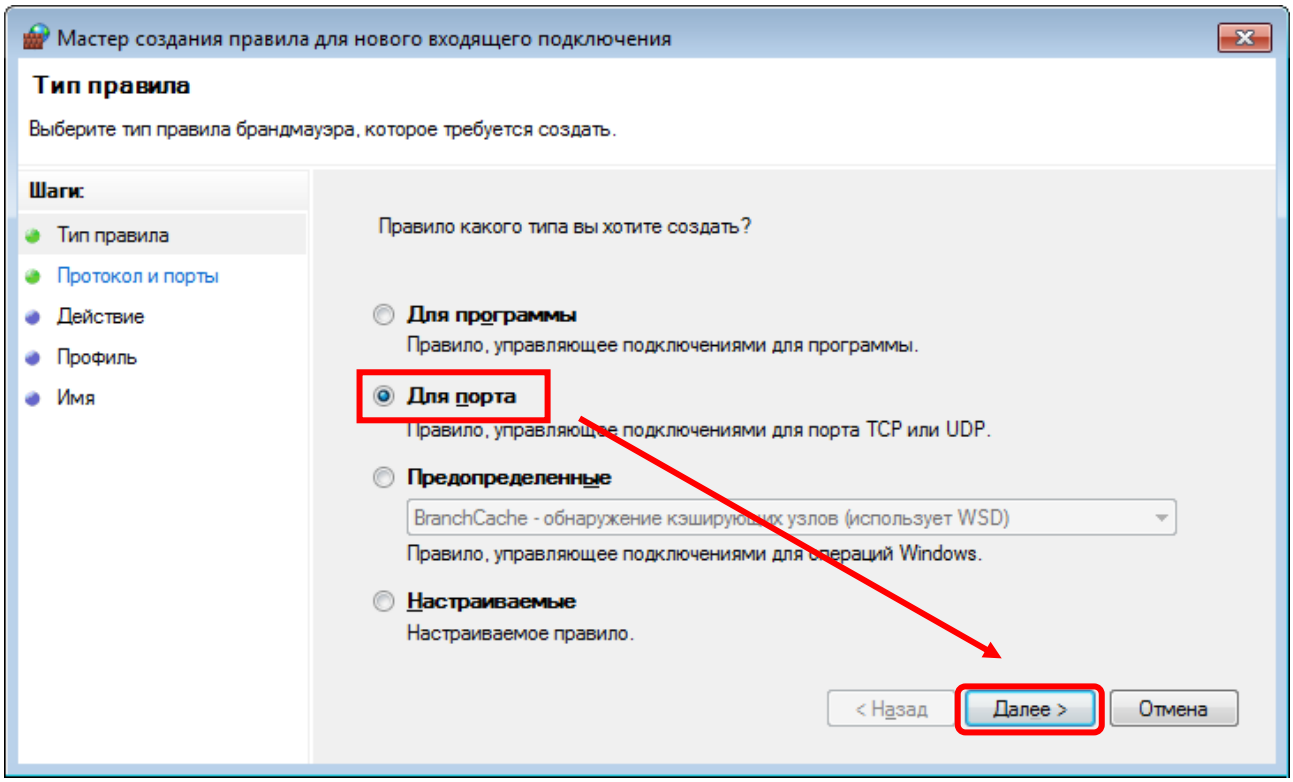

Рисунок 3.5 – Создание правила для порта

2 На шаге выбора протокола и порта необходимо установить переключатель в положение «**протокол TCP**», а в поле «**Определенные локальные порты**» ввести число **135** (рисунок 3.6).

3 На шаге выбора действия установить переключатель в положение «**Разрешить подключение**» (рисунок 3.7).

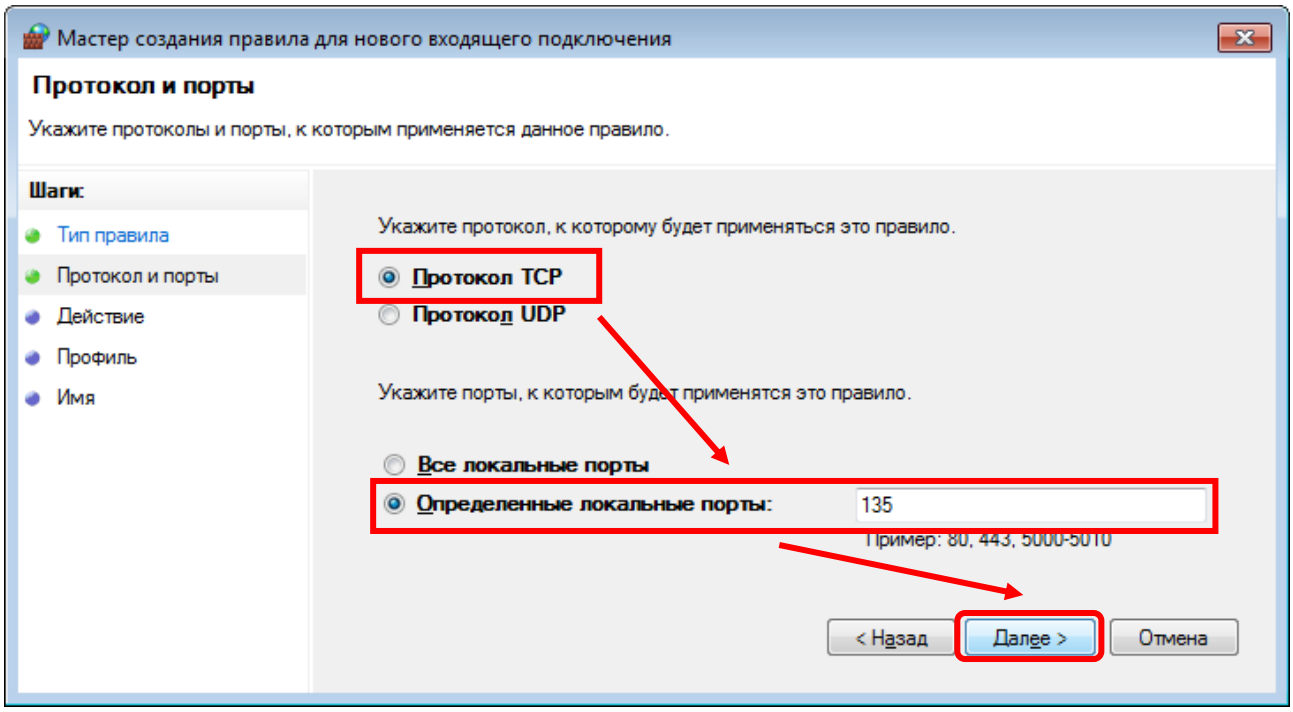

Рисунок 3.6 – Выбор протокола и порта

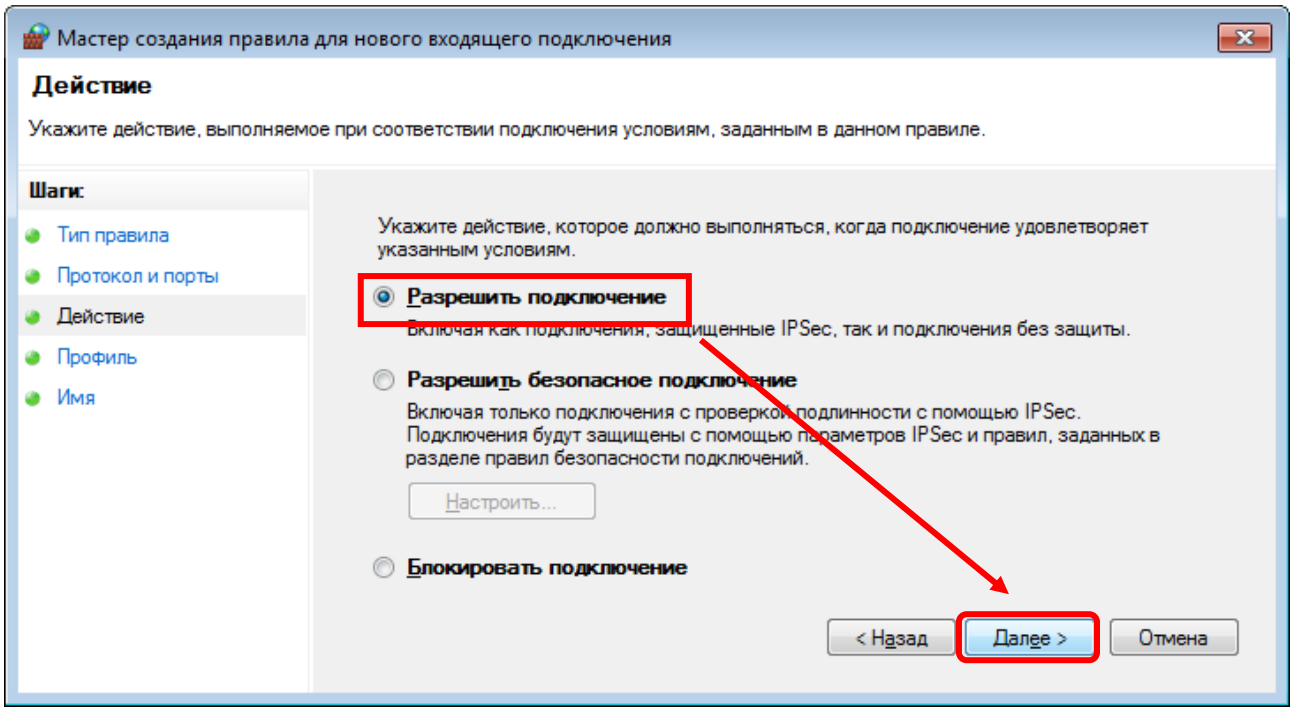

Рисунок 3.7 – Определение свойств правила

4 Поставить галочки напротив всех вариантов профилей (рисунок 3.8).

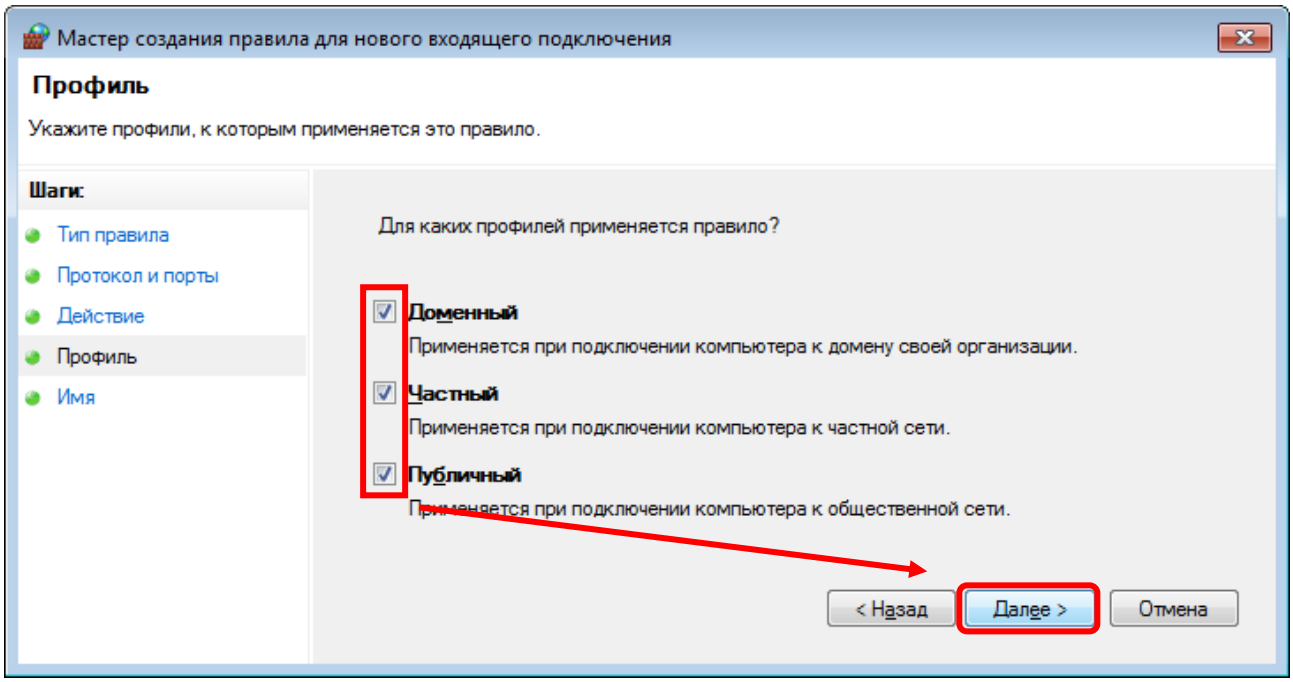

Рисунок 3.8 – Выбор области действия правила

5 Ввести имя правила (например, «**DCOM**») и нажать кнопку «**Готово**» для завершения процедуры создания нового правила для порта (рисунок 3.9).

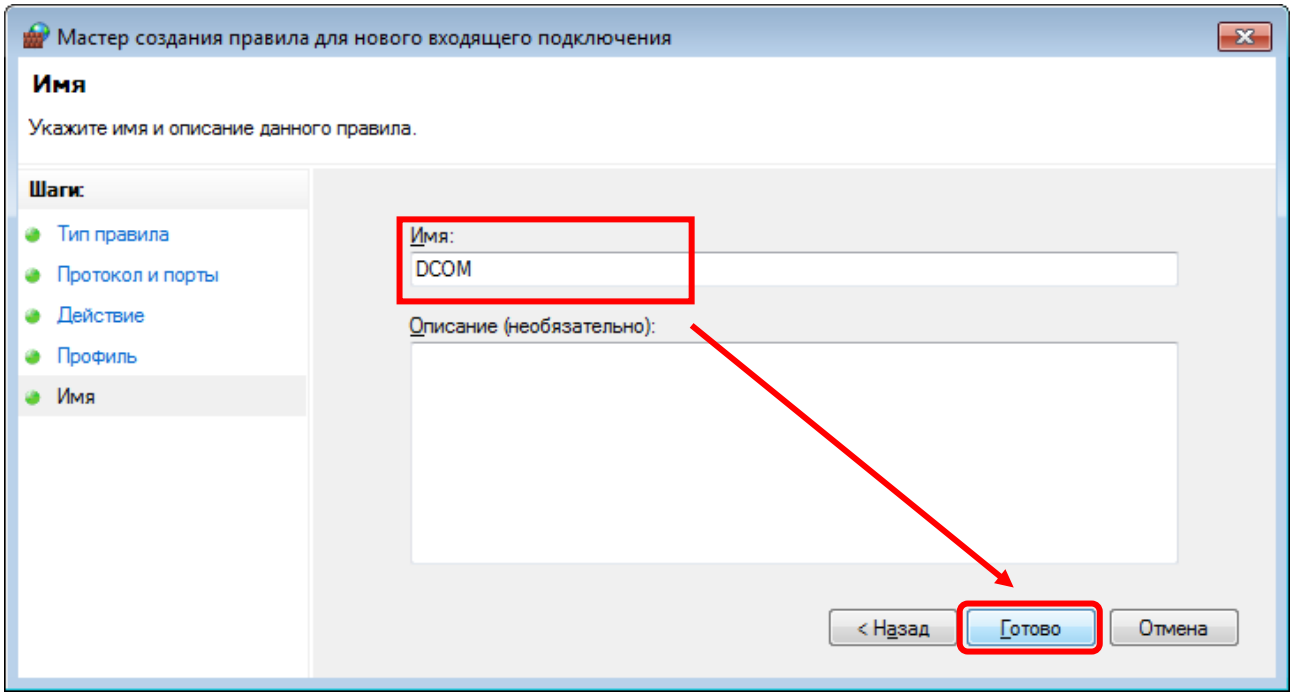

Рисунок 3.9 – Завершение мастера создания правила

После создания исключения для порта, необходимо разрешить работу для каждого OPC-сервера, а так же для системной службы OpcEnum, которая позволяет получить клиенту список OPC-серверов на удаленном компьютере.

Шаги по созданию правила для программы идентичны указанным выше за исключением первых двух, заключающихся в следующем.

1 Вызвать «**Мастер создания правила...**» и указать в качестве типа правила вариант «**Для программы**» (рисунок 3.10).

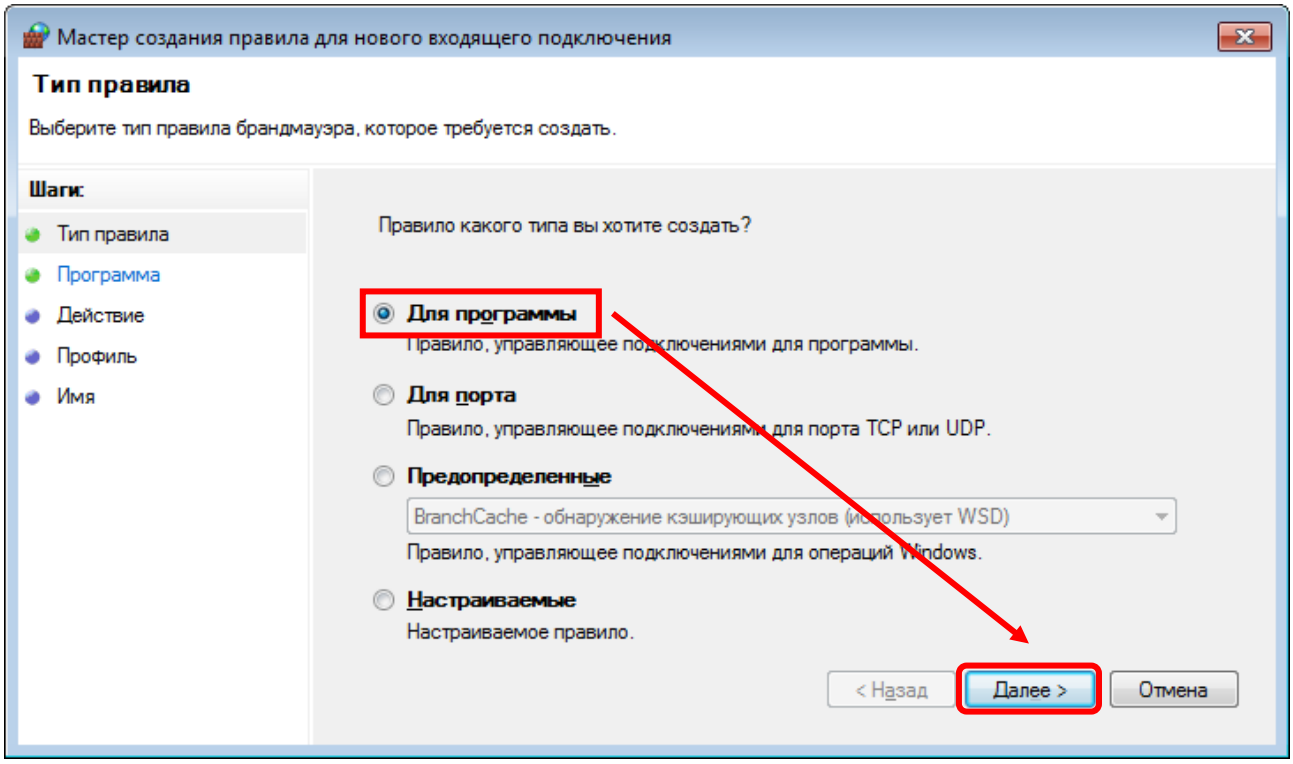

Рисунок 3.10 – Создание правила для программы

2 Установить переключатель в положение «**Путь программы**» и указать полный путь вместе с именем программы (вручную или с помощью кнопки «**Обзор...**»). Например, при добавлении службы OpcEnum это будет файл **OpcEnum.exe**, расположенный по адресу «**C:\Windows\system32**» (рисунок 3.11).

То же самое нужно проделать для каждого OPC-сервера, к которому предполагается удаленное подключение, а так же для каждого OPC-клиента.

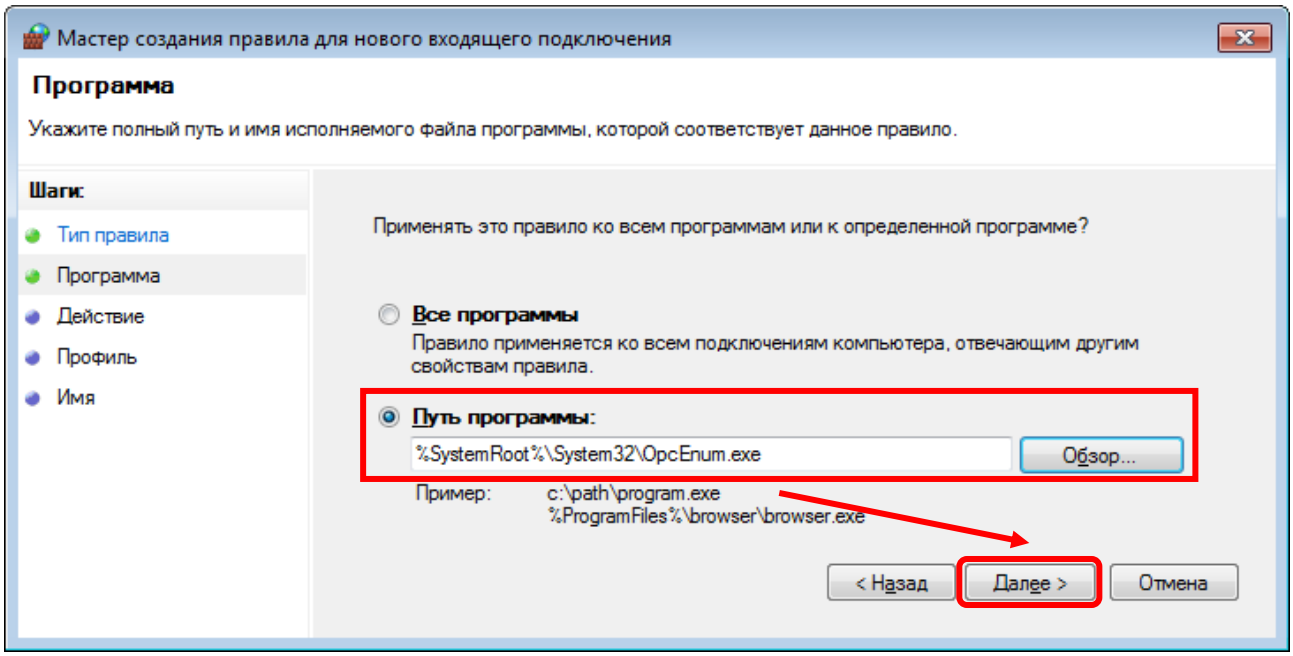

Рисунок 3.11 – Выбор файла программы

3.3 Настройка брандмауэра для Windows Server 2008, Windows Server 2012

3.3.1 Настройка через пользовательский интерфейс

Чтобы запустить консоль управления брандмауэром, необходимо открыть системное меню «**Пуск / Панель управления / Брандмауэр Windows**» или выполнить из командной строки (**Win+R**) инструкцию «**firewal.cpl**». В открывшемся окне перейти по ссылке «**Изменить параметры**».

По умолчанию подключения с других компьютеров заблокированы в брандмауэре Windows. Для того чтобы OPC-клиенты могли подсоединяться к OPC-серверам на данном компьютере, необходимо создать правила для входящих соединений DCOM. Для этого на компьютерах клиента и сервера необходимо в консоли управления брандмауэром перейти на вкладку «**Исключения**» и нажать на кнопку «**Добавить порт**» (рисунок 3.12).

В окне «**Добавление порта**» в поле «**Имя**» задается название для исключения (например «**DCOM**») и номер порта (**135**). В качестве протокола указывается «**порт TCP**». Кнопкой «**ОК**» производится сохранение созданного исключения для порта 135.

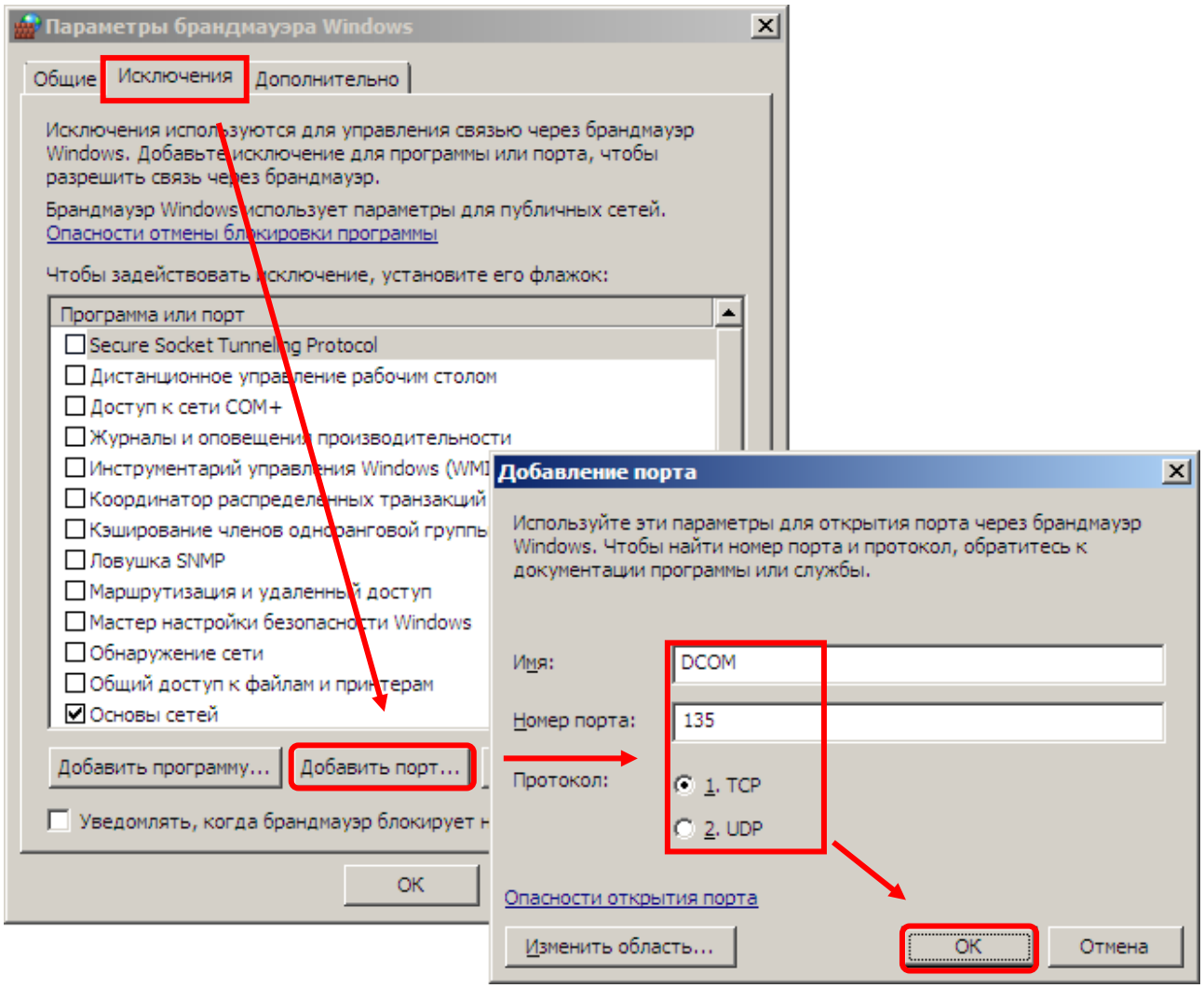

Рисунок 3.12 – Добавление порта DCOM в исключения брандмауэра

Следующим шагом будет добавление исключений, разрешающих работу в сети, для каждого OPC-сервера, а так же для системной службы OpcEnum, которая позволяет получить клиенту список OPC-серверов на удаленном компьютере.

Чтобы добавить в исключения программу, нужно на вкладке «**Исключения**» консоли управления брандмауэром нажать кнопку «**Добавить программу**». Далее с помощью кнопки «**Обзор**» найти и добавить исполняемый файл приложения. При добавлении службы OpcEnum это будет файл **OpcEnum.exe**, расположенный по адресу «**C:\Windows\system32**» (рисунок 3.13). Кнопка «**ОК**» сохраняет изменения.

То же самое нужно проделать для каждого OPC-сервера, к которому предполагается удаленное подключение, а так же для каждого OPC-клиента.

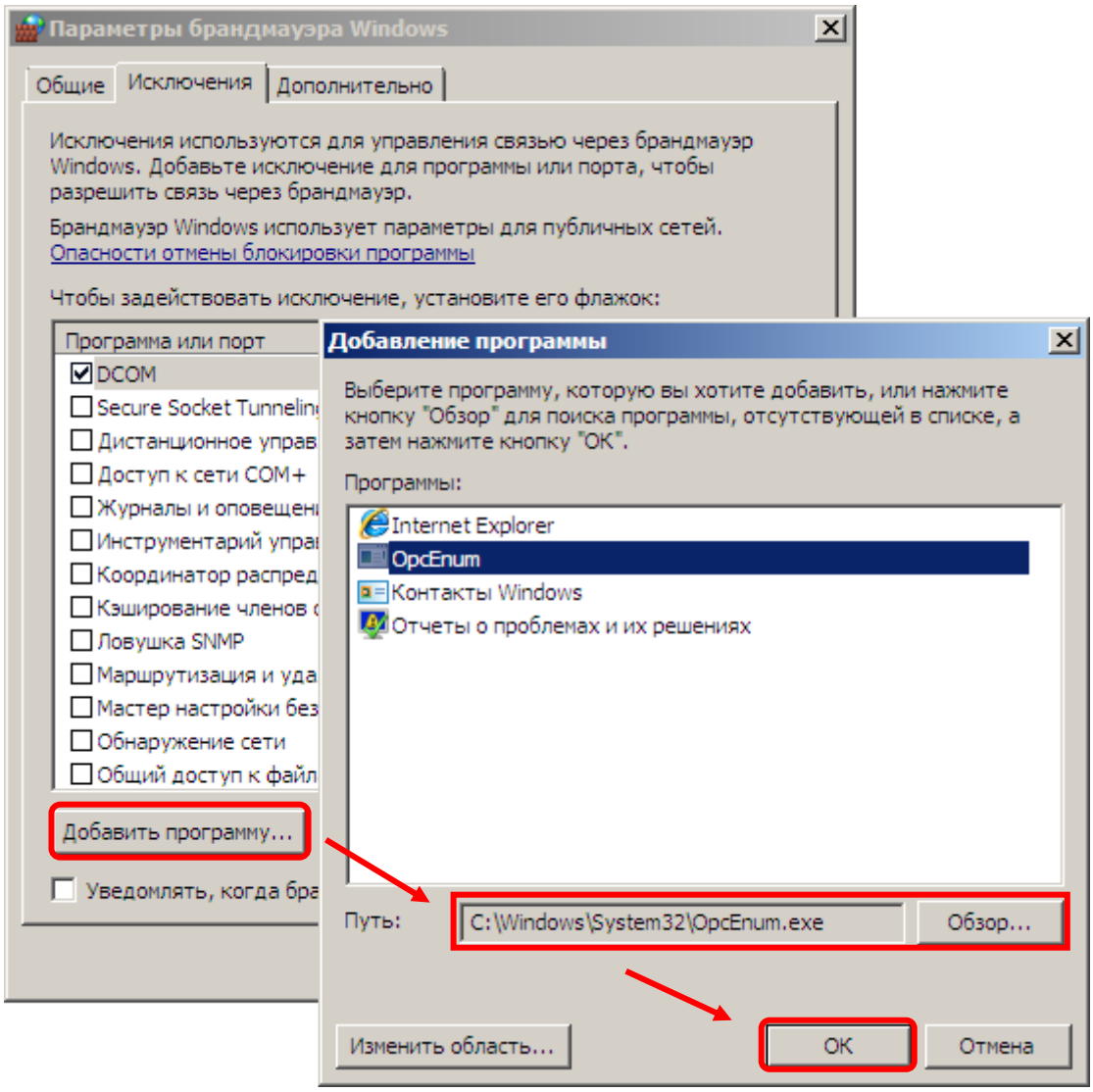

Рисунок 3.13 – Добавление программы в исключения брандмауэра

4 НАСТРОЙКА ПОЛИТИК БЕЗОПАСНОСТИ

☝**Внимание!!!**

Все настройки, описанные в этом пункте, производятся на компьютере, где установлен OPC-сервер, и на компьютере, где установлен OPC-клиент, если будет использоваться асинхронный опрос.

4.1 Настройка политики безопасности для Windows XP

Для работы с удаленным OPC-сервером нужно выполнить настройки политик безопасности на компьютере сервера. Для изменения политик безопасности можно воспользоваться утилитой «**Локальные параметры безопасности**» («Local Security Settings»). Чтобы открыть утилиту, нужно выбрать «**Пуск / Панель управления / Администрирование / Локальная политика безопасности**». Нужные политики находятся в разделе «**Локальные политики / Параметры безопасности**». Настройте следующие политики:

1 «**Сетевой доступ: модель совместного доступа и безопасности для локальных учётных записей**» (Network access: Sharing and security model for local accounts).
Установить обычную модель безопасности и совместного доступа. Для этого откройте диалоговое окно настройки параметра данной политики и выберите из ниспадающего списка пункт «Обычная – локальные пользователи удостоверяются как они сами» (Classic – local users authenticate as themselves), если выбрано другое значение (рисунок 4.1). Примените сделанное изменение нажатием кнопки «**OK**».

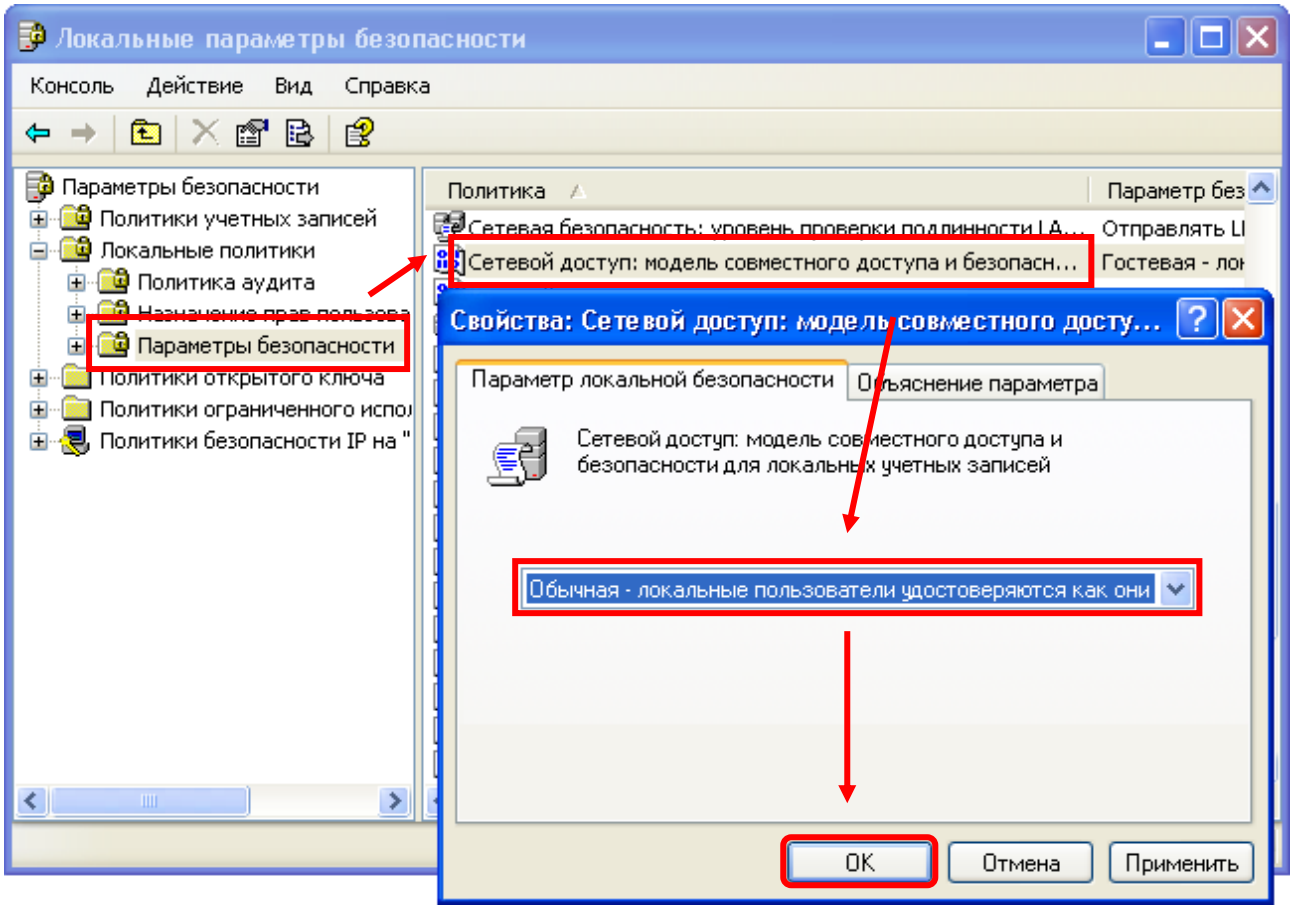

Рисунок 4.1 — Настройка политики «Сетевой доступ: модель совместного доступа и безопасности для локальных учётных записей»

2 «**DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)**».

Если эта политика уже была изменена ранее, необходимо добавить новые разрешения на доступ к приложениям DCOM. Для этого нажмите на кнопку «**Изменить безопасность…**». В открывшемся диалоговом окне для группы «**АНОНИМНЫЙ ВХОД**» установите галочки «**Разрешить**» для пунктов «**Локальный доступ**» и «**Удаленный доступ**» (рисунок 4.2).

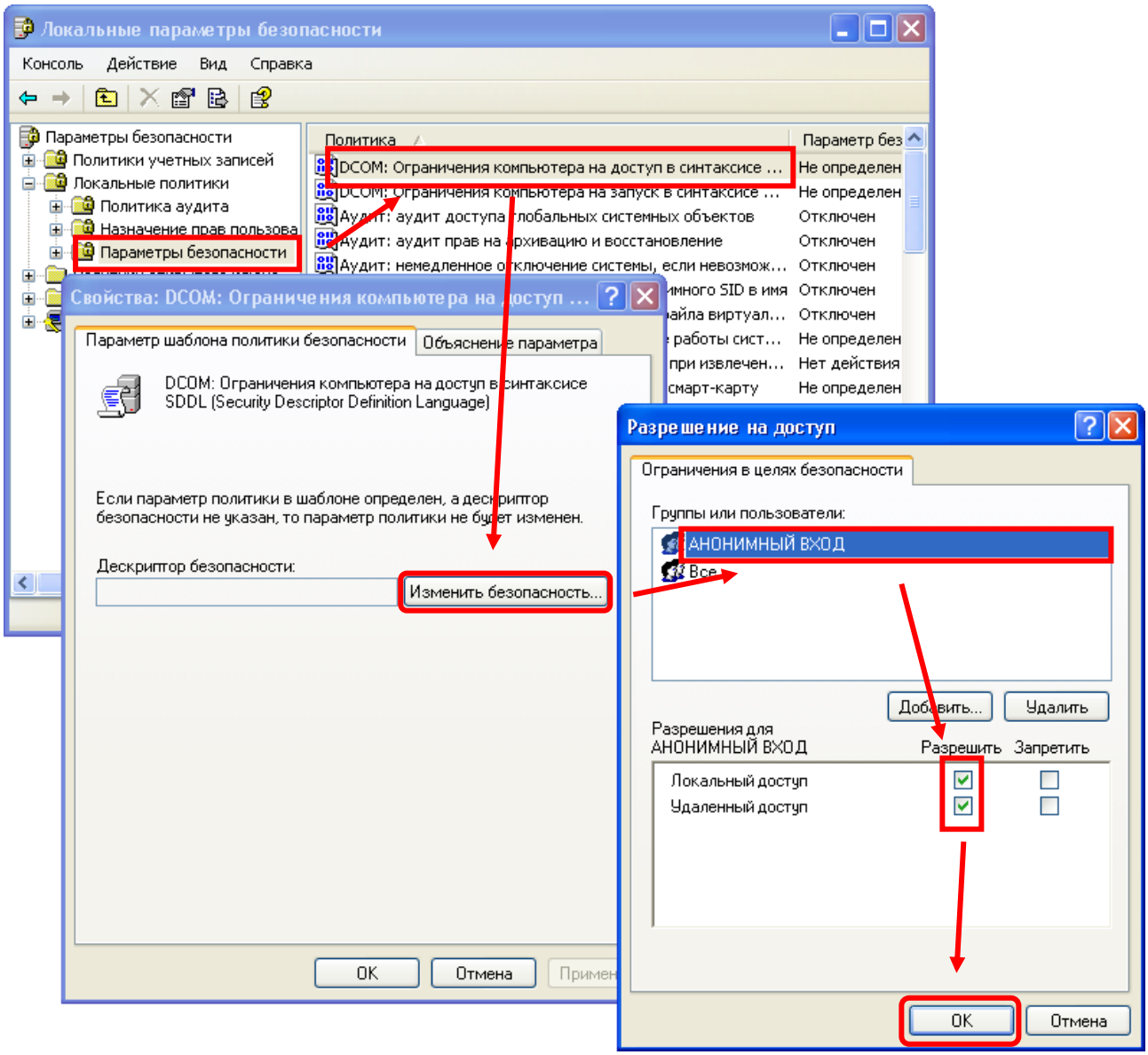

Рисунок 4.2 — Настройка политики «DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)»

3 «**DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language)**».
Если эта политика уже была изменена ранее, необходимо добавить новые разрешения на запуск приложений DCOM. Для этого нажмите на кнопку «**Изменить безопасность…**». В открывшемся диалоговом окне нажмите кнопку «**Добавить**» и добавьте группу, созданную в разделе 2 «**Создание и настройка учетных записей Пользователей**» («**Users OPC**»). Для этой группы поставьте галочки «**Разрешить**» для всех пунктов. Если пользователи группы должны получить только удаленный

доступ к OPC-серверу, поставьте галочки «**Разрешить**» только для пунктов «**Удаленный запуск**» и «**Удаленная активация**» (рисунок 4.3).

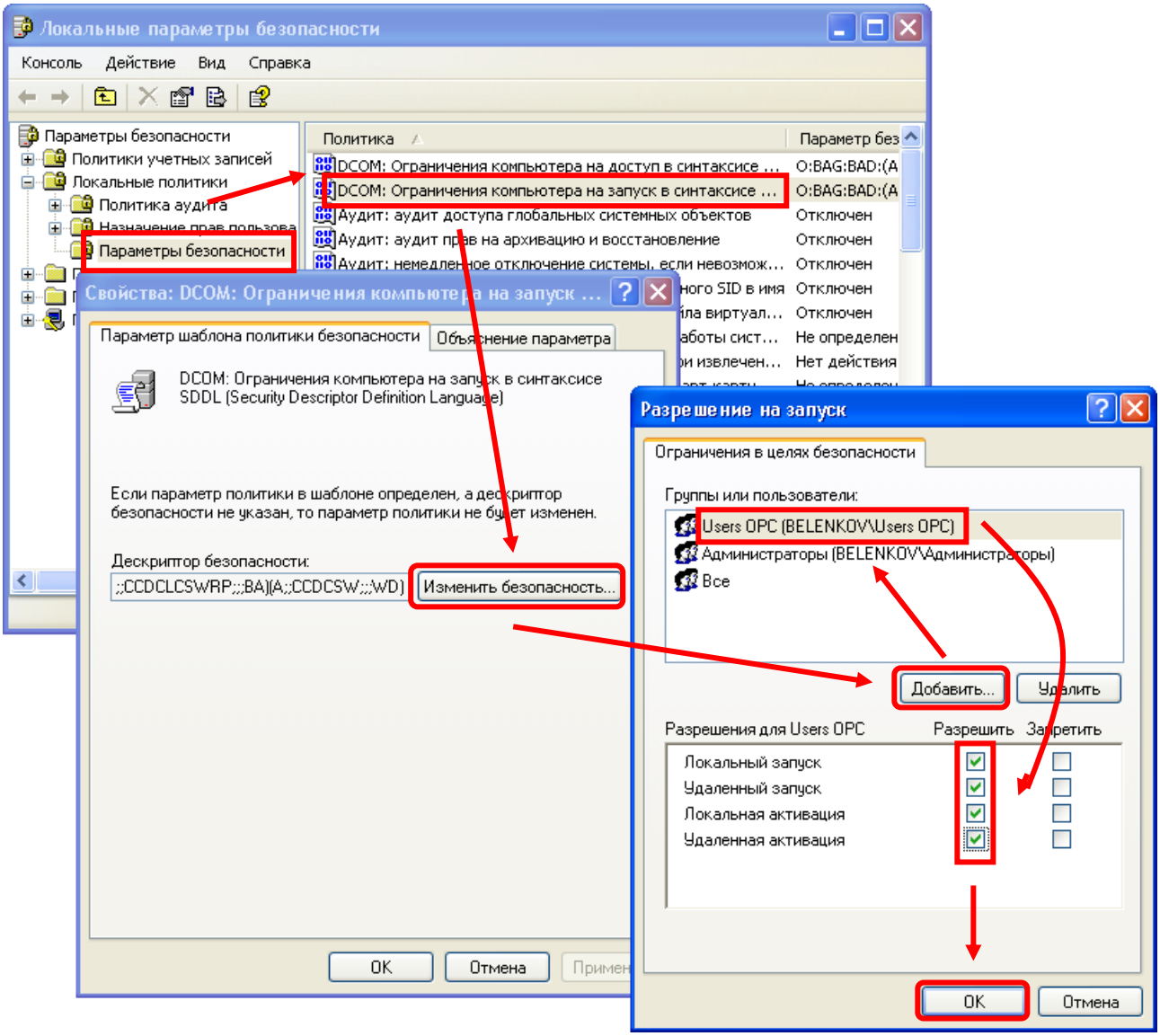

Рисунок 4.3 — Настройка политики «DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language)»

4.2 Настройка политики безопасности для Windows 7, Windows 8

Для работы с удаленным OPC-сервером нужно выполнить настройки политик безопасности на компьютере сервера. Для изменения политик безопасности можно воспользоваться утилитой «**Локальные параметры безопасности**» («Local Security Settings»). Чтобы открыть утилиту, нужно выбрать «**Пуск / Панель управления / Система и безопасность /**

Администрирование / Локальная политика безопасности». Нужные политики находятся в разделе «**Локальные политики / Параметры безопасности**». Необходимо настроить следующие политики.

1 «**Сетевой доступ: модель совместного доступа и безопасности для локальных учётных записей**» (Network access: Sharing and security model for local accounts). Установить обычную модель безопасности и совместного доступа. Для этого откройте диалоговое окно настройки параметра данной политики и выберите из ниспадающего списка пункт «**Обычная – локальные пользователи удостоверяются как они сами**» (Classic – local users authenticate as themselves), если выбрано другое значение (рисунок 4.4). Примените сделанное изменение нажатием кнопки «**OK**».

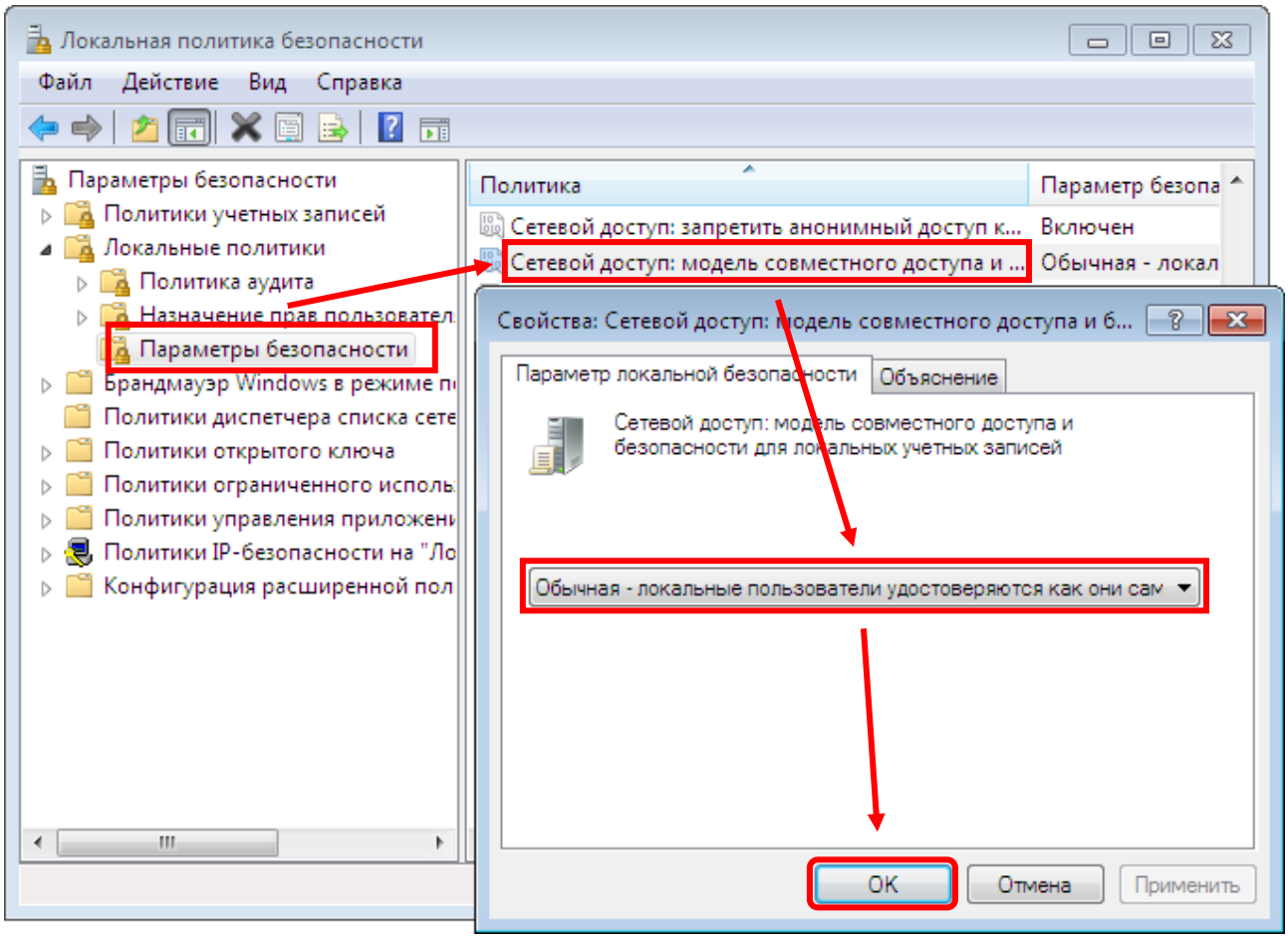

Рисунок 4.4 – Настройка политики сетевого доступа

2 «**DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)**».

Если эта политика уже была изменена ранее, необходимо добавить новые разрешения на доступ к приложениям DCOM. Для этого нажмите на кнопку «**Изменить безопасность…**». В открывшемся диалоговом окне для группы «**АНОНИМНЫЙ ВХОД**» установите галочки «**Разрешить**» для пунктов «**Локальный доступ**» и «**Удаленный доступ**» (рисунок 4.5).

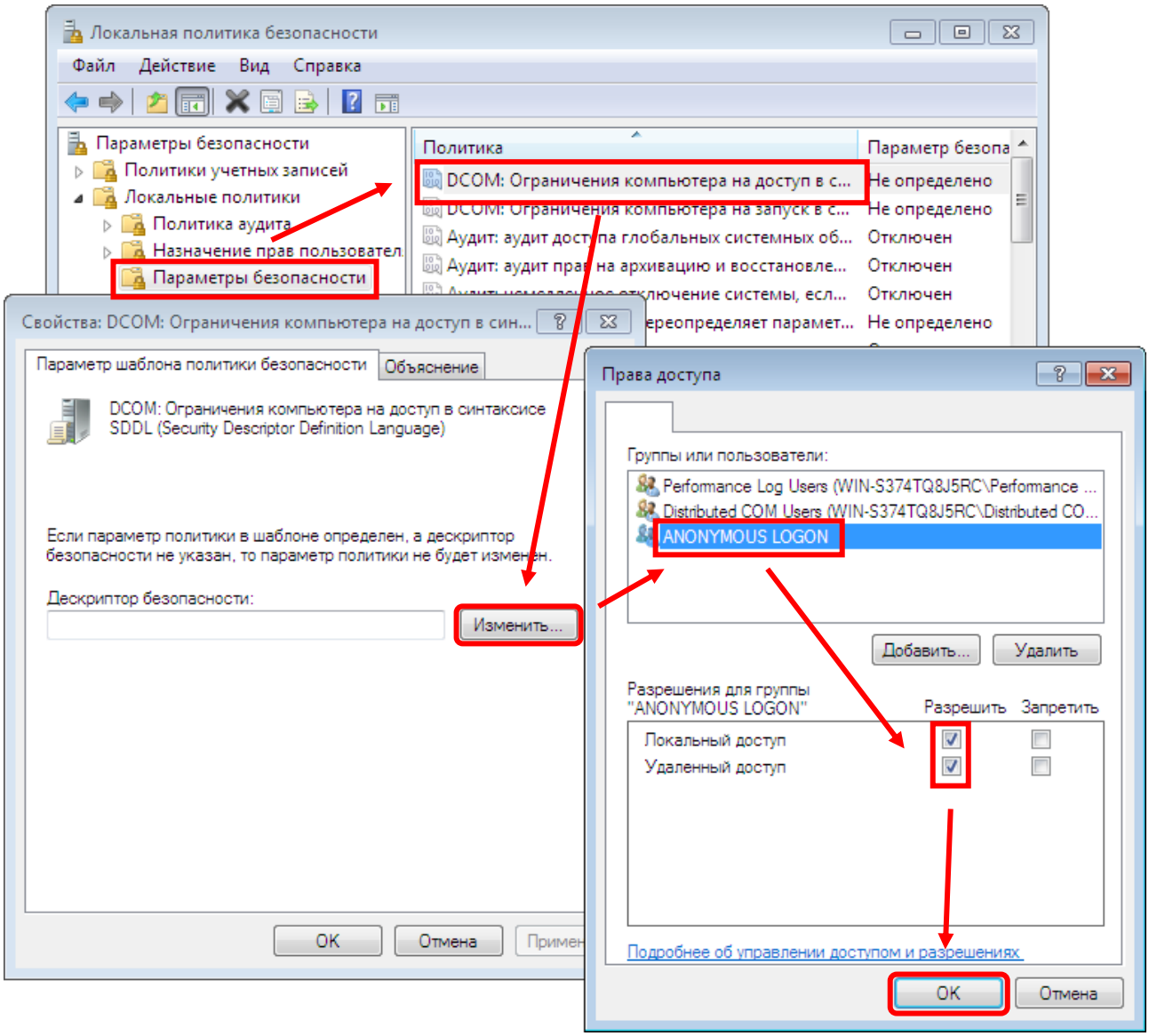

Рисунок 4.5 – Настройка DCOM-политики ограничения компьютера на доступ

3 «**DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language)**».

Если эта политика уже была изменена ранее, необходимо добавить новые разрешения на запуск приложений DCOM. Для этого нажмите на кнопку «**Изменить безопасность…**». В открывшемся диалоговом окне нажмите кнопку «**Добавить**» и добавьте группу, созданную в разделе 2 «**Создание и настройка учетных записей Пользователей**» («**Users OPC**»). Для этой группы поставьте галочки «**Разрешить**» для всех пунктов. Если пользователи группы должны получить только удаленный доступ к OPC-серверу, поставьте галочки «**Разрешить**» только для пунктов «**Удаленный запуск**» и «**Удаленная активация**» (рисунок 4.6).

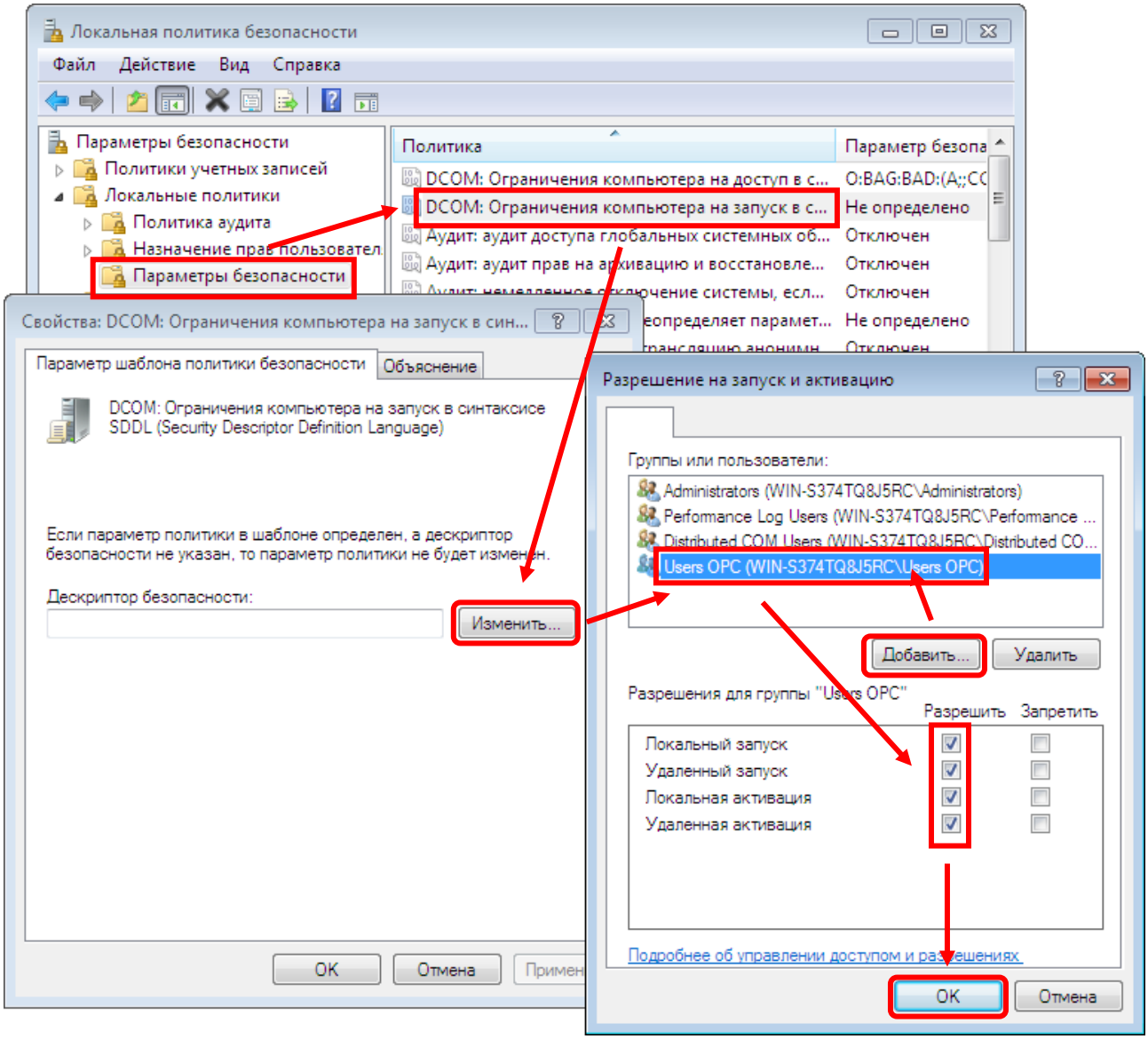

Рисунок 4.6 - Настройка DCOM-политики ограничения компьютера на запуск

4.3 Настройка политики безопасности для Windows Server 2008, Windows Server 2012

Для работы с удаленным OPC-сервером нужно выполнить настройки политик безопасности на компьютере сервера. Для изменения политик безопасности можно воспользоваться утилитой «**Локальные параметры безопасности**» («Local Security Settings»). Чтобы открыть утилиту, нужно выбрать «**Пуск / Панель управления / Администрирование / Локальная политика безопасности**». Нужные политики находятся в разделе «**Локальные политики / Параметры безопасности**». Необходимо настроить следующие политики.

1 «**Сетевой доступ: модель совместного доступа и безопасности для локальных учётных записей**» (Network access: Sharing and security model for local accounts).

Установить обычную модель безопасности и совместного доступа. Для этого откройте диалоговое окно настройки параметра данной политики и выберите из ниспадающего списка пункт «**Обычная – локальные пользователи удостоверяются как они сами**» (Classic – local users authenticate as themselves), если выбрано другое значение (рисунок 4.7). Примените сделанное изменение нажатием кнопки «**OK**».

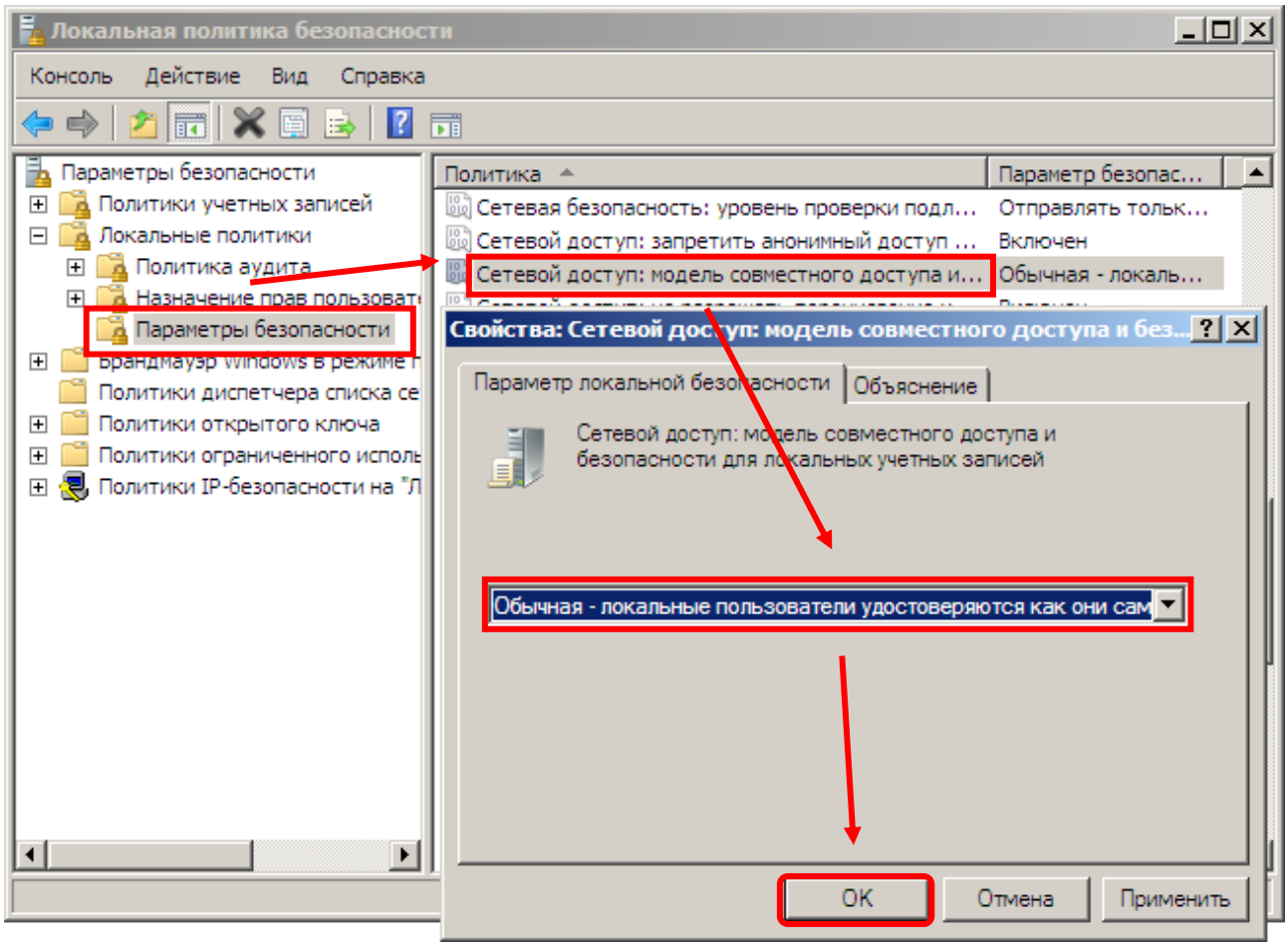

Рисунок 4.7 – Настройка политики сетевого доступа

2 «**DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)**».

Если эта политика уже была изменена ранее, необходимо добавить новые разрешения на доступ к приложениям DCOM. Для этого нажмите на кнопку «**Изменить безопасность…**». В открывшемся диалоговом окне для группы «**АНОНИМНЫЙ ВХОД**» установите галочки «**Разрешить**» для пунктов «**Локальный доступ**» и «**Удаленный доступ**» (рисунок 4.8).

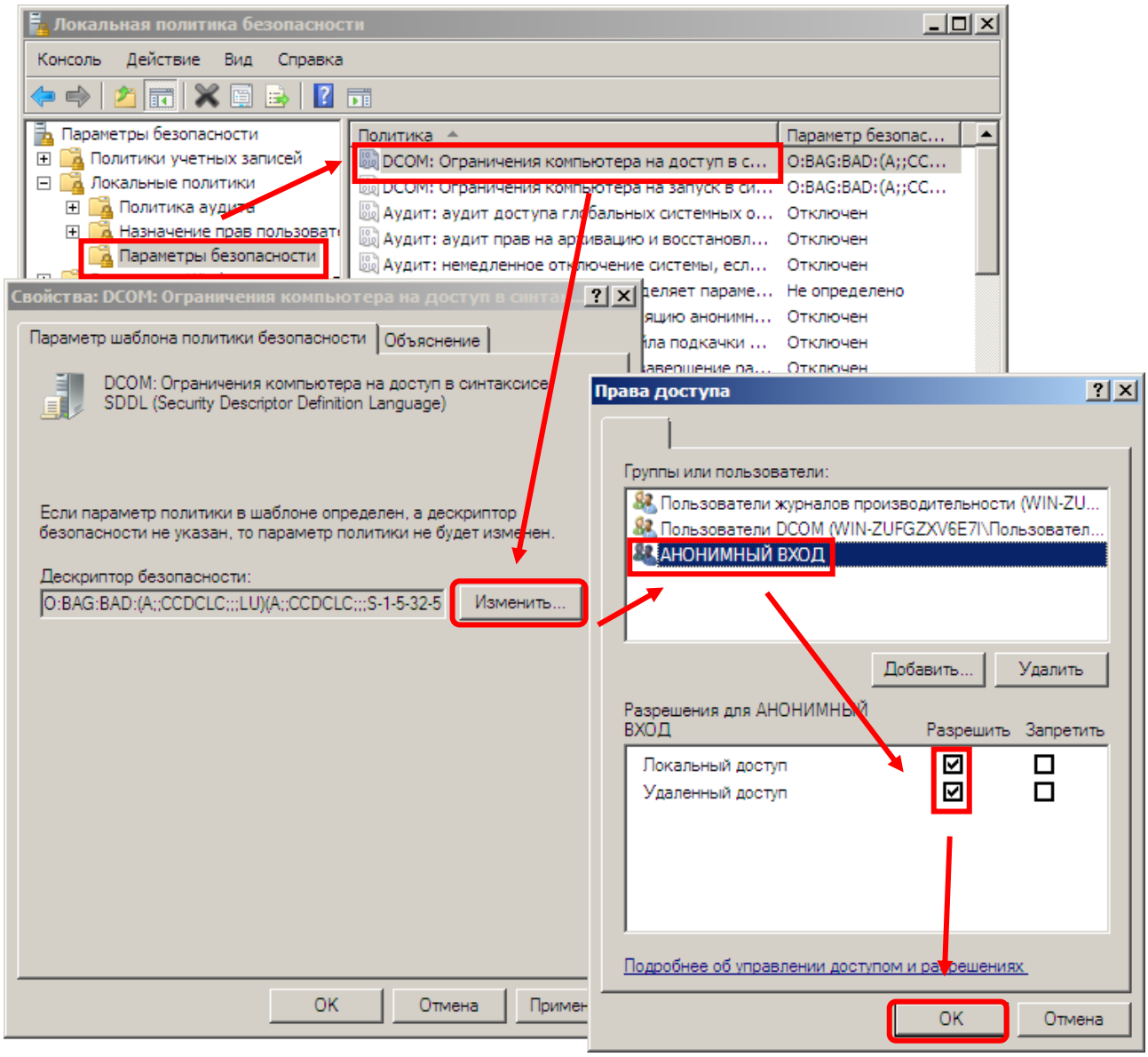

Рисунок 4.8 – Настройка DCOM-политики ограничения компьютера на доступ

3 «**DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language)**».
Если эта политика уже была изменена ранее, необходимо добавить новые разрешения на запуск приложений DCOM. Для этого нажмите на кнопку «**Изменить безопасность…**». В открывшемся диалоговом окне нажмите кнопку «**Добавить**» и добавьте группу, созданную в разделе 2 «**Создание и настройка учетных записей Пользователей**» («**Users OPC**»). Для этой группы поставьте галочки «**Разрешить**» для всех пунктов. Если пользователи группы должны получить только удаленный

доступ к OPC-серверу, поставьте галочки «**Разрешить**» только для пунктов «**Удаленный запуск**» и «**Удаленная активация**» (рисунок 4.9).

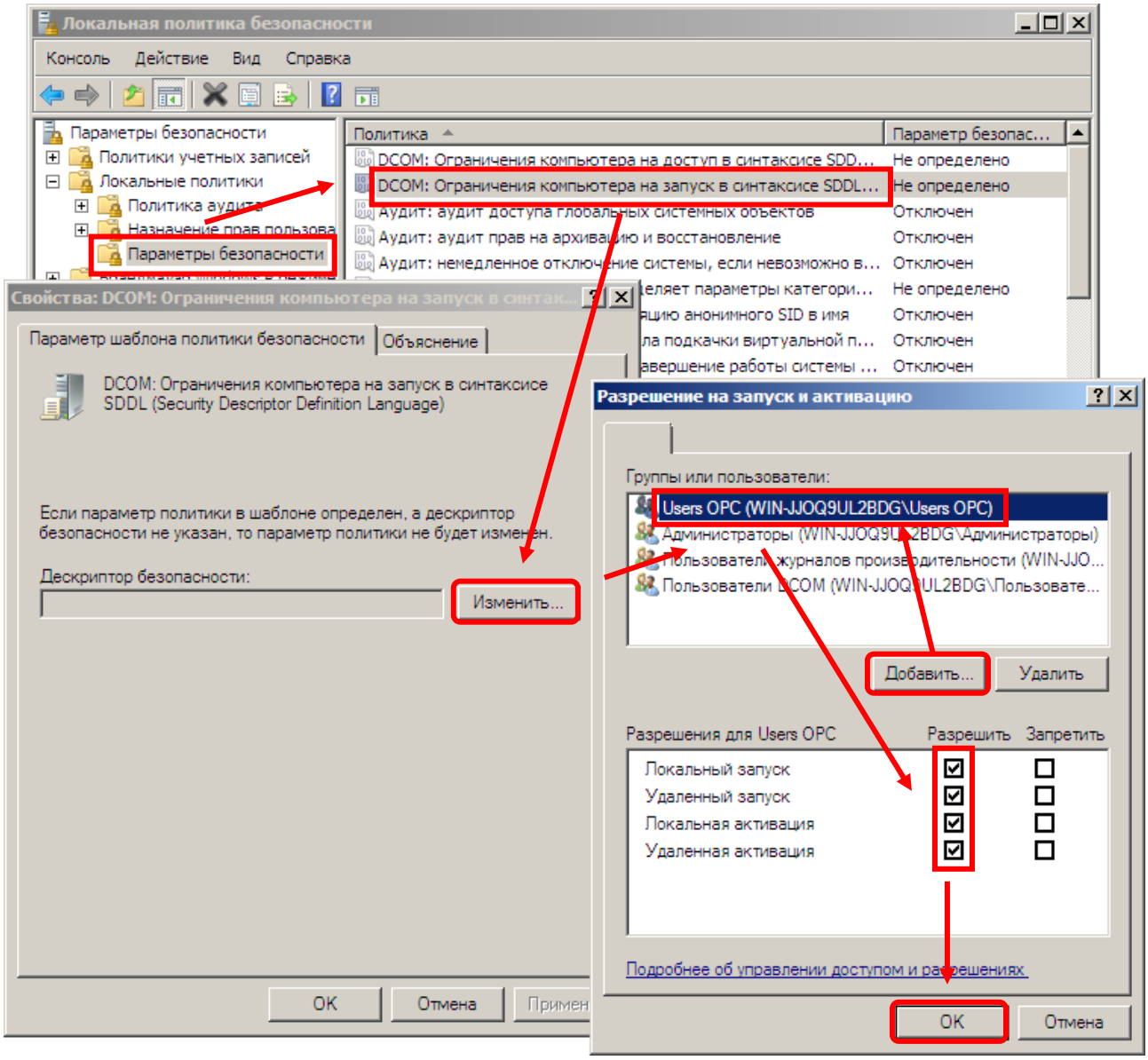

Рисунок 4.9 - Настройка DCOM-политики ограничения компьютера на запуск

5 НАСТРОЙКА DCOM

5.1 Настройка DCOM для Windows XP

5.1.1 Запуск утилиты настройки DCOM

Для настройки прав доступа к DCOM-приложениям в операционной системе Windows XP используется утилита «**Службы компонентов»** (Component Services) консоли управления. Утилиту можно вызвать:

- из системного меню **«Пуск/Выполнить»**, выполнив команду **dcomcnfg** (рисунок 5.1);

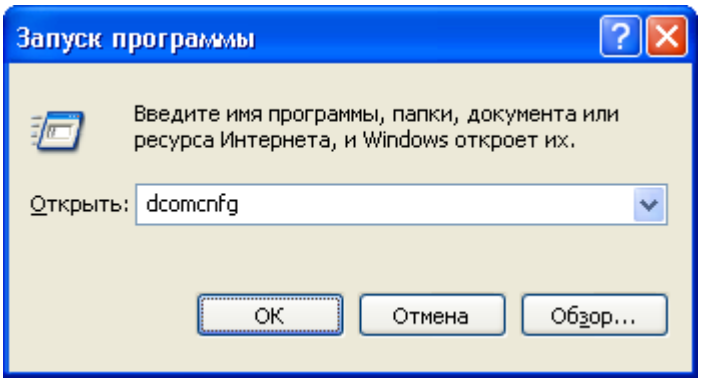

Рисунок 5.1 - Запуск утилиты dcomcnfg

- из системного меню **«Пуск/Панель управления/Администрирование/Службы компонентов»** (рисунок 5.2);

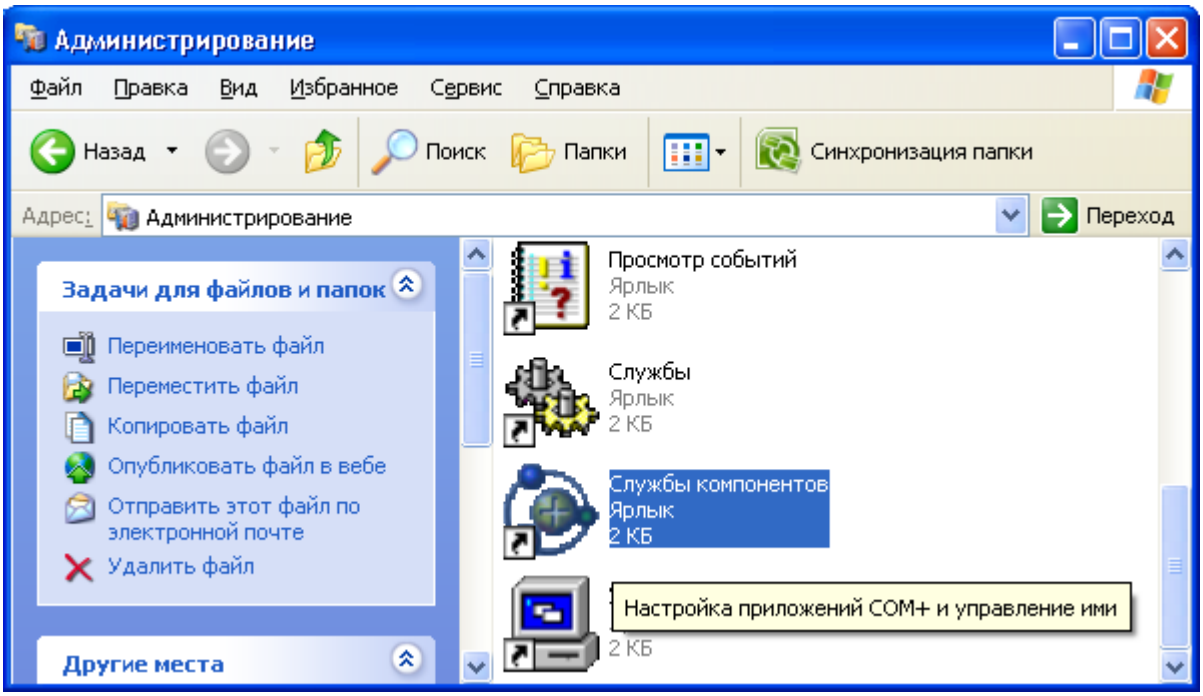

Рисунок 5.2 – Системные инструментальные средства «Службы компонентов»

ВНИМАНИЕ!!!

После запуска утилиты «Службы компонентов» производится поиск COM-приложений, которые ещё не зарегистрированы в системе на данный момент, и предлагается зарегистрировать их. Обычно, следует разрешать регистрацию, за исключением случаев, когда иное не указано в документации на программное обеспечение.

После запуска появляется окно «**Службы компонентов**» (рисунок 5.3).

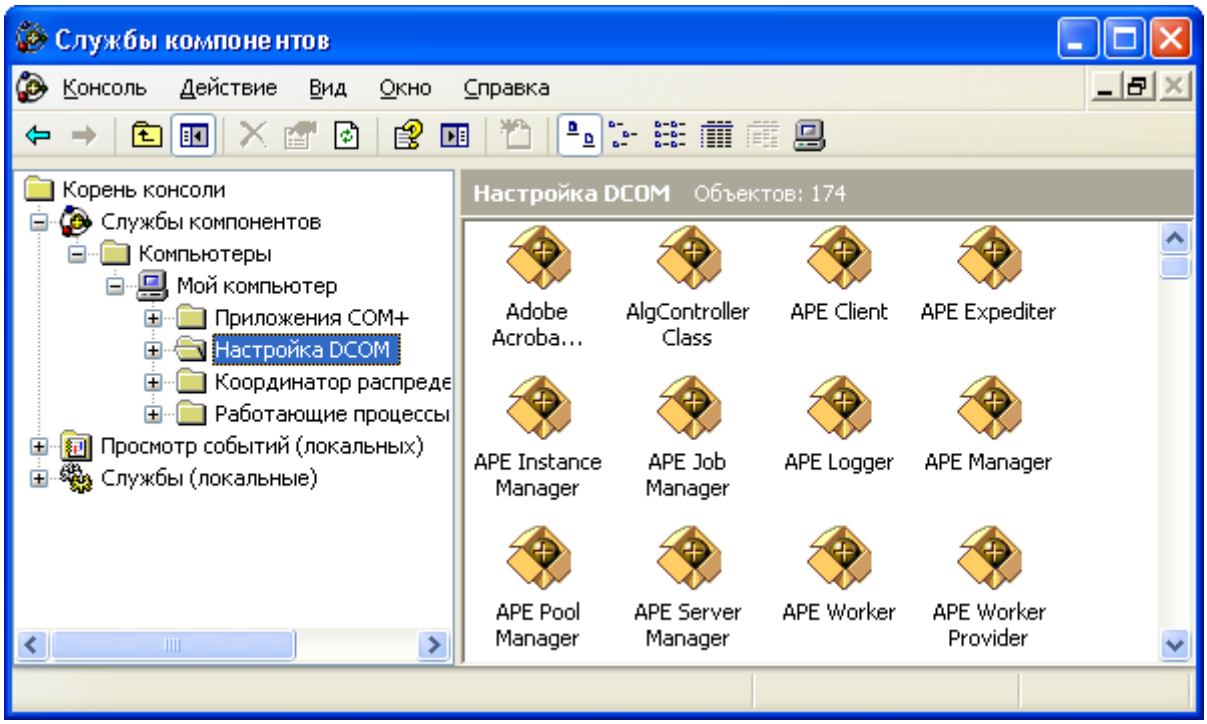

Рисунок 5.3 - Утилита «Службы компонентов»

5.1.2 Настройка общих параметров DCOM

Для установления связи с удаленными OPC-серверами сначала следует настроить общие параметры DCOM.

Для этого следует:

1. Необходимо запустить утилиту «**Службы компонентов**» и выбрать раздел «**Корень консоли/Службы компонентов/Компьютеры**» («Console Root/Component Services/Computers»).

2 Открыть контекстное меню элемента **«Мой компьютер»** («My Computer») и выбрать пункт **«Свойства»** («Properties») – рисунок 5.4

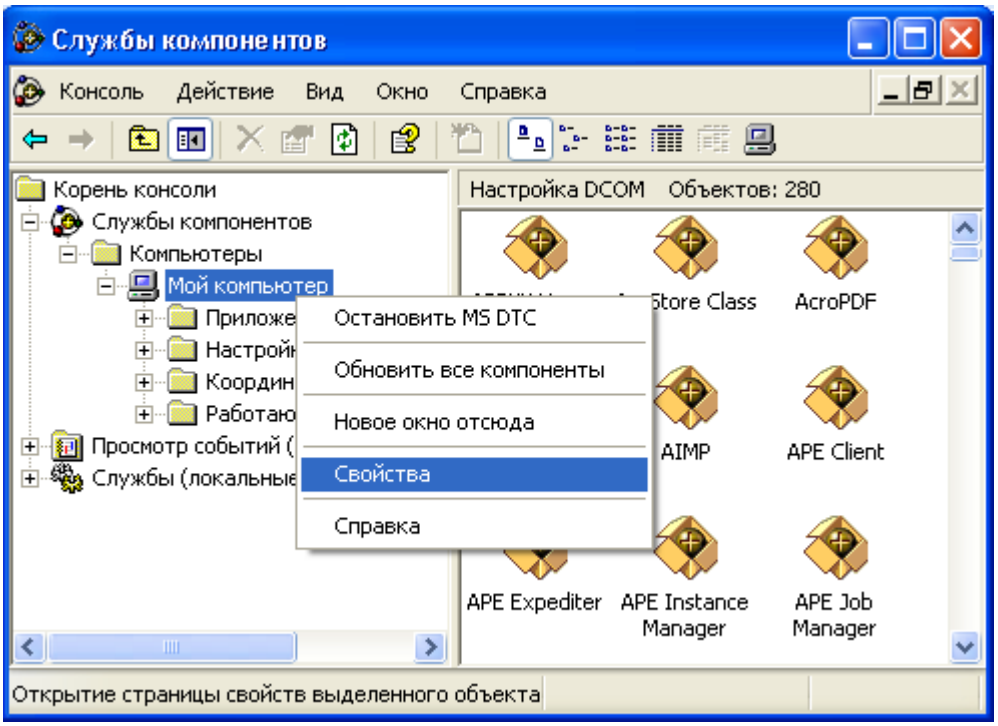

Рисунок 5.4 - Контекстное меню «Мой компьютер»

3 В открывшемся окне «**Свойства: Мой компьютер**» (рисунок 5.5) нужно перейти на закладку «**Безопасность**» (“COM Security”)

4 Нажать на кнопку «**Изменить ограничения…**» в секции «**Права доступа**» (рисунок 5.5). В открывшемся окне «**Разрешение на доступ**» для группы «**АНОНИМНЫЙ ВХОД**» установите галочки «**Разрешить**» для пунктов «**Локальный доступ**» и «**Удаленный доступ**» (рисунок 5.6).

Кнопка «**Изменить ограничения…**» может быть не доступна, если была изменена политика «**DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)**». В этом случае можно пропустить текущий шаг.

Эти настройки необходимы для функционирования утилиты поиска OPC-серверов (**OPCEnum.exe**) и некоторых OPC-серверов, для которых «**Уровень проверки подлинности**» («Authentication Level») установлен «**Нет**» («None»).

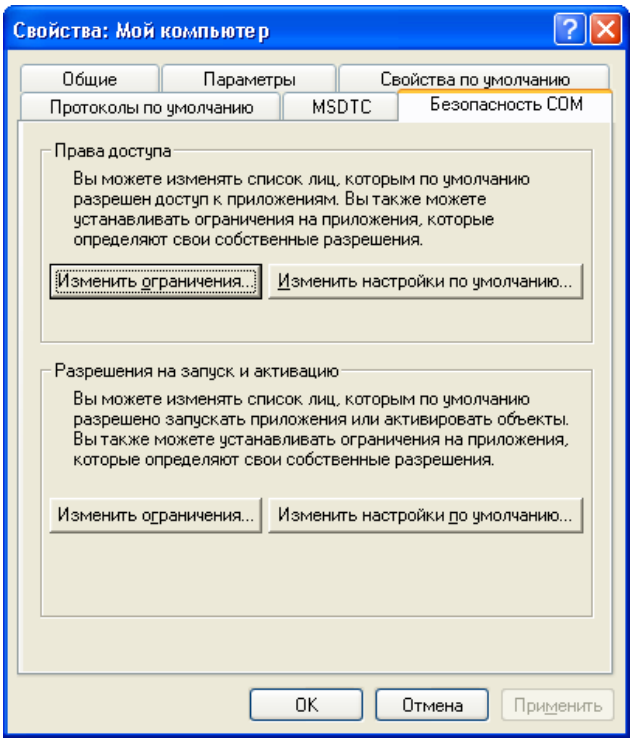

Рисунок 5.5 - Свойства компьютера, закладка «Безопасность COM»

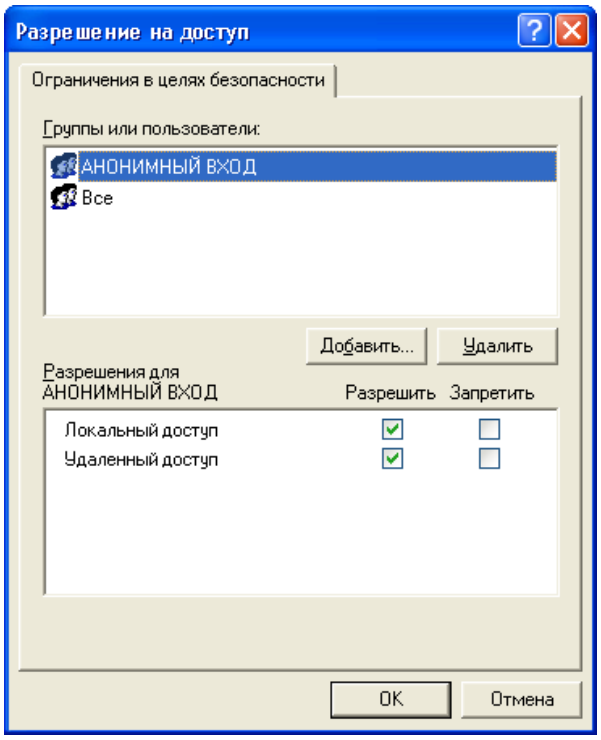

Рисунок 5.6 - Окно настройки «Разрешение на доступ»

ВНИМАНИЕ!!!

Этот шаг настройки необходимо выполнить как на компьютере, где установлен OPC-сервер, так и на компьютере, где установлен OPC-клиент. Остальные шаги выполняются на компьютере сервера.

5 Нажать на кнопку «**Изменить ограничения…**» в секции «**Разрешения на запуск и активацию**» (рисунок 5.5). В открывшемся окне «**Разрешение на запуск**» нажать кнопку «**Добавить**» и добавить группу «**Users OPC**». Для этой группы поставить галочки «**Разрешить**» для всех вариантов запуска и активации (рисунок 5.7).

Кнопка «**Изменить ограничения…**» может быть не доступна, если была изменена политика «**DCOM: Ограничения компьютера на запуск в синтаксисе SDDL**» («Security Descriptor Definition Language»). В этом случае пропустите текущий шаг.

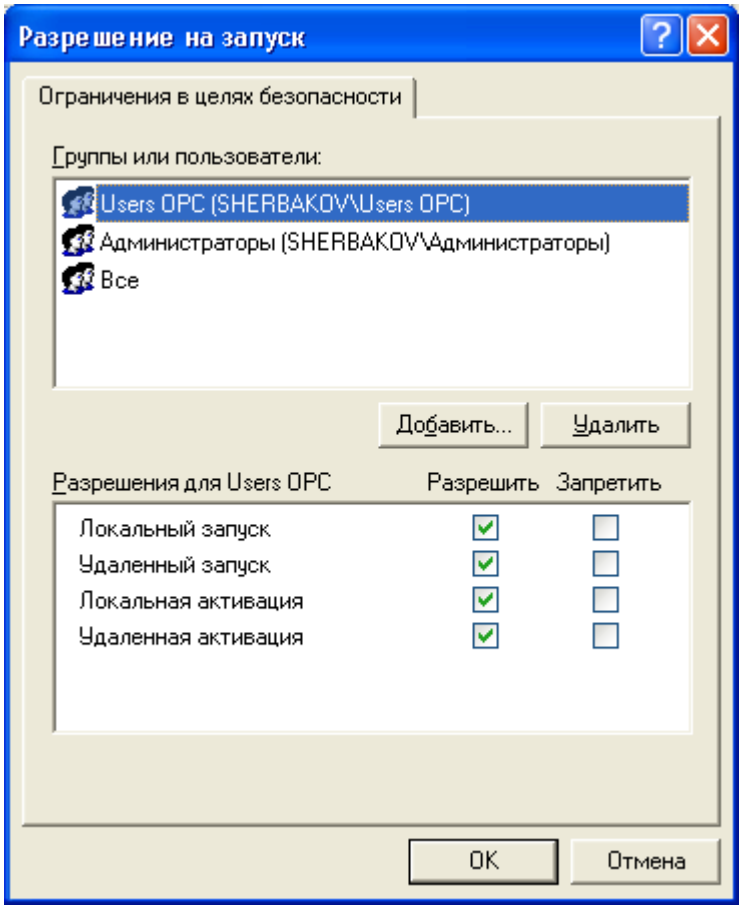

Рисунок 5.7 - Окно настройки «Разрешение на запуск»

Если Пользователи группы должны получить только удаленный доступ к OPC-серверу, следует поставить галочки «**Разрешить**» только для пунктов «**Удаленный запуск**» и «**Удаленная активация**».

6 Остальные общие параметры DCOM могут остаться по умолчанию. Если они были изменены, и это нарушило работу OPC-серверов, верните их в прежнее состояние. Список параметров по умолчанию приведен ниже:

- Вкладка **«Свойства по умолчанию»** (рисунок 5.8)

  Значения по умолчанию:

  - Установлена галочка «**Разрешить использование DCOM на этом компьютере**».
  - «Уровень проверки подлинности по умолчанию» – «**Подключение**».
  - «Уровень олицетворения по умолчанию» – «**Идентификация**».
  - Снята галочка «**Повышенная безопасность для отслеживания ссылок**».

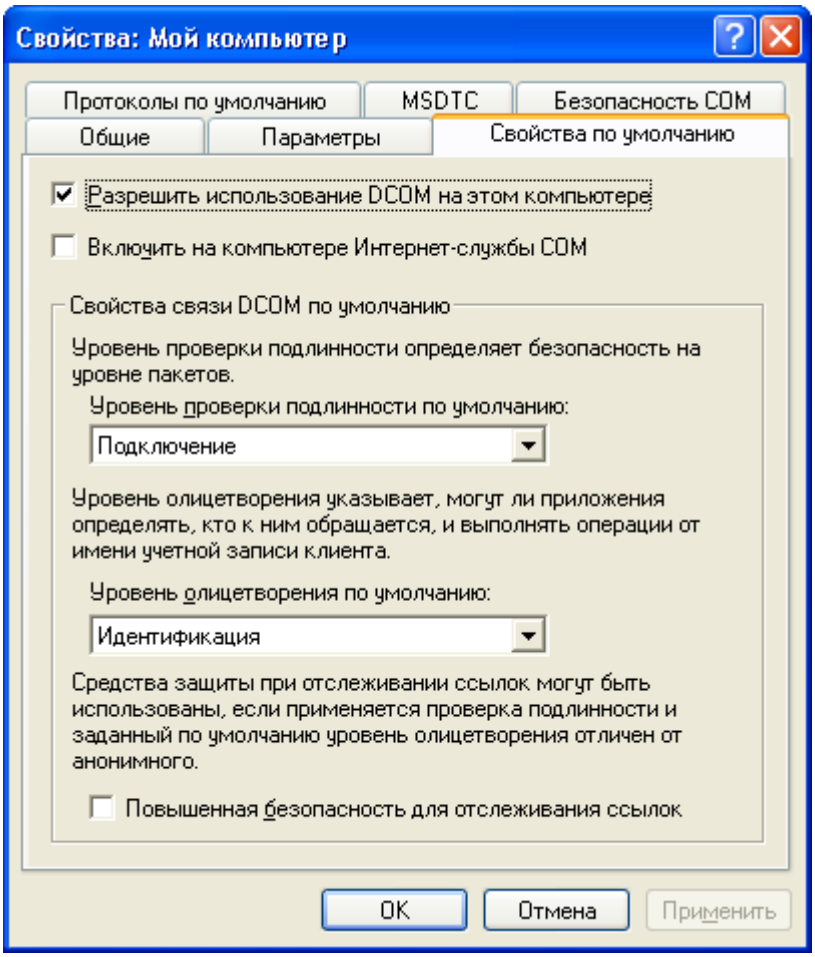

Рисунок 5.8 — Свойства компьютера, закладка «Свойства по умолчанию»

- Вкладка «Протоколы по умолчанию» (рисунок 5.9)

  Добавлены следующие протоколы DCOM:

  - «TCP/IP с ориентацией на подключения»
  - «SPX с ориентацией на подключения».

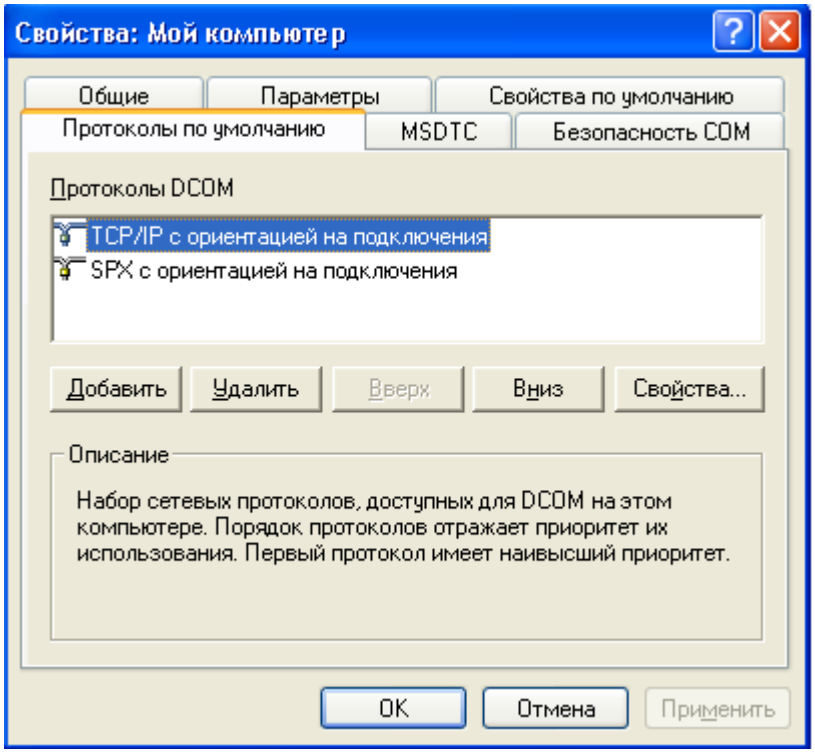

Рисунок 5.9 - Свойства компьютера, закладка «Протоколы по умолчанию»

- Закладка «**Параметры**» (рисунок 5.10)

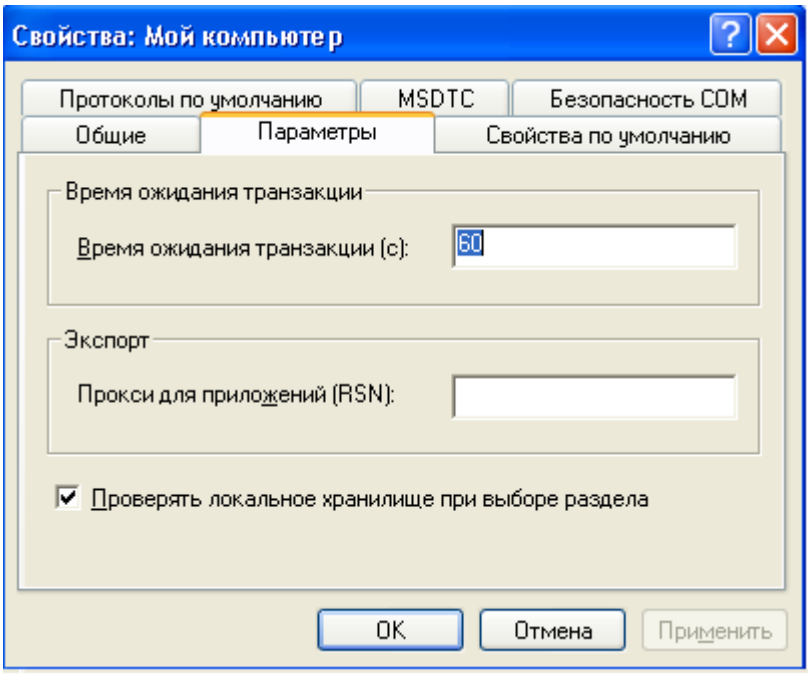

Рисунок 5.10 - Свойства компьютера, закладка «Параметры»

Значения по умолчанию:

- Установлена галочка «**Проверять локальное хранилище при выборе раздела**».
- «Время ожидания транзакции (с)»: **60**.

  При работе в компьютерной сети в случае возникновения обрывов, переполнения и других критических ситуациях при попытках восстановления связи DCOM-приложения используют время ожидания транзакции (Transaction timeout). Это время, в течение которого DCOM-приложение посылает запрос к источнику данных и ожидает восстановления связи. DCOM-приложение совершает до 6 таких попыток, прежде чем подаст сигнал об ошибке в сети.
  По умолчанию этот интервал равен 60 секундам. Соответственно, максимальное время, за которое DCOM-приложение определит, что сеть неисправна – 60*6 = 360 секунд или 6 минут.

  Однако это время не всегда может устроить Пользователей DCOM-приложения. Очевидно, что чем короче время ожидания транзакции, тем быстрее DCOM-приложение сможет сообщить Пользователю об ошибке в сети. Поэтому, если Пользователь DCOM-приложения хочет сократить время определения ошибки в сети, он может уменьшить время ожидания транзакции.

ВНИМАНИЕ !!!

Времени ожидания транзакции настраивается на компьютере сервера. При изменении времени ожидания транзакции следует понимать, что это коснется ВСЕХ DCOM-приложений, работающих на этом компьютере. Поэтому, если нет сильной необходимости изменить значение по умолчанию для этого пункта, то изменять его не рекомендуется.

5.1.3 Настройка параметров DCOM для OPC-сервера

ВНИМАНИЕ!!!

Настройки, описанные в этом пункте, производятся на компьютере, где установлен OPC-сервер.

Для того чтобы настроить параметры DCOM для конкретного OPC-сервера, следует:

1. В утилите «**Службы компонентов**» выбрать раздел «**Корень консоли / Службы компонентов / Компьютеры / Мой компьютер / Настройка DCOM**» («Console Root / Component Services / Computers / My Computer / DCOM Config»).

2. Открыть контекстное меню нужного OPC-сервера (рисунок 5.11) и выбрать пункт «**Свойства**» («Properties»).

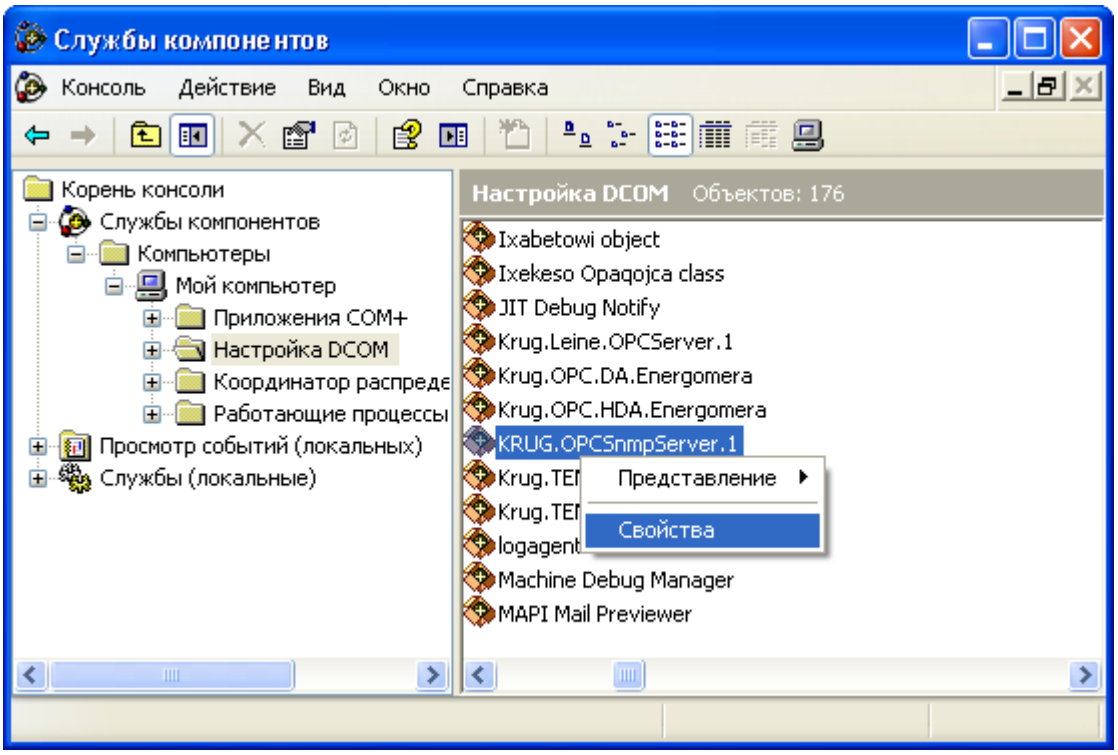

Рисунок 5.11 - Выбор свойств OPC-сервера

3. В открывшемся окне «**Свойства:**…» перейти на вкладку «**Безопасность**» («Security»).

4 В секции «**Разрешения на запуск и активацию**» выбрать «**Настроить**» и нажать на кнопку «**Изменить…**». В открывшемся окне «**Разрешение на запуск**» (рисунок 5.12) нажать кнопку «**Добавить**» и добавить группу «**Users OPC**».

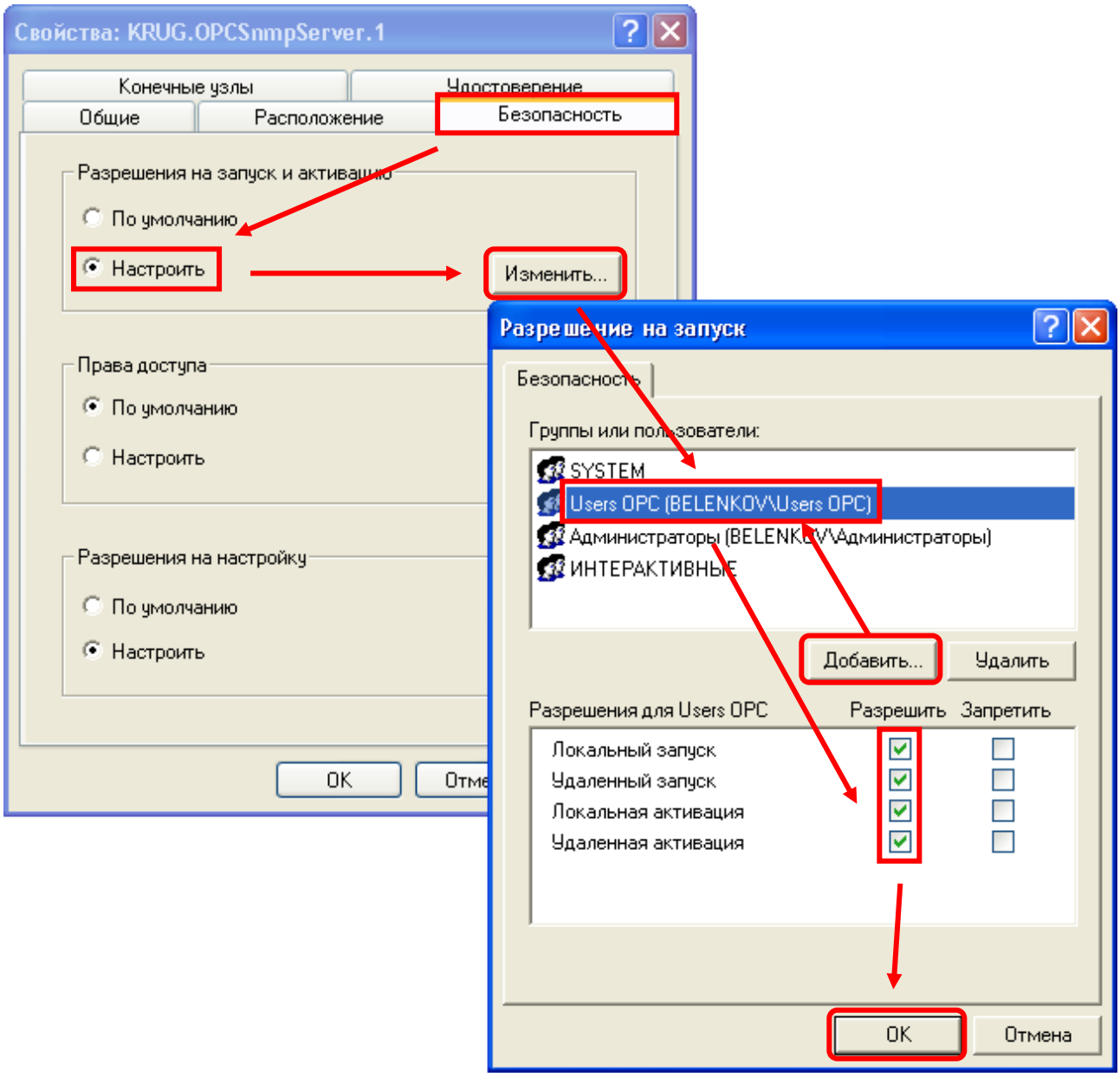

Рисунок 5.12 - Окно настройки «Разрешение на запуск» для OPC-сервера

Для группы «**Users OPC**» поставить галочки «**Разрешить**» для всех пунктов. Если Пользователи группы должны получить только удаленный доступ к OPC-серверу,

поставить галочки «**Разрешить**» только для пунктов «**Удаленный запуск**» и «**Удаленная активация**»

5 На секции «**Права доступа**» (вкладка «Безопасность») выбрать «**Настроить**» и нажать на кнопку «**Изменить…**». В открывшемся окне «**Разрешение на доступ**» (рисунок 5.13) нажать кнопку «**Добавить**» и добавить группу «**Users OPC**».

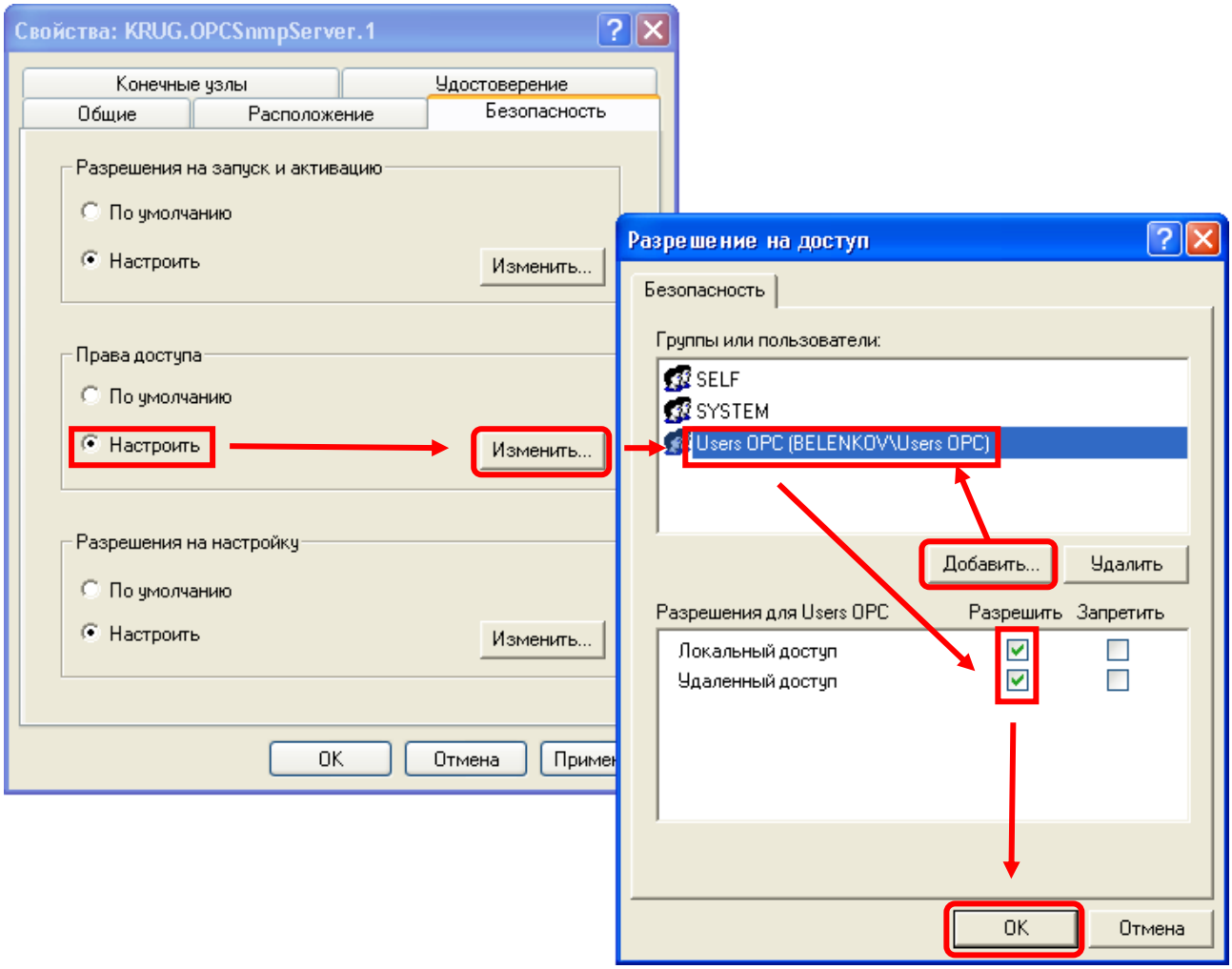

Рисунок 5.13 - Окно настройки «Разрешение на доступ» для OPC-сервера

Для этой группы («**Users OPC**») поставьте галочки «**Разрешить**» для всех вариантов доступа. Если Пользователи группы должны получить только удаленный доступ к OPC-серверу, поставьте галочку «**Разрешить**» только для пункта «**Удаленный доступ**».

6 Для того, чтобы указать под какой учетной записью будет запускаться OPC-сервер, нужно перейти на вкладку «**Удостоверение**» (рисунок 5.14).

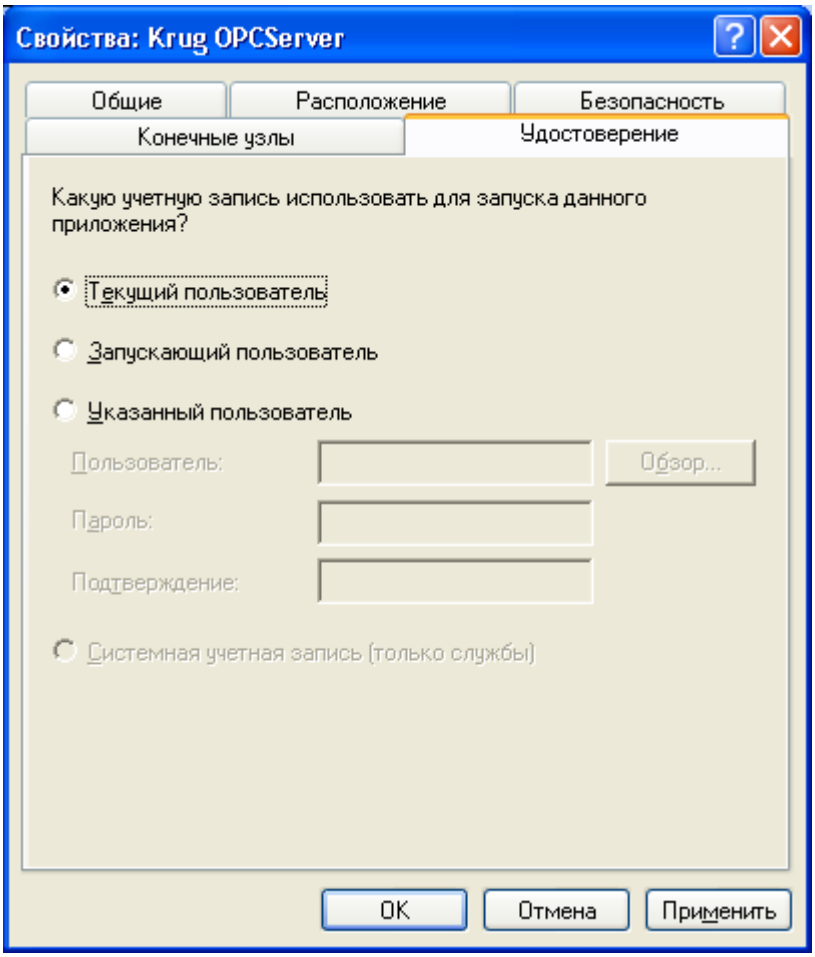

Рисунок 5.14 - Свойства OPC-сервера, закладка «Удостоверение»

Выбор учетной записи для запуска данного приложения зависит от реализации данного OPC-сервера. Следует воспользоваться документацией к OPC-серверу, чтобы выбрать тип Пользователя.

Общие рекомендации по выбору Пользователя для запуска OPC-сервера приведены в таблице 5.1.

Таблица 5.1 Рекомендации по выбору Пользователя для запуска OPC-сервера

Параметр	Описание
«**Текущий Пользователь**» (The Interactive User)	OPC-сервер будет запускаться под учетной записью вошедшего в систему интерактивного Пользователя. Это позволит OPC-сервер взаимодействовать с Пользователем, т.е. Пользователь увидит все видимые окна, открываемые OPC-сервером (например, диалоги, сообщения об ошибках). Однако если компьютер не используется ни одним из Пользователей, т.е. текущего Пользователя не существует, в этом случае OPC-сервер запущен не будет. К тому же, если в систему зайдет Пользователь с недостаточными правами, работоспособность приложения может оказаться под угрозой. Когда интерактивный Пользователь выходит из системы, все OPC-серверы с данной настройкой принудительно закрываются. Этот вариант запуска недоступен, если сервер зарегистрирован как сервис. **Рекомендуется использовать данный тип Пользователя, если OPC-сервер выводит на экран диалоговые окна, требующие реакции Пользователя.**
«**Запускающий Пользователь**» (The Launching User)	OPC-сервер будет запускаться под учетной записью запускающего Пользователя (обычно удаленного). Этому Пользователю должны быть предоставлены необходимые разрешения. Пользователь также должен обладать разрешениями, принимаемыми по умолчанию, введенными для группы Пользователей на этом компьютере. Другими словами, он должен принадлежать группе Пользователей. OPC-сервер не сможет напрямую взаимодействовать с интерактивным Пользователем. Т.е. Пользователь НЕ увидит открываемые OPC-сервером окна. **При подключении нового OPC-клиента будет запускаться отдельная копия OPC-сервера. Это может вызвать проблемы в работе. Например, при работе нескольких экземпляров OPC-сервера с устройством через один COM - порт.**

Параметр	Описание
«**Указанный Пользователь**» (This user)	OPC-сервер будет запускаться под учетной записью, указанной в поле «Пользователь» (User), которое становится доступно после активизации данного варианта загрузки. Требуется задать пароль. При этом имя учетной записи проверяется на правильность. Верность пароля при вводе не проверяется, о неправильности пароля вы узнаете только после того, как получите соответствующее сообщение об ошибке при попытке запустить OPC-сервер. OPC-сервер не сможет напрямую взаимодействовать с интерактивным Пользователем. Т.е. Пользователь НЕ увидит открываемые OPC-сервером окна. **Рекомендуется использовать данный тип Пользователя, если запускаемый OPC-сервер должен обладать специфическими правами доступа. Например, если требуется запустить OPC-сервер с правами Администратора, а ни текущий Пользователь, ни запускающий не принадлежат к группе «Администраторы».**
Системная учетная запись (The System Account)	OPC-сервер будет запускаться под учетной записью **SYSTEM**. Этот тип доступен, если сервер зарегистрирован как сервис. **Рекомендуется использовать данный тип Пользователя, если OPC-сервер является сервисом.**

☝**ВНИМАНИЕ!!!**

Если OPC-сервер запускается под учетной записью Пользователя, к которой нет доступа на компьютере клиента, то будет не доступен асинхронный опрос OPC-сервера.
Если компьютеры в рабочей группе, и должен использоваться асинхронный опрос, то нужно создать на клиенте такую же учетную запись.
Если компьютеры входят в состав домена, используйте для запуска OPC-сервера учетную запись Пользователя домена или системную учетную запись.

7 После выбора Пользователя для запуска OPC-сервера необходимо проверить, есть ли у него доступ к исполняемому файлу OPC-сервера.
Например, если exe-файл OPC-сервера помещен в папку, к которой запрещен доступ учетной записи, используемой для запуска OPC-сервера, тогда при запуске OPC-сервера клиент получит сообщение об ошибке «Отказ в доступе».

Чтобы проверить разрешения на доступ к исполняемому файлу OPC-сервера, нужно выполнить следующую последовательность действий:

- Открыть контекстное меню для папки, в которой находится exe-файл OPC-сервера, и выбрать пункт «**Свойства**» («Properties»).
- В открывшемся окне «**Свойства:**…» перейти на вкладку «**Безопасность**» (рисунок 5.15).

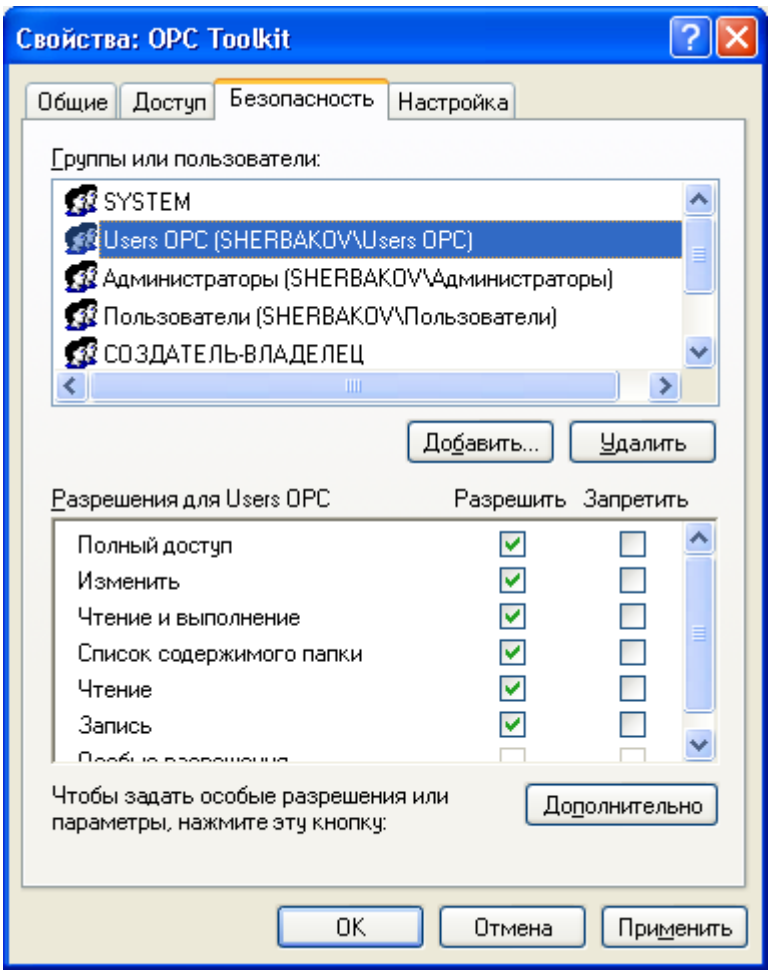

Рисунок 5.15 - Свойства папки, закладка «Безопасность»

- В списке «**Группы или Пользователи**» должен быть Пользователь, который используется для запуска OPC-сервера, или группа, в которую он включен. Если Пользователь отсутствует, нажать кнопку «**Добавить**» и добавить требуемого Пользователя.
- Если для выбранного Пользователя не установлен вариант доступа «**Полный доступ**», поставить галочку «**Разрешить**» для этого варианта.
- Нажать кнопку «**OK**» для сохранения сделанных изменений.

8 Для сохранения изменений нажать кнопку «**OK»**.
Чтобы изменения были применены к OPC-серверу, его необходимо перезапустить (если он был запущен ранее).

☝**ВНИМАНИЕ!!!**

Без перезапуска OPC-сервера измененные настройки не будут применены к нему.

Если OPC-сервер не имеет интерфейса Пользователя, с помощью которого он может быть перезапущен, завершить процесс OPC-сервера можно следующей последовательностью действий:

- открыть **Диспетчер задач Windows** и перейти на вкладку «**Процессы**»;
- выбрать процесс настраиваемого OPC-сервера и нажать кнопку «**Завершить процесс**».

После нового подключения OPC-клиента, OPC-сервер будет загружен уже с новыми настройками.

5.1.4 Настройка параметров DCOM для утилиты поиска OPC-серверов

☝ **ВНИМАНИЕ!!!**

Настройки параметров DCOM для утилиты OPCEnum.exe производятся только на компьютере, где установлены удаленные OPC-серверы.

При доступе к данным удаленного OPC-сервера используется стандартная OPC-утилита **OPCEnum.exe,** которая формирует список доступных OPC–серверов. Для использования этой утилиты необходимо настроить параметры DCOM.

Настройка разрешений осуществляется аналогично настройке OPC-серверов, описанной выше. Отличие заключается в том, что в списке приложений (компонент) необходимо выбирать **OpcEnum** (рисунок 5.16).

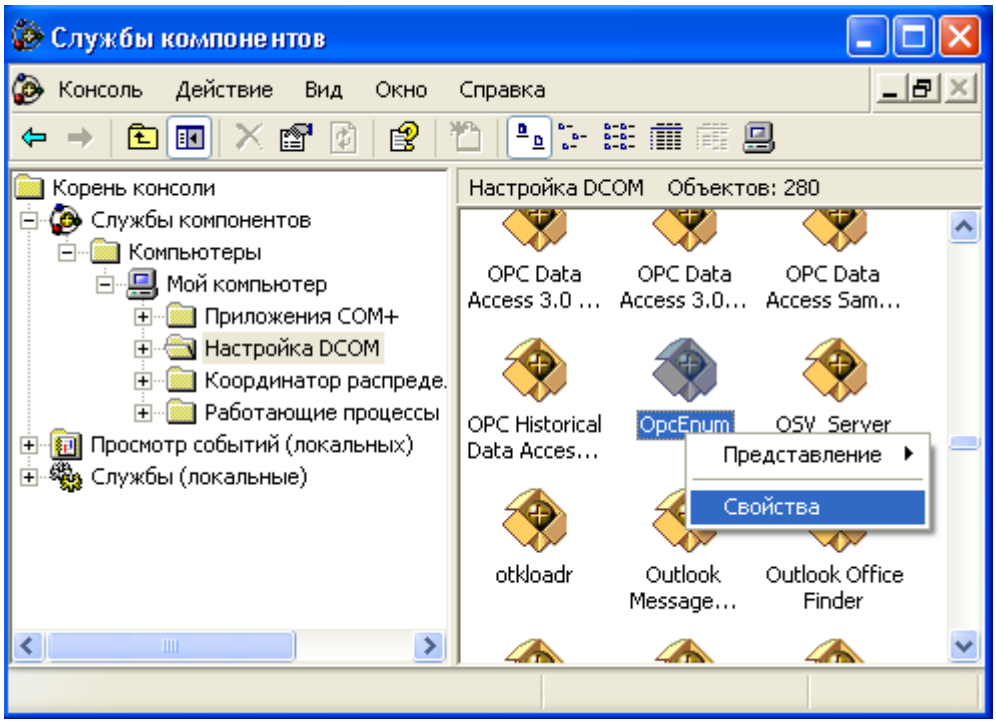

Рисунок 5.16 - Выбор свойств утилиты OPCEnum

5.2 Настройка DCOM для Windows 7, Windows 8

5.2.1 Запуск утилиты настройки DCOM

Для настройки прав доступа к DCOM-приложениям в операционной системе Windows 7 / 8 используется утилита «**Службы компонентов»** (Component Services) консоли управления.

В зависимости от разрядности операционной системы и приложения OPC-сервера необходимо запускать соответствующую версию этой утилиты:

- Версия Windows 32-х битная - команда "**dcomcnfg**" (рисунок 5.17).

- Версия Windows 64-х битная, исполняемый файл OPC сервера 64-х битный - команда "**dcomcnfg**" (рисунок 5.17).
- Версия Windows 64-х битная, исполняемый файл OPC сервера 32-х битный - команда "**mmc comexp.msc /32**".

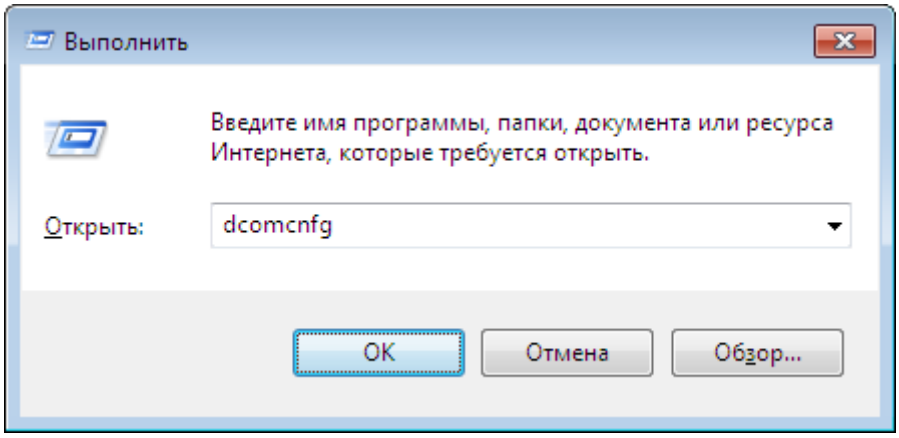

Рисунок 5.17 - Запуск утилиты dcomcnfg

Также утилиту «Службы компонентов» можно запустить из системного меню **«Пуск / Панель управления / Система и безопасность / Администрирование / Службы компонентов»** (рисунок 5.18).

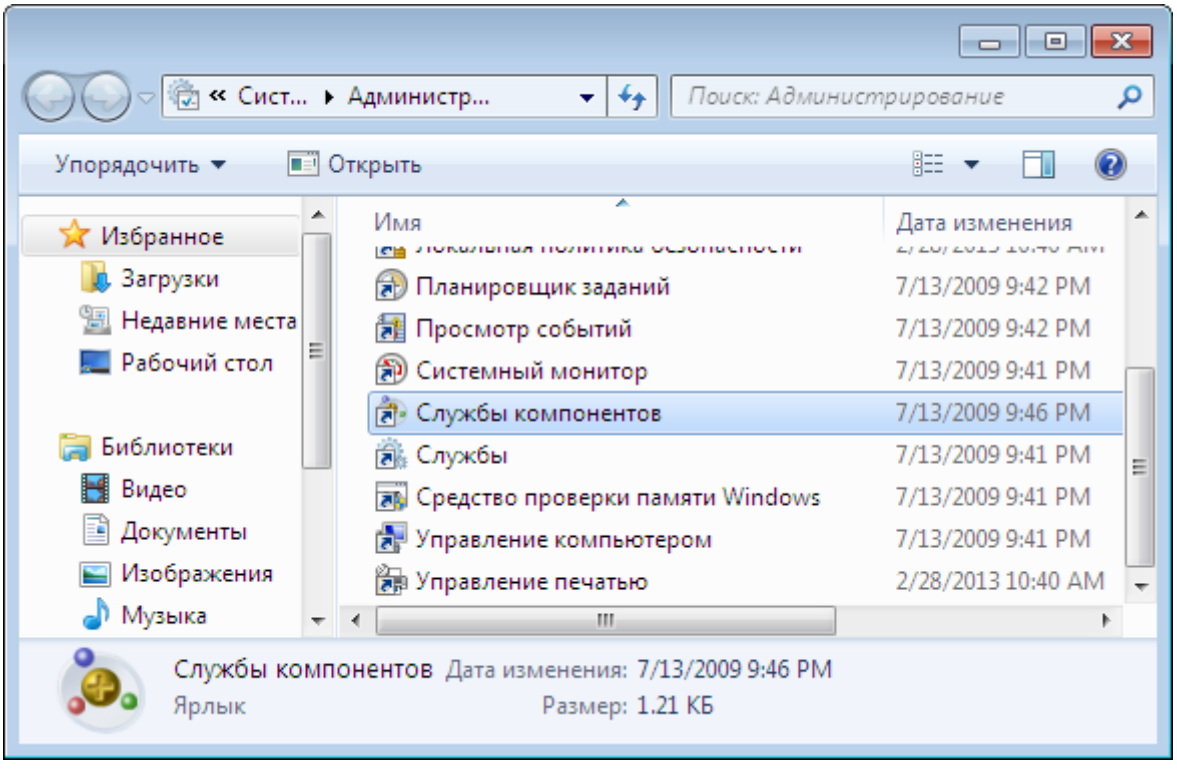

Рисунок 5.18 – Системные инструментальные средства «Службы компонентов»

ВНИМАНИЕ!!!

После запуска утилиты «Службы компонентов» производится поиск COM-приложений, которые ещё не зарегистрированы в системе на данный момент, и предлагается зарегистрировать их. Обычно, следует разрешать регистрацию, за исключением случаев, когда иное не указано в документации на программное обеспечение.

После запуска появляется окно «**Службы компонентов**» (рисунок 5.19).

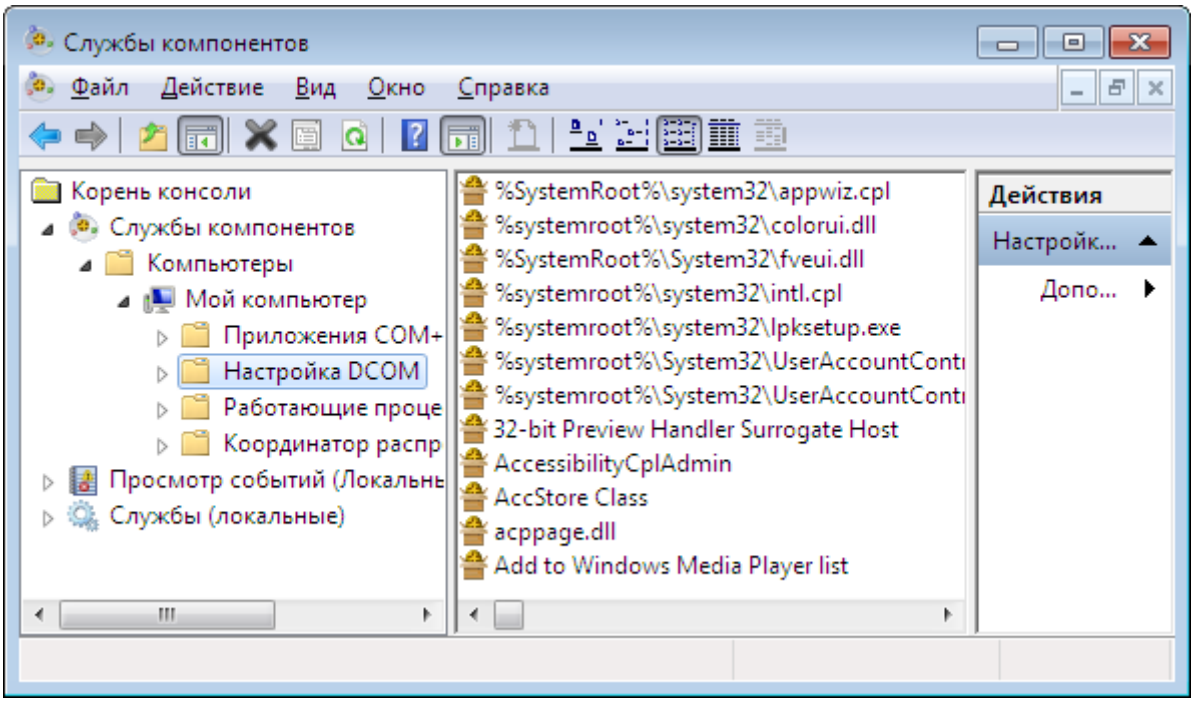

Рисунок 5.19 - Утилита «Службы компонентов»

5.2.2 Настройка общих параметров DCOM

Для установления связи с удаленными OPC-серверами сначала следует настроить общие параметры DCOM.

Для этого следует:

1. Необходимо запустить утилиту «**Службы компонентов**» и выбрать раздел «**Корень консоли / Службы компонентов / Компьютеры**» («Console Root / Component Services / Computers»).

2 Открыть контекстное меню элемента **«Мой компьютер»** («My Computer») и выбрать пункт **«Свойства»** («Properties») – рисунок 5.20.

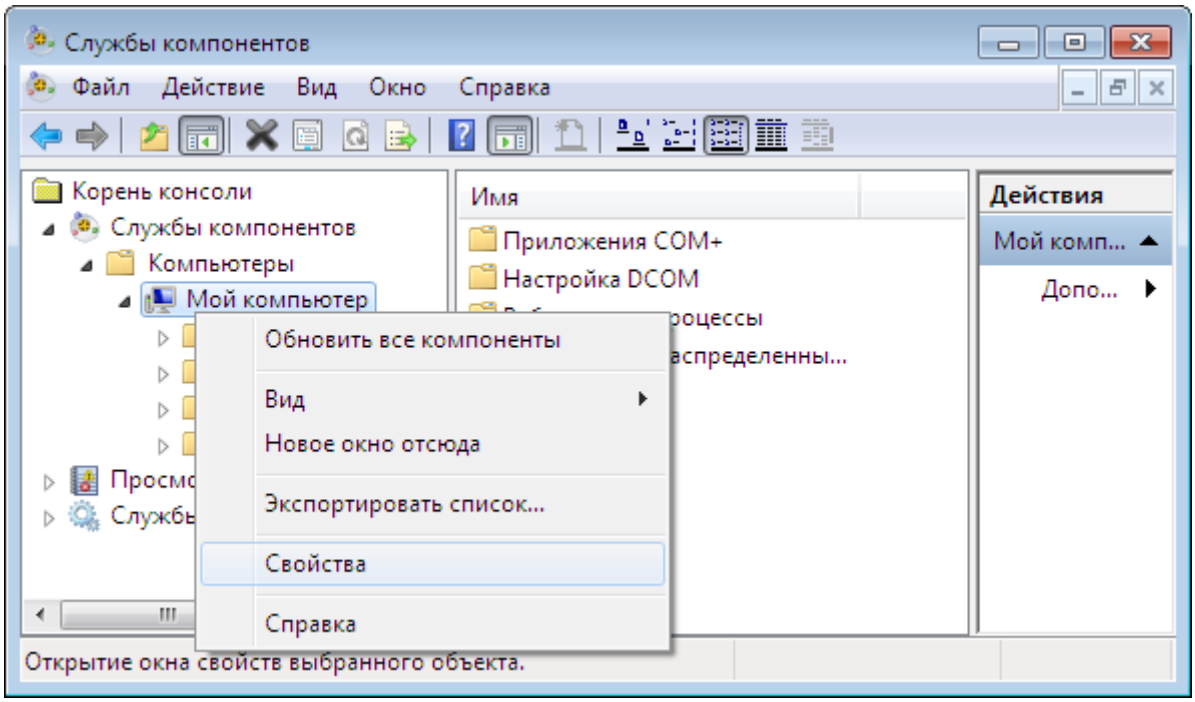

Рисунок 5.20 - Контекстное меню «Мой компьютер»

3 В открывшемся окне «**Свойства: Мой компьютер**» (рисунок 5.21) нужно перейти на закладку «**Безопасность COM**» («COM Security»)

4 Нажать на кнопку «**Изменить ограничения…**» в секции «**Права доступа**». В открывшемся окне «**Разрешение на доступ**» для группы «**АНОНИМНЫЙ ВХОД**» («ANONYMOUS LOGON») установите галочки «**Разрешить**» для пунктов «**Локальный доступ**» и «**Удаленный доступ**» (рисунок 5.21).

Кнопка «**Изменить ограничения…**» может быть не доступна, если была изменена политика «**DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)**». В этом случае можно пропустить текущий шаг.

Эти настройки необходимы для функционирования утилиты поиска OPC-серверов (**OPCEnum.exe**) и некоторых OPC-серверов, для которых «**Уровень проверки подлинности**» («Authentication Level») установлен «**Нет**» («None»).

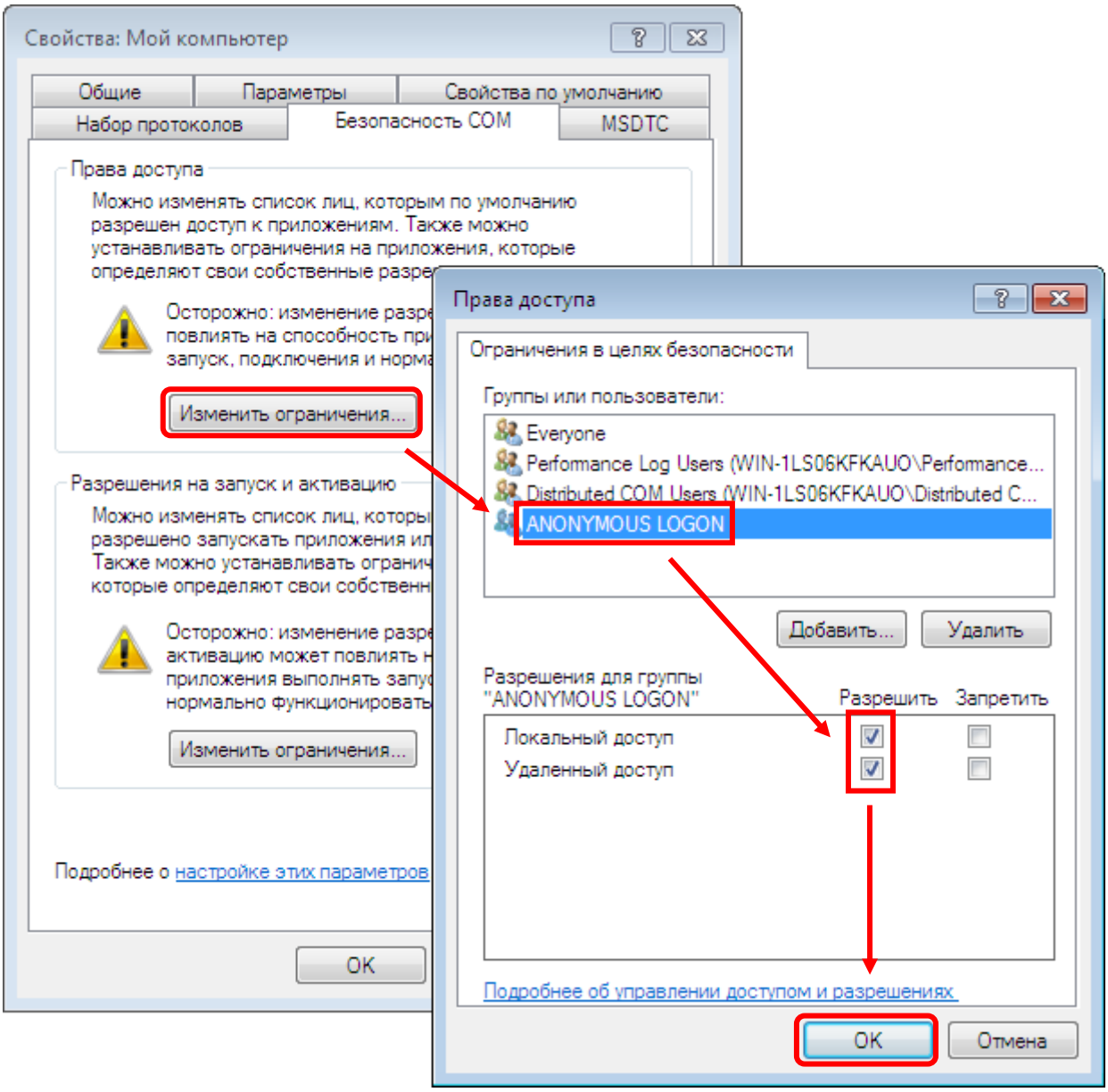

Рисунок 5.21 - Свойства компьютера, закладка «Безопасность COM»

ВНИМАНИЕ!!!

Этот шаг настройки необходимо выполнить как на компьютере, где установлен OPC-сервер, так и на компьютере, где установлен OPC-клиент. Остальные шаги выполняются на компьютере сервера.

5 Нажать на кнопку «**Изменить ограничения…**» в секции «**Разрешения на запуск и активацию**» (рисунок 5.22). В открывшемся окне «**Разрешение на запуск**» нажать кнопку «**Добавить**» и добавить группу «**Users OPC**». Для этой группы поставить галочки «**Разрешить**» для всех вариантов запуска и активации (рисунок 5.22).

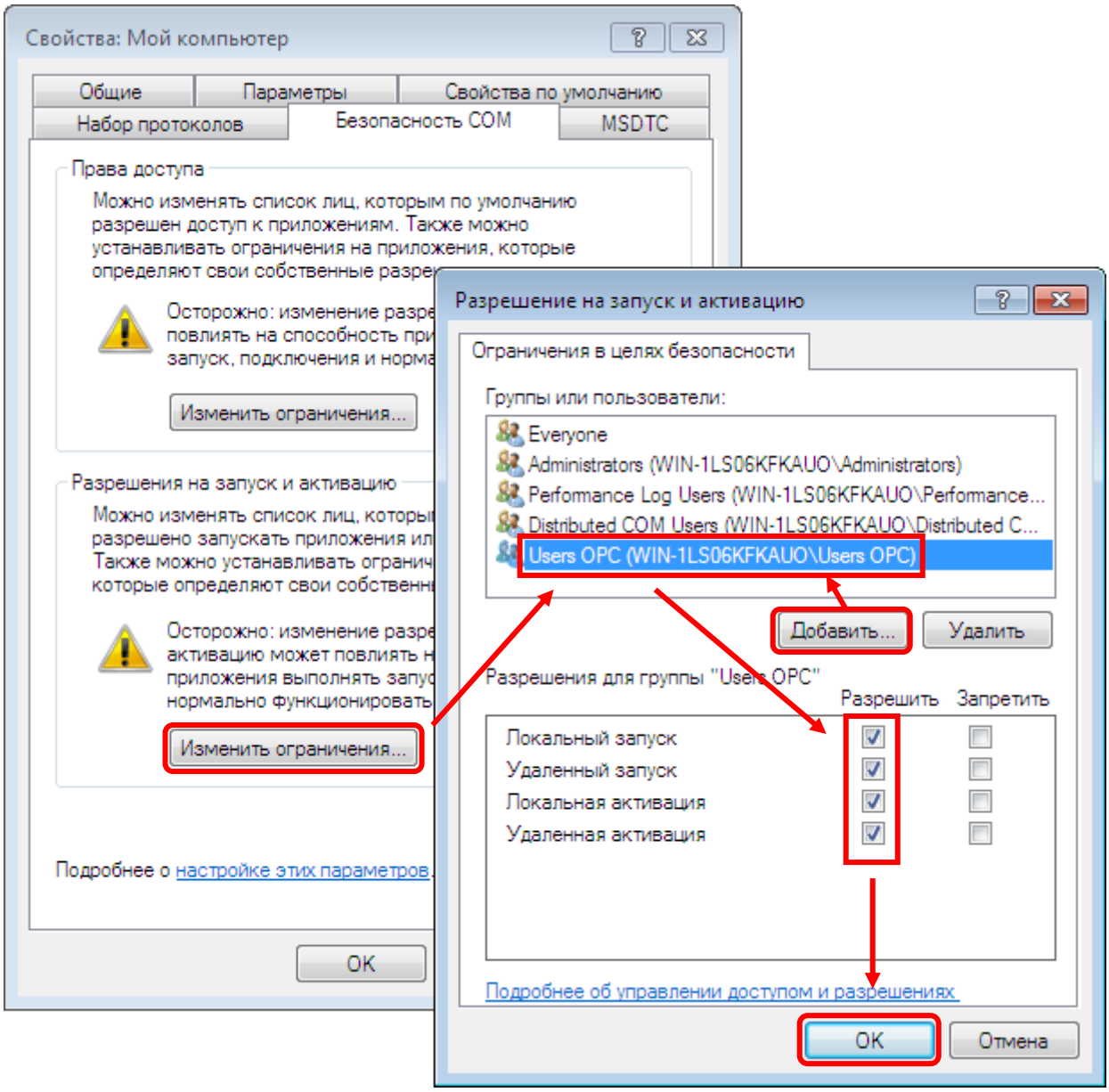

Рисунок 5.22 - Окно настройки «Разрешение на запуск»

Кнопка «**Изменить ограничения…**» может быть не доступна, если была изменена политика «**DCOM: Ограничения компьютера на запуск в синтаксисе SDDL**» («Security Descriptor Definition Language»). В этом случае пропустите текущий шаг.

Если Пользователи группы должны получить только удаленный доступ к OPC-серверу, следует поставить галочки «**Разрешить**» только для пунктов «**Удаленный запуск**» и «**Удаленная активация**».

6 Остальные общие параметры DCOM могут остаться по умолчанию. Если они были изменены, и это нарушило работу OPC-серверов, верните их в прежнее состояние. Список параметров по умолчанию приведен ниже:

- Вкладка **«Свойства по умолчанию»** (рисунок 5.23)

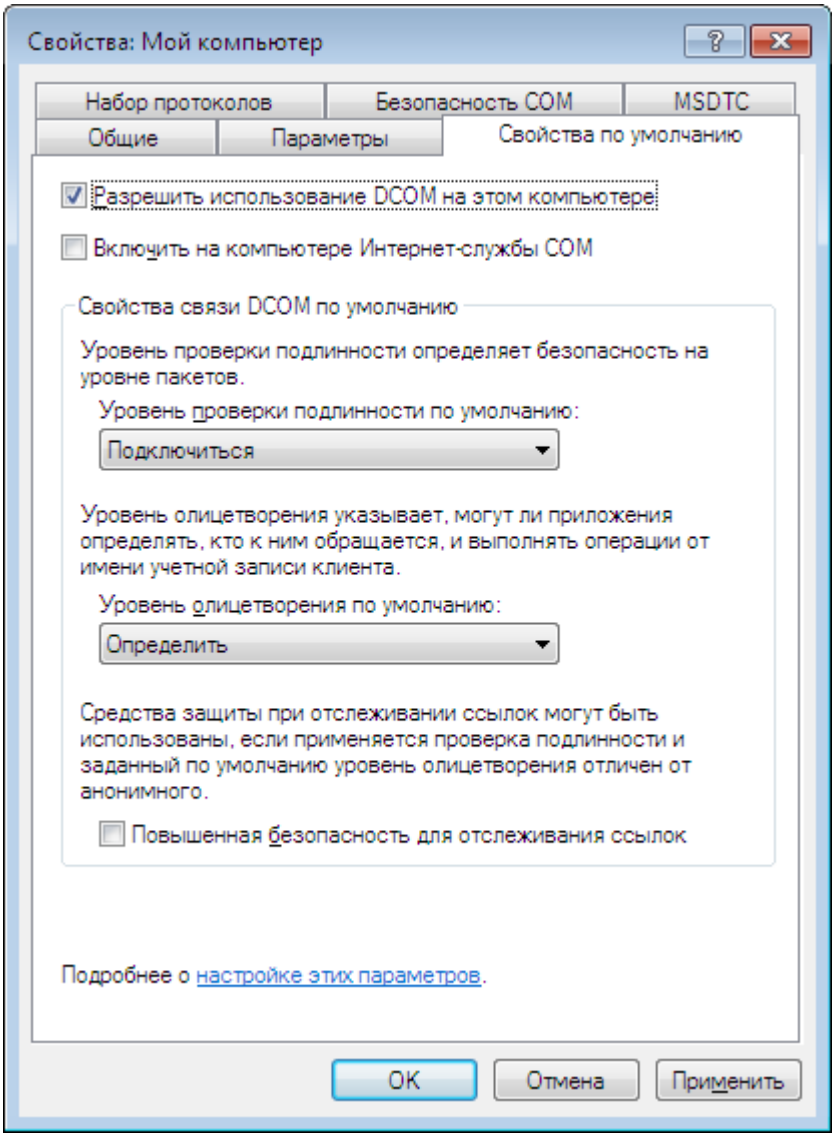

Рисунок 5.23 — Свойства компьютера, закладка «Свойства по умолчанию»

Значения по умолчанию:

- Установлена галочка «**Разрешить использование DCOM на этом компьютере**».
- «Уровень проверки подлинности по умолчанию» – «**Подключение**».
- «Уровень олицетворения по умолчанию» – «**Идентификация**».
- Снята галочка «**Повышенная безопасность для отслеживания ссылок**».

- Вкладка «**Протоколы по умолчанию**» (рисунок 5.24)

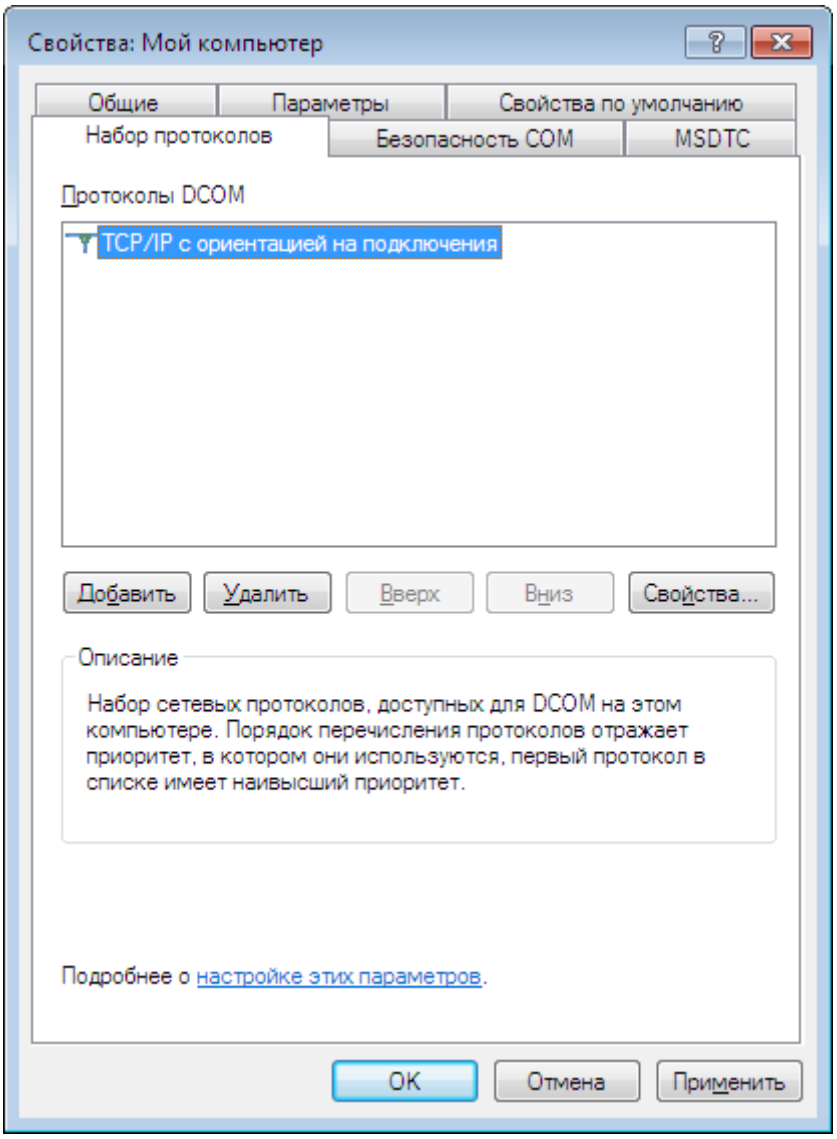

Рисунок 5.24 - Свойства компьютера, закладка «Протоколы по умолчанию»

Добавлены следующие протоколы DCOM:

- «TCP/IP с ориентацией на подключения»
- «SPX с ориентацией на подключения».

- Закладка «**Параметры**» (рисунок 5.25)

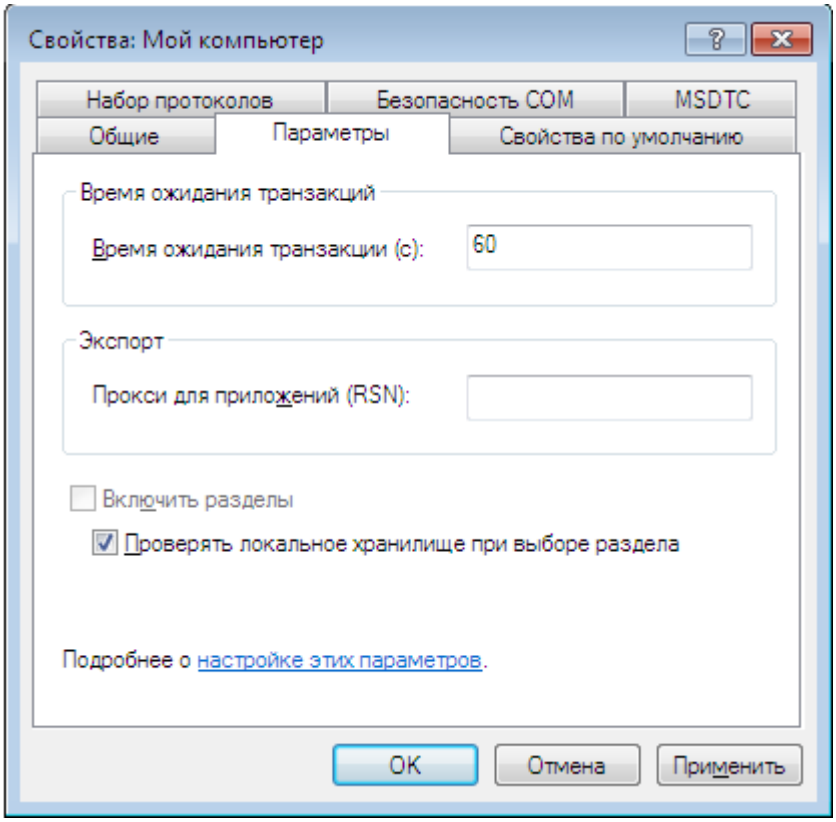

Рисунок 5.25 - Свойства компьютера, закладка «Параметры»

Значения по умолчанию:

- Установлена галочка «**Проверять локальное хранилище при выборе раздела**».
- «Время ожидания транзакции (с)»: **60**.

  При работе в компьютерной сети в случае возникновения обрывов, переполнения и других критических ситуациях при попытках восстановления связи DCOM-приложения используют время ожидания транзакции (Transaction timeout). Это время, в течение которого DCOM-приложение посылает запрос к источнику данных и ожидает восстановления связи. DCOM-приложение совершает до 6 таких попыток, прежде чем подаст сигнал об ошибке в сети.

  По умолчанию этот интервал равен 60 секундам. Соответственно, максимальное время, за которое DCOM-приложение определит, что сеть неисправна – 60*6 = 360 секунд или 6 минут.

Однако это время не всегда может устроить Пользователей DCOM-приложения. Очевидно, что чем короче время ожидания транзакции, тем быстрее DCOM-приложение сможет сообщить Пользователю об ошибке в сети. Поэтому, если Пользователь DCOM-приложения хочет сократить время определения ошибки в сети, он может уменьшить время ожидания транзакции.

ВНИМАНИЕ!!!

Времени ожидания транзакции настраивается на компьютере сервера. При изменении времени ожидания транзакции следует понимать, что это коснется ВСЕХ DCOM-приложений, работающих на этом компьютере. Поэтому, если нет сильной необходимости изменить значение по умолчанию для этого пункта, то изменять его не рекомендуется.

5.2.3 Настройка параметров DCOM для OPC-сервера

Внимание!!!

Настройки, описанные в этом пункте, производятся на компьютере, где установлен OPC-сервер.

Для того чтобы настроить параметры DCOM для конкретного OPC-сервера, следует:

1. В утилите «**Службы компонентов**» выбрать раздел «**Корень консоли / Службы компонентов / Компьютеры / Мой компьютер / Настройка DCOM**» («Console Root / Component Services / Computers / My Computer / DCOM Config»).

2. Открыть контекстное меню нужного OPC-сервера (рисунок 5.26) и выбрать пункт «**Свойства**» («Properties»).

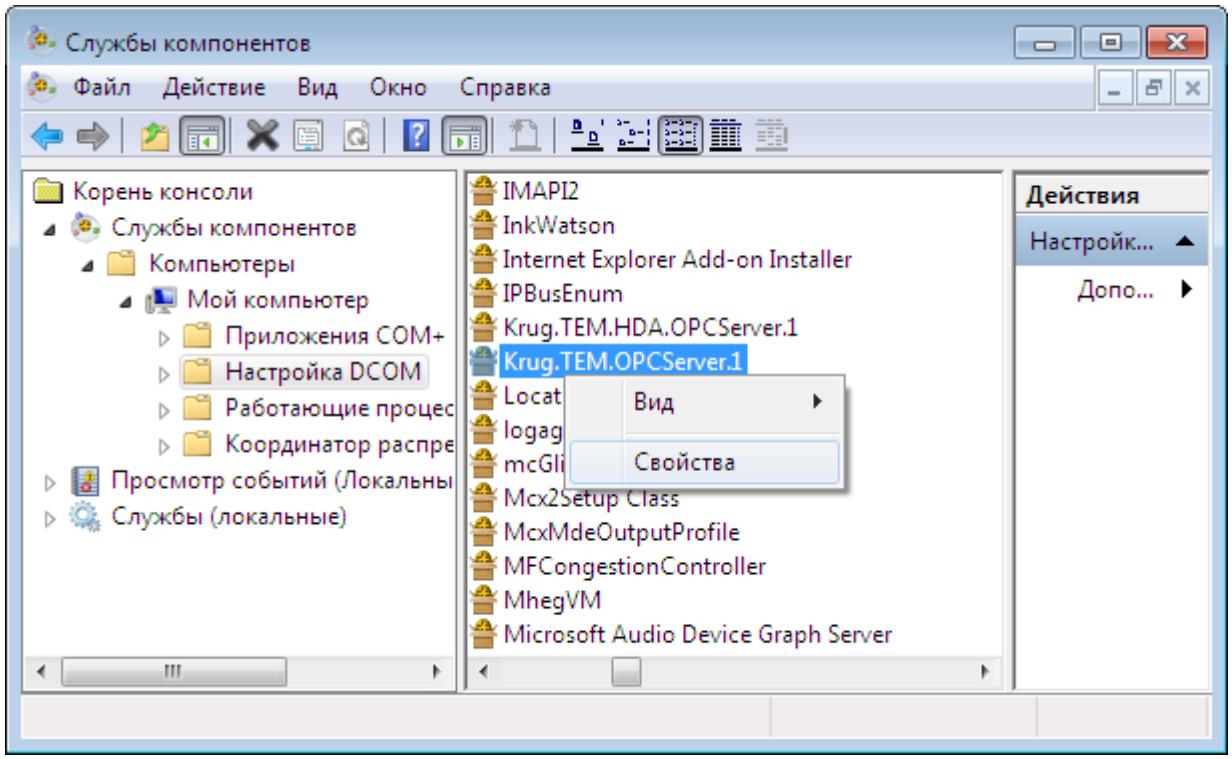

Рисунок 5.26 - Выбор свойств OPC-сервера

3 В открывшемся окне «**Свойства:**…» перейти на вкладку «**Безопасность**» («Security»).

4 В секции «**Разрешения на запуск и активацию**» выбрать «**Настроить**» и нажать на кнопку «**Изменить…**». В открывшемся окне «**Разрешение на запуск**» (рисунок 5.27) нажать кнопку «**Добавить**» и добавить группу «**Users OPC**».

Для группы «**Users OPC**» поставить галочки «**Разрешить**» для всех пунктов. Если Пользователи группы должны получить только удаленный доступ к OPC-серверу, поставить галочки «**Разрешить**» только для пунктов «**Удаленный запуск**» и «**Удаленная активация**»

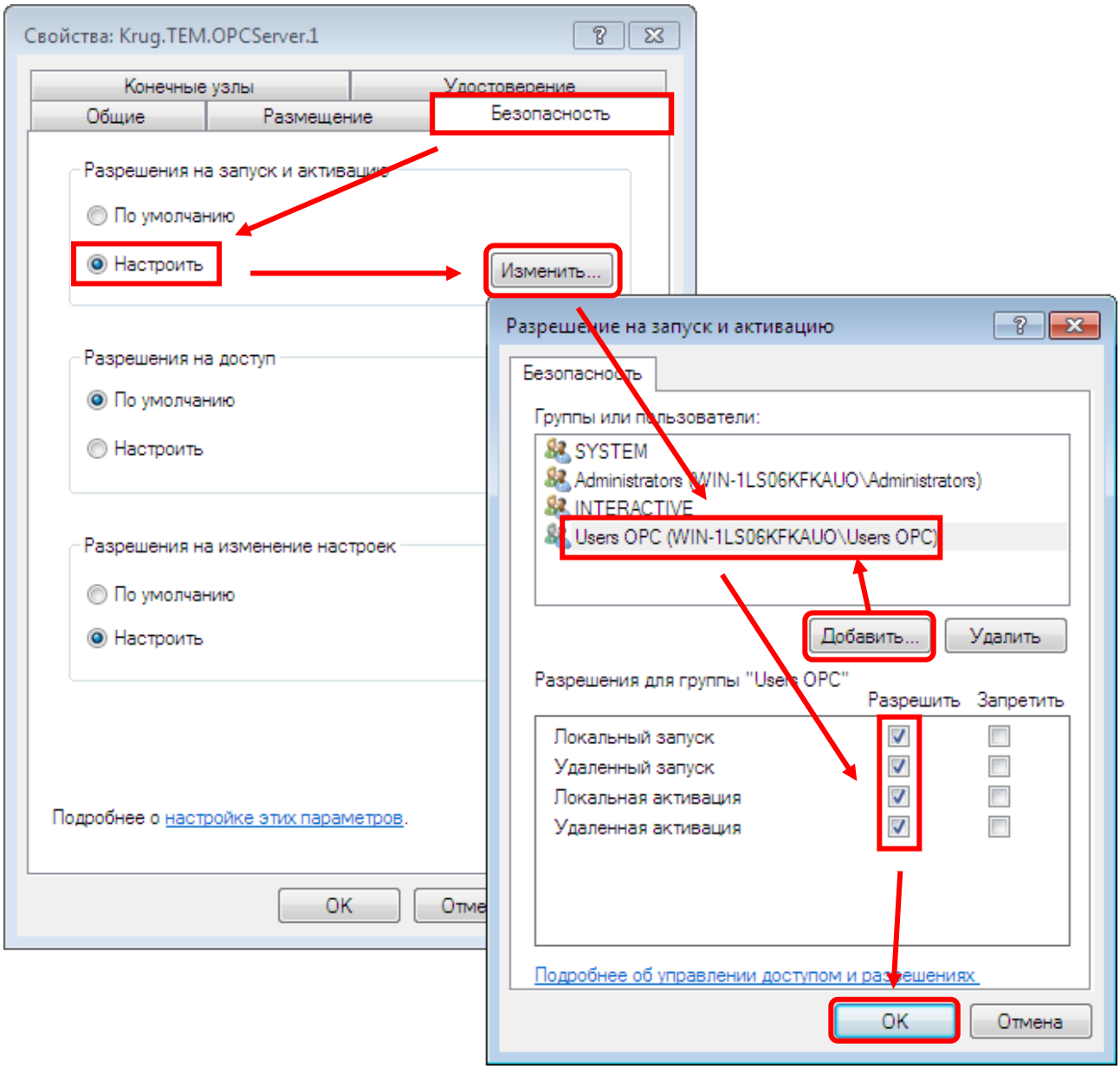

Рисунок 5.27 - Окно настройки «Разрешение на запуск» для OPC-сервера

5 На секции «**Разрешения на доступ**» (вкладка «Безопасность») выбрать «**Настроить**» и нажать на кнопку «**Изменить…**». В открывшемся окне «**Права доступа**» (рисунок 5.28) нажать кнопку «**Добавить**» и добавить группу «**Users OPC**».

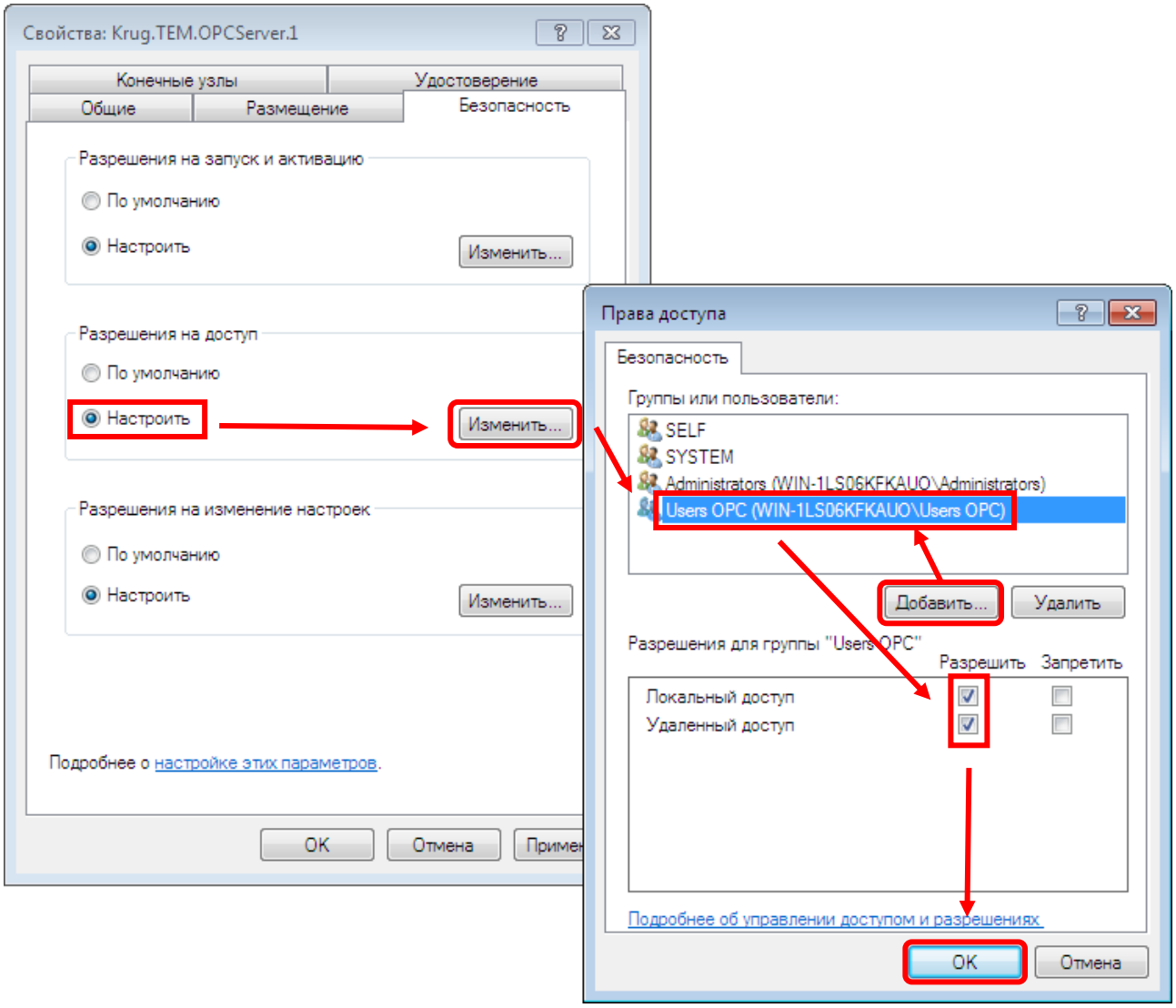

Рисунок 5.28 - Окно настройки «Разрешение на доступ» для OPC-сервера

Для этой группы («**Users OPC**») поставьте галочки «**Разрешить**» для всех вариантов доступа. Если Пользователи группы должны получить только удаленный доступ к OPC-серверу, поставьте галочку «**Разрешить**» только для пункта «**Удаленный доступ**».

6 Для того, чтобы указать под какой учетной записью будет запускаться OPC-сервер, нужно перейти на вкладку «**Удостоверение**» (рисунок 5.29).

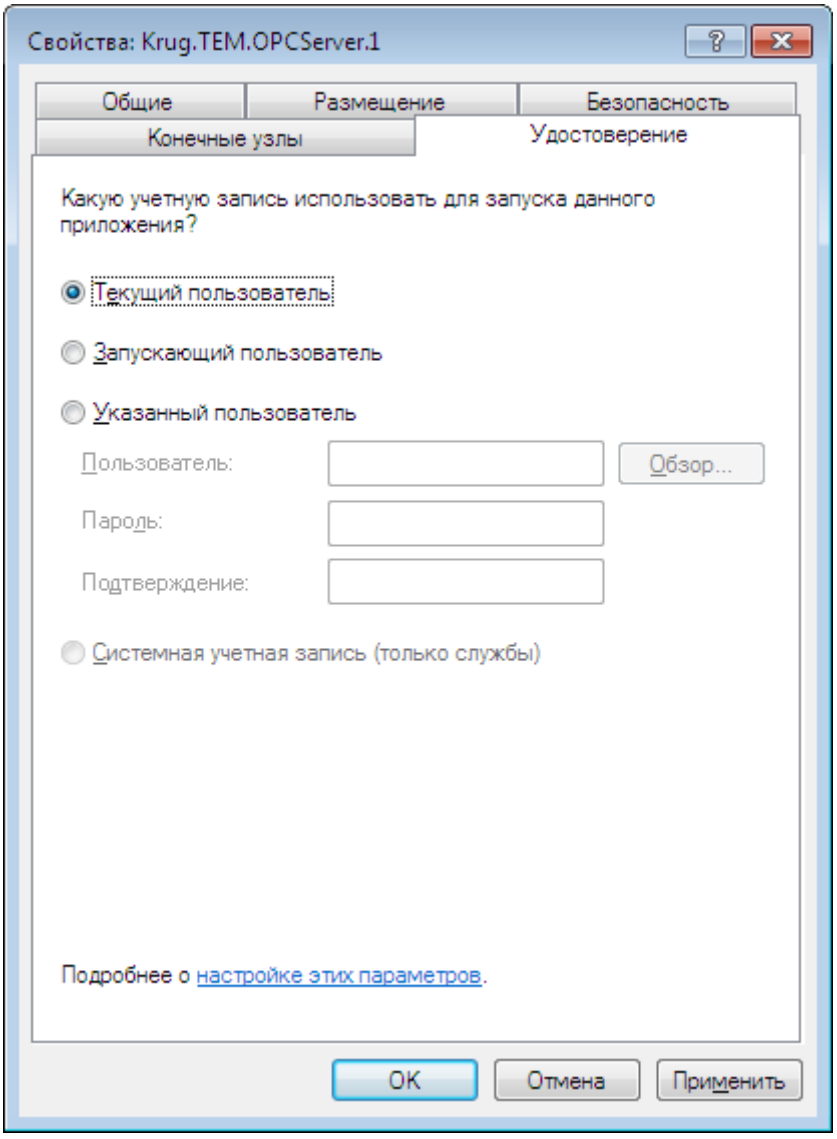

Рисунок 5.29 - Свойства OPC-сервера, закладка «Удостоверение»

Выбор учетной записи для запуска данного приложения зависит от реализации данного OPC-сервера. Следует воспользоваться документацией к OPC-серверу, чтобы выбрать тип Пользователя.

Общие рекомендации по выбору Пользователя для запуска OPC-сервера приведены в таблице 5.1.

7 После выбора Пользователя для запуска OPC-сервера необходимо проверить, есть ли у него доступ к исполняемому файлу OPC-сервера.
Например, если exe-файл OPC-сервера помещен в папку, к которой запрещен доступ учетной записи, используемой для запуска OPC-сервера, тогда при запуске OPC-сервера клиент получит сообщение об ошибке «**Отказ в доступе**».

Чтобы проверить разрешения на доступ к исполняемому файлу OPC-сервера, нужно выполнить следующую последовательность действий:

- Открыть контекстное меню для папки, в которой находится exe-файл OPC-сервера, и выбрать пункт «**Свойства**» («Properties»).
- В открывшемся окне «**Свойства:**…» перейти на вкладку «**Безопасность**» (рисунок 5.30).

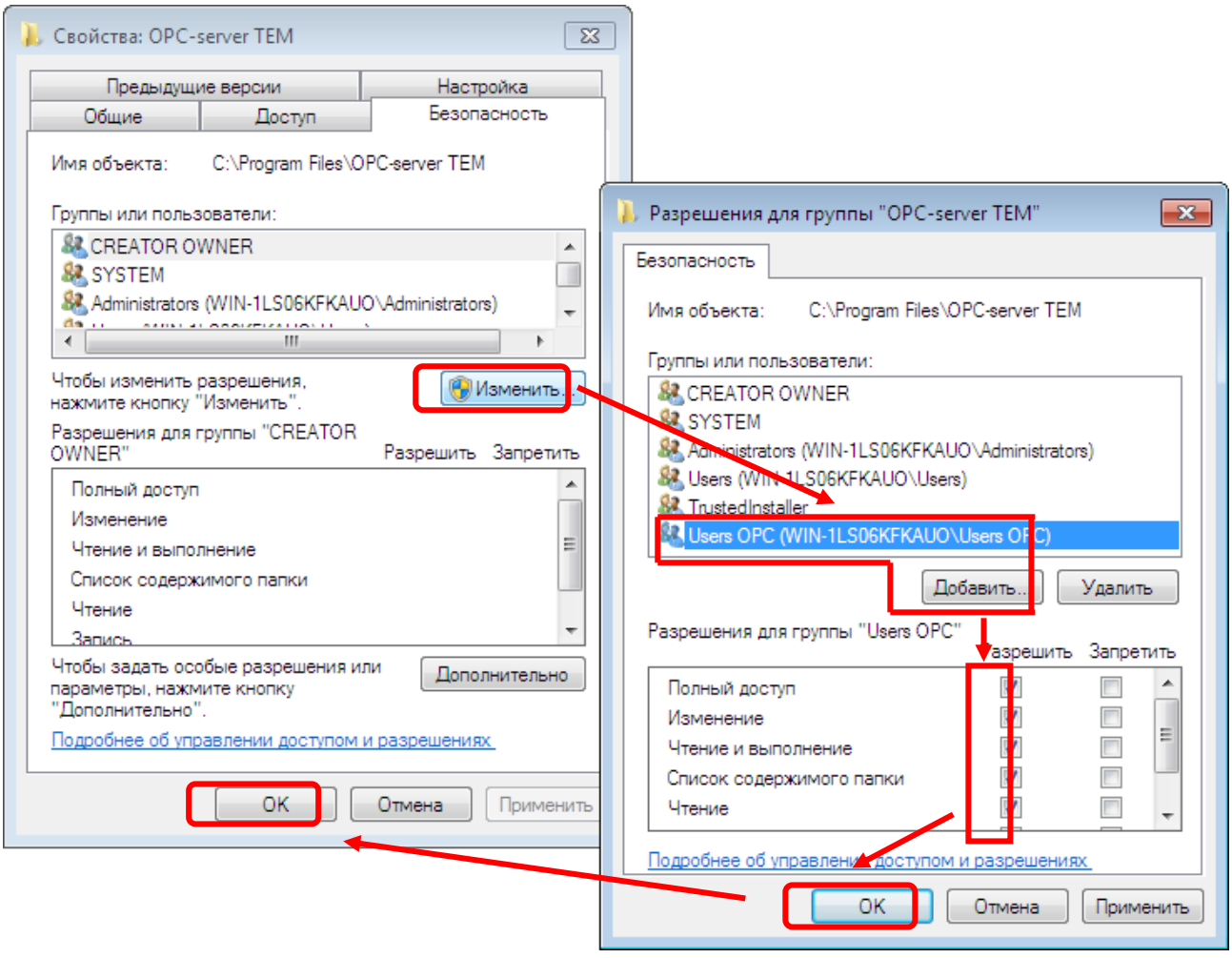

Рисунок 5.30 - Свойства папки, закладка «Безопасность»

- В списке «**Группы или Пользователи**» должен быть Пользователь, который используется для запуска OPC-сервера, или группа, в которую он включен. Если Пользователь отсутствует, нажать кнопку «**Изменить...**», после чего в новом окне нажать кнопку «**Добавить**» и добавить требуемого Пользователя или группу, в которую он включен. Если для выбранного Пользователя не установлен вариант доступа «**Полный доступ**», поставить галочку «**Разрешить**» для этого варианта.
- Нажать кнопку «**OK**» для сохранения сделанных изменений.

8 Для сохранения изменений нажать кнопку «**OK»**.
Чтобы изменения были применены к OPC-серверу, его необходимо перезапустить (если он был запущен ранее).

☝**ВНИМАНИЕ!!!**

Без перезапуска OPC-сервера измененные настройки не будут применены к нему.

Если OPC-сервер не имеет интерфейса Пользователя, с помощью которого он может быть перезапущен, завершить процесс OPC-сервера можно следующей последовательностью действий:

- открыть **Диспетчер задач Windows** и перейти на вкладку «**Процессы**»;
- выбрать процесс настраиваемого OPC-сервера и нажать кнопку «**Завершить процесс**».

После нового подключения OPC-клиента, OPC-сервер будет загружен уже с новыми настройками.

5.2.4 Настройка параметров DCOM для утилиты поиска OPC-серверов

☝**Внимание!!!**

Настройки параметров DCOM для утилиты OPCEnum.exe производятся только на компьютере, где установлены удаленные OPC-серверы.

При доступе к данным удаленного OPC-сервера используется стандартная OPC-утилита **OPCEnum.exe,** которая формирует список доступных OPC–серверов. Для использования этой утилиты необходимо настроить параметры DCOM.

Настройка разрешений осуществляется аналогично настройке OPC-серверов, описанной выше. Отличие заключается в том, что в списке приложений (компонент) необходимо выбирать **OpcEnum** (рисунок 5.31).

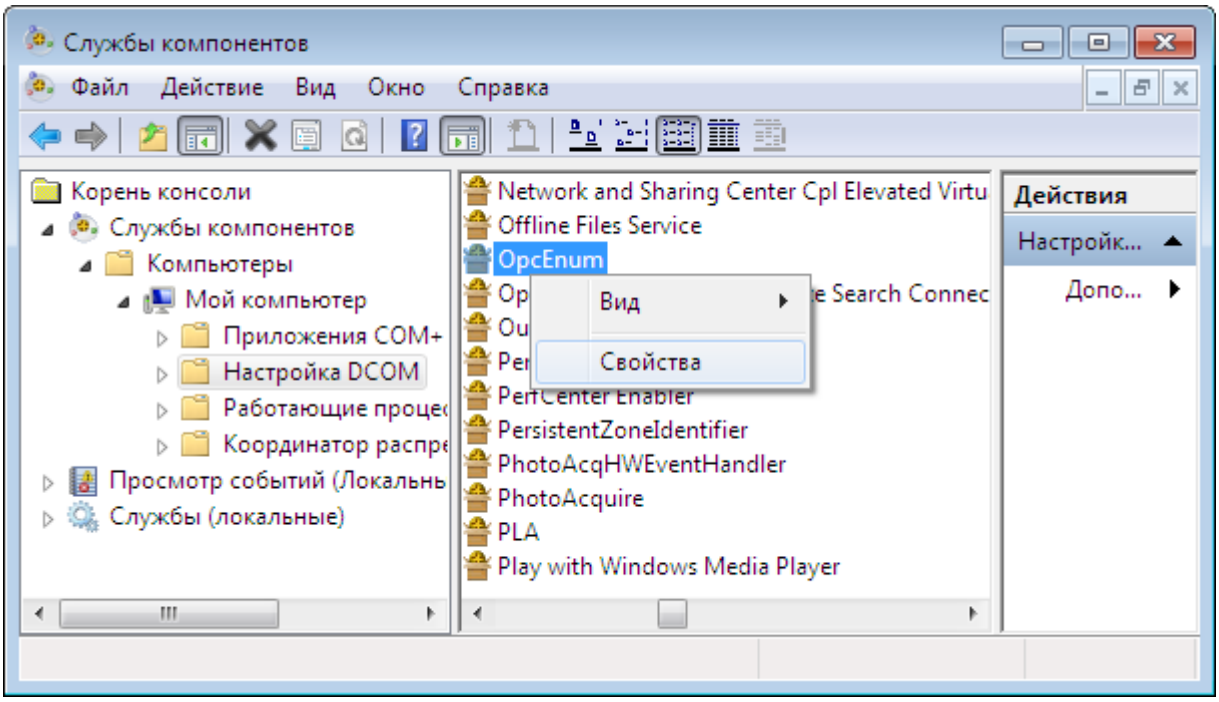

Рисунок 5.31 - Выбор свойств утилиты OPCEnum

5.3 Настройка DCOM для Windows Server 2008, Windows Server 2012

5.3.1 Запуск утилиты настройки DCOM

Для настройки прав доступа к DCOM-приложениям в операционной системе Windows Server 2008 используется утилита «**Службы компонентов»** (Component Services) консоли управления. В зависимости от разрядности операционной системы и приложения OPC-сервера необходимо запускать соответствующую версию этой утилиты:

- Версия Windows 32-х битная - команда "**dcomcnfg**" (рисунок 5.32).
- Версия Windows 64-х битная, исполняемый файл OPC сервера 64-х битный - команда "**dcomcnfg**" (рисунок 5.32).

- Версия Windows 64-х битная, исполняемый файл OPC сервера 32-х битный - команда "**mmc comexp.msc /32**".

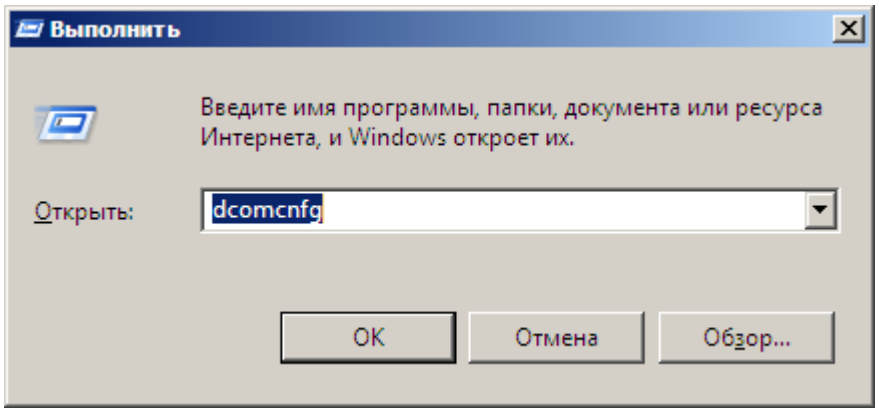

Рисунок 5.32 - Запуск утилиты dcomcnfg

Также утилиту «Службы компонентов» можно запустить из системного меню **«Пуск / Панель управления / Система и безопасность / Администрирование / Службы компонентов»** (рисунок 5.33);

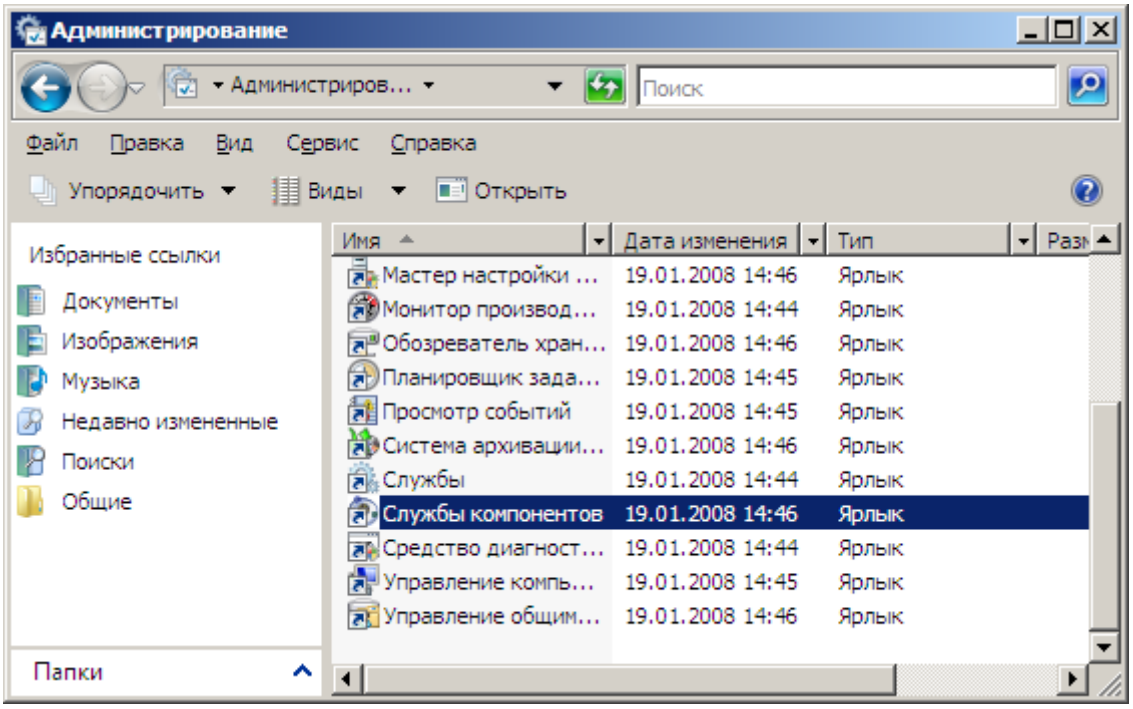

Рисунок 5.33 – Системные инструментальные средства «Службы компонентов»

☝**ВНИМАНИЕ!!!**

После запуска утилиты «Службы компонентов» производится поиск COM-приложений, которые ещё не зарегистрированы в системе на данный момент, и

предлагается зарегистрировать их. Обычно, следует разрешать регистрацию, за исключением случаев, когда иное не указано в документации на программное обеспечение.

После запуска появляется окно «**Службы компонентов**» (рисунок 5.34).

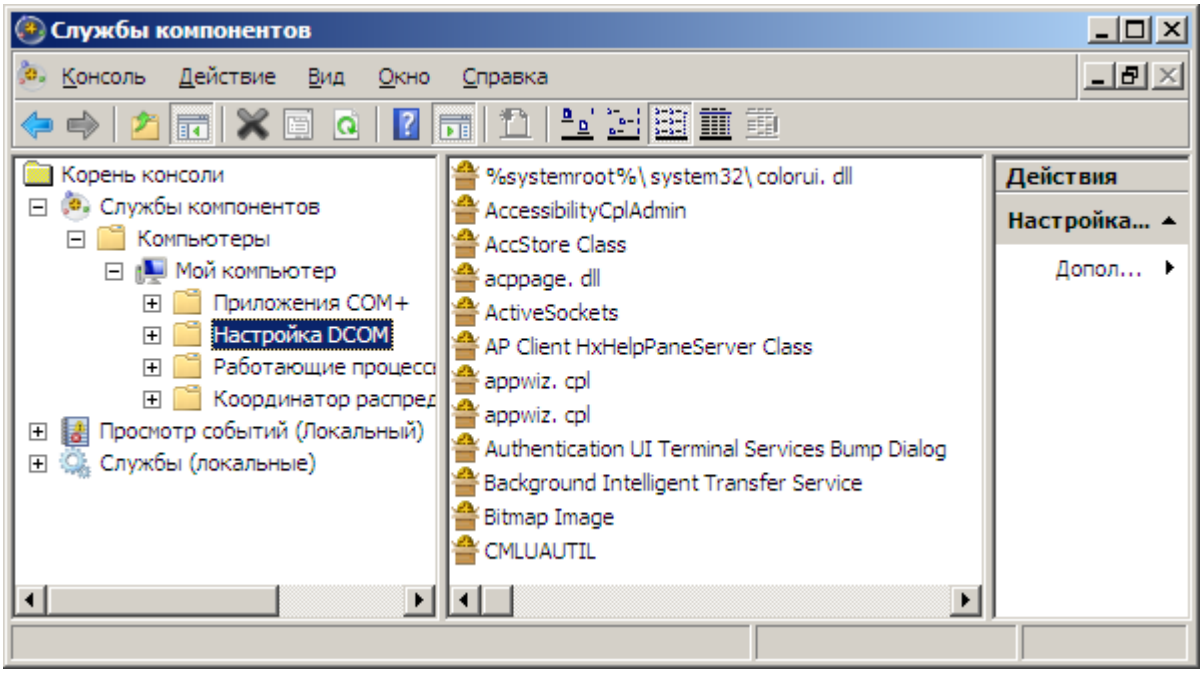

Рисунок 5.34 - Утилита «Службы компонентов»

5.3.2 Настройка общих параметров DCOM

Для установления связи с удаленными OPC-серверами сначала следует настроить общие параметры DCOM.

Для этого следует:

1. Необходимо запустить утилиту «**Службы компонентов**» и выбрать раздел «**Корень консоли / Службы компонентов / Компьютеры**» («Console Root / Component Services / Computers»).

2. Открыть контекстное меню элемента **«Мой компьютер»** («My Computer») и выбрать пункт **«Свойства»** («Properties») – рисунок 5.35.

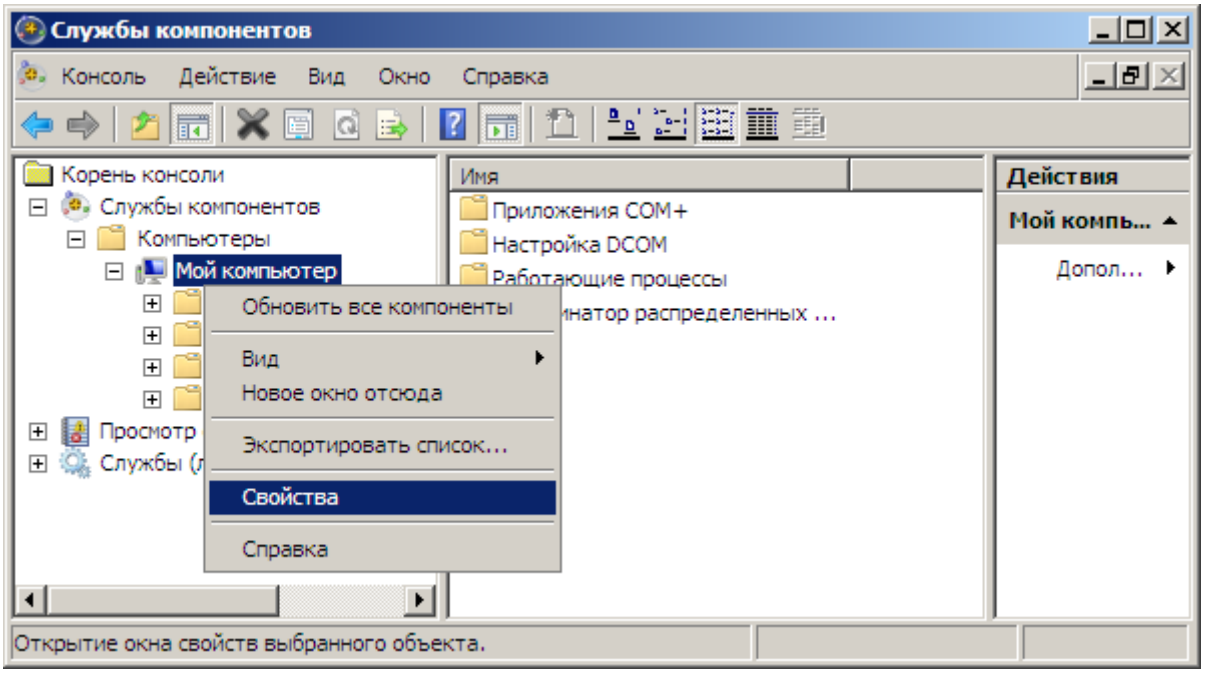

Рисунок 5.35 - Контекстное меню «Мой компьютер»

3 В открывшемся окне «**Свойства: Мой компьютер**» (рисунок 5.36) нужно перейти на закладку «**Безопасность COM**» («COM Security»)

4 Нажать на кнопку «**Изменить ограничения…**» в секции «**Права доступа**». В открывшемся окне «**Разрешение на доступ**» для группы «**АНОНИМНЫЙ ВХОД**» («ANONYMOUS LOGON») установите галочки «**Разрешить**» для пунктов «**Локальный доступ**» и «**Удаленный доступ**» (рисунок 5.36).

Кнопка «**Изменить ограничения…**» может быть не доступна, если была изменена политика «**DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)**». В этом случае можно пропустить текущий шаг.

Эти настройки необходимы для функционирования утилиты поиска OPC-серверов (**OPCEnum.exe**) и некоторых OPC-серверов, для которых «**Уровень проверки подлинности**» («Authentication Level») установлен «**Нет**» («None»).

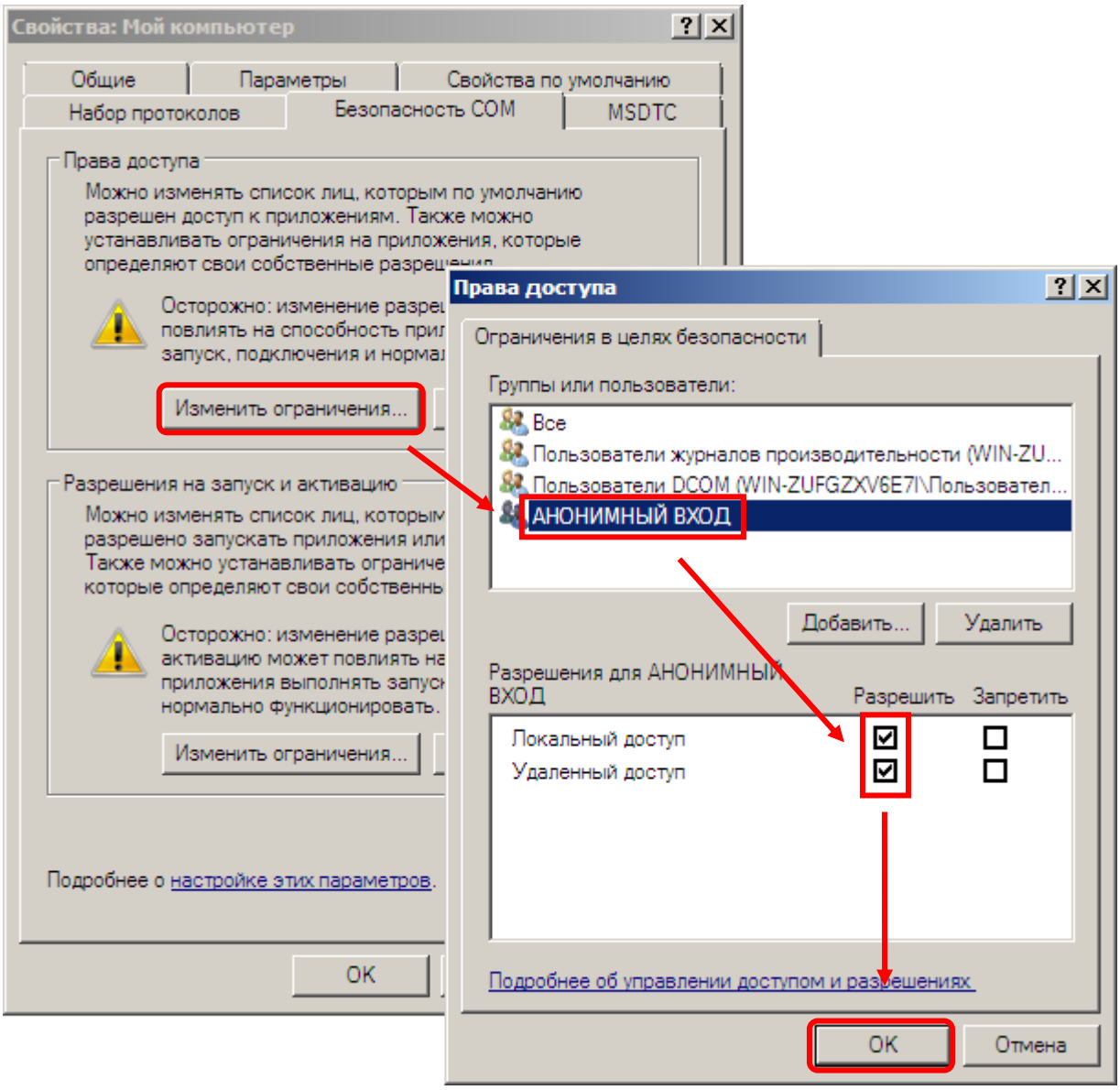

Рисунок 5.36 - Свойства компьютера, закладка «Безопасность COM»

ВНИМАНИЕ!!!

Этот шаг настройки необходимо выполнить как на компьютере, где установлен OPC-сервер, так и на компьютере, где установлен OPC-клиент. Остальные шаги выполняются на компьютере сервера.

5 Нажать на кнопку «**Изменить ограничения…**» в секции «**Разрешения на запуск и активацию**» (рисунок 5.37). В открывшемся окне «**Разрешение на запуск**» нажать кнопку «**Добавить**» и добавить группу «**Users OPC**». Для этой группы поставить галочки «**Разрешить**» для всех вариантов запуска и активации (рисунок 5.37).

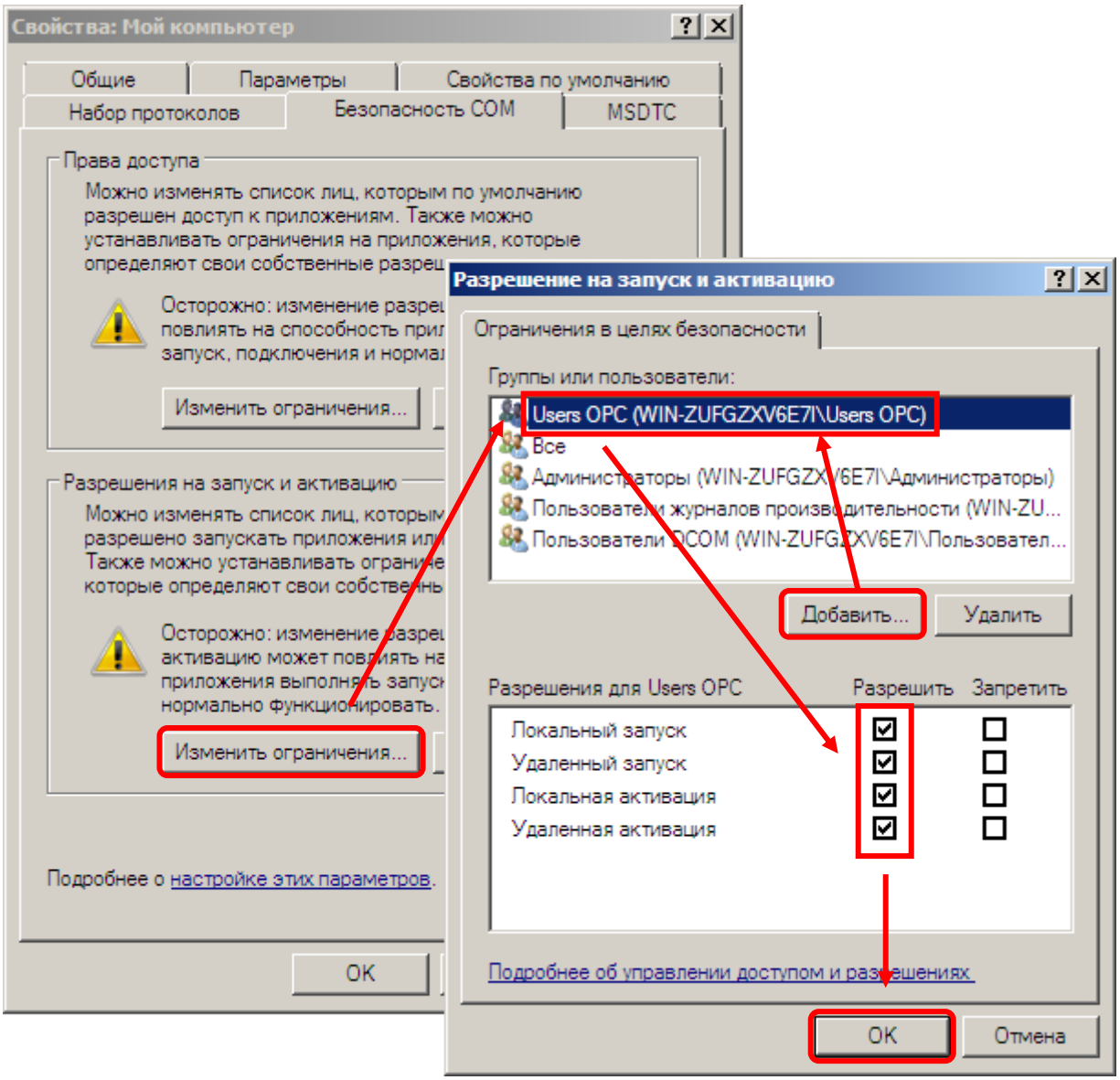

Рисунок 5.37 - Окно настройки «Разрешение на запуск»

Кнопка «**Изменить ограничения…**» может быть не доступна, если была изменена политика «**DCOM: Ограничения компьютера на запуск в синтаксисе SDDL**» («Security Descriptor Definition Language»). В этом случае пропустите текущий шаг.

Если Пользователи группы должны получить только удаленный доступ к OPC-серверу, следует поставить галочки «**Разрешить**» только для пунктов «**Удаленный запуск**» и «**Удаленная активация**».

6 Остальные общие параметры DCOM могут остаться по умолчанию. Если они были изменены, и это нарушило работу OPC-серверов, верните их в прежнее состояние. Список параметров по умолчанию приведен ниже:

- Вкладка **«Свойства по умолчанию»** (рисунок 5.38)

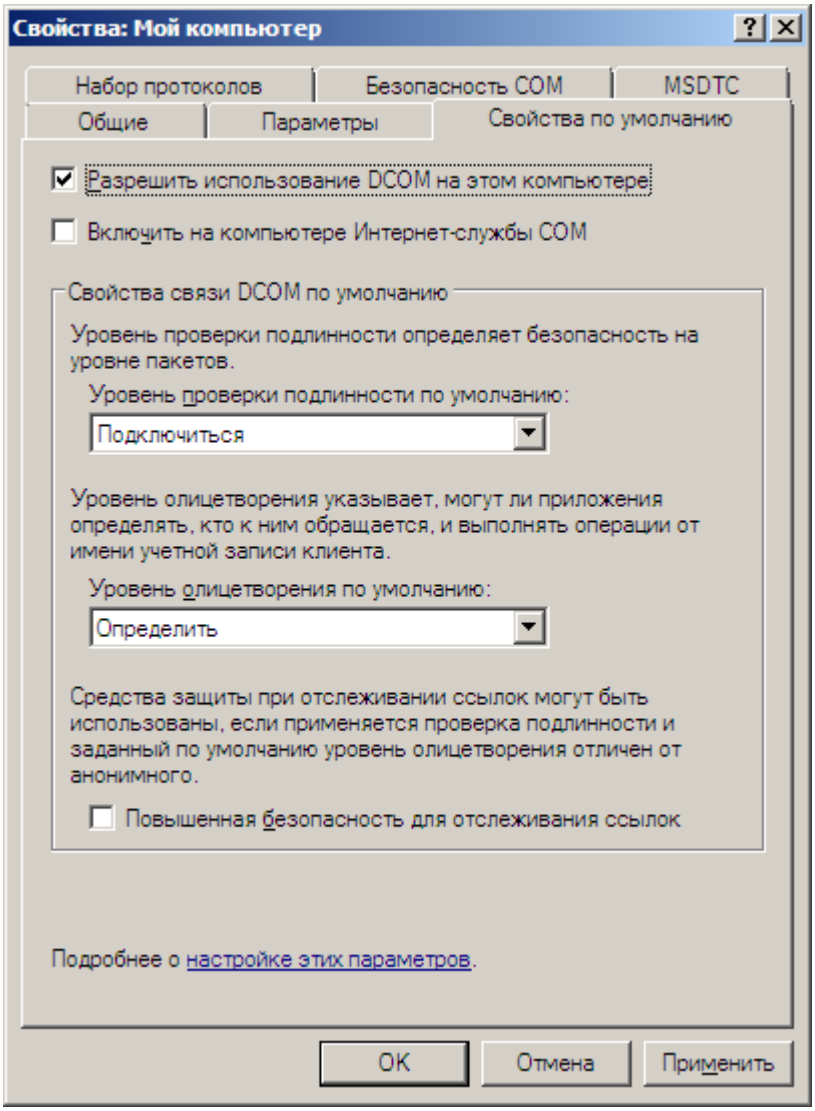

Рисунок 5.38 — Свойства компьютера, закладка «Свойства по умолчанию»

Значения по умолчанию:

- Установлена галочка «**Разрешить использование DCOM на этом компьютере**».
- «Уровень проверки подлинности по умолчанию» – «**Подключение**».
- «Уровень олицетворения по умолчанию» – «**Идентификация**».
- Снята галочка «**Повышенная безопасность для отслеживания ссылок**».

- Вкладка «Протоколы по умолчанию» (рисунок 5.39)

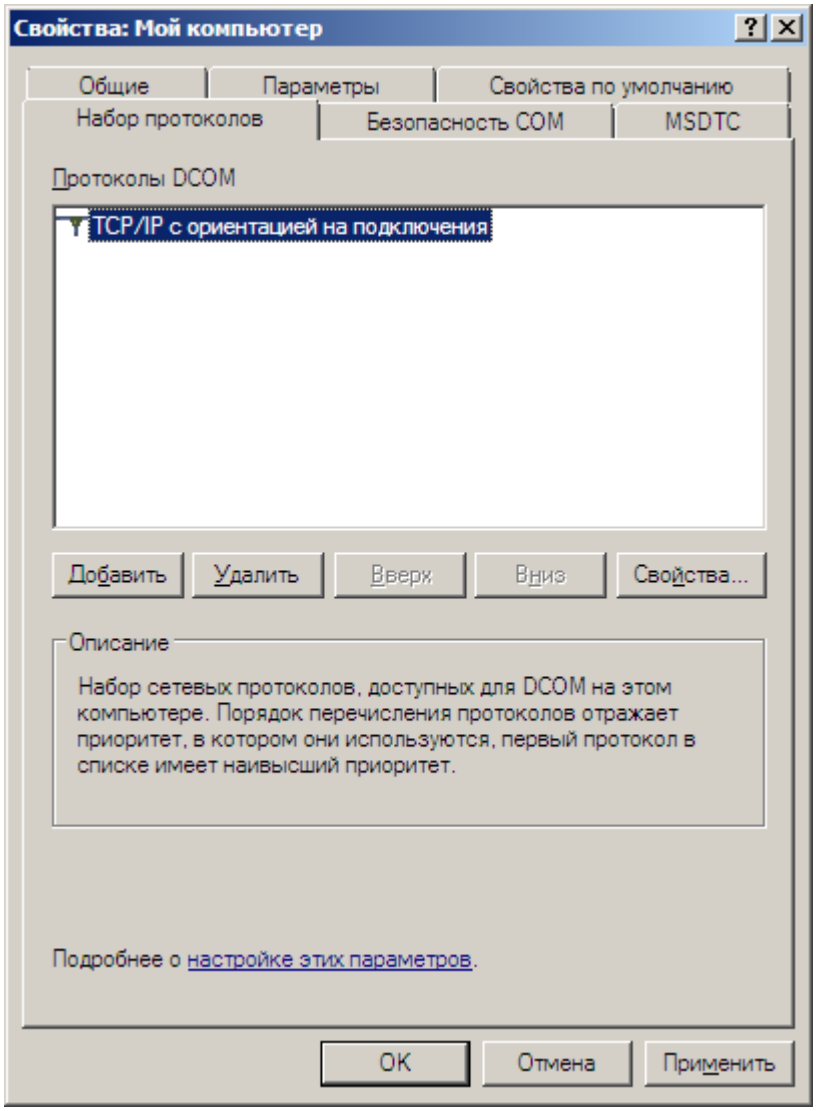

Рисунок 5.39 - Свойства компьютера, закладка «Протоколы по умолчанию»

Добавлены следующие протоколы DCOM:

- «TCP/IP с ориентацией на подключения»

- Закладка «**Параметры**» (рисунок 5.40)

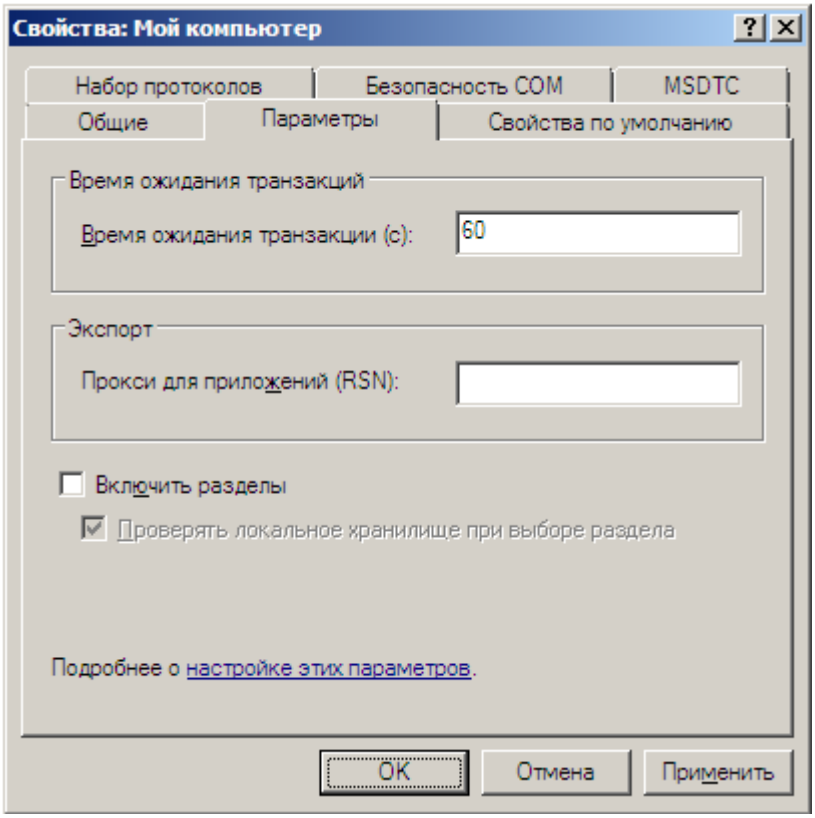

Рисунок 5.40 - Свойства компьютера, закладка «Параметры»

Значения по умолчанию:

- Установлена галочка «**Проверять локальное хранилище при выборе раздела**».
- «Время ожидания транзакции (с)»: **60**.

  При работе в компьютерной сети в случае возникновения обрывов, переполнения и других критических ситуациях при попытках восстановления связи DCOM-приложения используют время ожидания транзакции (Transaction timeout). Это время, в течение которого DCOM-приложение посылает запрос к источнику данных и ожидает восстановления связи. DCOM-приложение совершает до 6 таких попыток, прежде чем подаст сигнал об ошибке в сети.

  По умолчанию этот интервал равен 60 секундам. Соответственно, максимальное время, за которое DCOM-приложение определит, что сеть неисправна – 60*6 = 360 секунд или 6 минут.

Однако это время не всегда может устроить Пользователей DCOM-приложения. Очевидно, что чем короче время ожидания транзакции, тем быстрее DCOM-приложение сможет сообщить Пользователю об ошибке в сети. Поэтому, если Пользователь DCOM-приложения хочет сократить время определения ошибки в сети, он может уменьшить время ожидания транзакции.

ВНИМАНИЕ !!!

Времени ожидания транзакции настраивается на компьютере сервера. При изменении времени ожидания транзакции следует понимать, что это коснется ВСЕХ DCOM-приложений, работающих на этом компьютере. Поэтому, если нет сильной необходимости изменить значение по умолчанию для этого пункта, то изменять его не рекомендуется.

5.3.3 Настройка параметров DCOM для OPC-сервера

Внимание!!!

Настройки, описанные в этом пункте, производятся на компьютере, где установлен OPC-сервер.

Для того чтобы настроить параметры DCOM для конкретного OPC-сервера, следует:

1. В утилите «**Службы компонентов**» выбрать раздел «**Корень консоли / Службы компонентов / Компьютеры / Мой компьютер / Настройка DCOM**» («Console Root / Component Services / Computers / My Computer / DCOM Config»).

2. Открыть контекстное меню нужного OPC-сервера (рисунок 5.41) и выбрать пункт «**Свойства**» («Properties»).

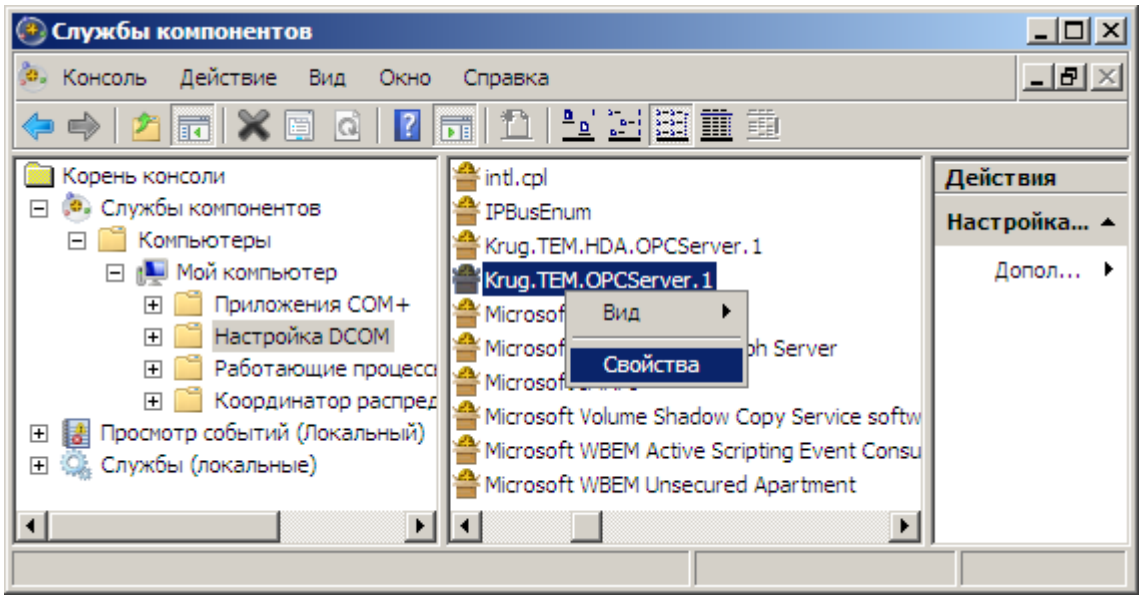

Рисунок 5.41 - Выбор свойств OPC-сервера

3 В открывшемся окне «**Свойства:**…» перейти на вкладку «**Безопасность**» («Security»).

4 В секции «**Разрешения на запуск и активацию**» выбрать «**Настроить**» и нажать на кнопку «**Изменить…**». В открывшемся окне «**Разрешение на запуск**» (рисунок 5.42) нажать кнопку «**Добавить**» и добавить группу «**Users OPC**».

Для группы «**Users OPC**» поставить галочки «**Разрешить**» для всех пунктов. Если Пользователи группы должны получить только удаленный доступ к OPC-серверу, поставить галочки «**Разрешить**» только для пунктов «**Удаленный запуск**» и «**Удаленная активация**»

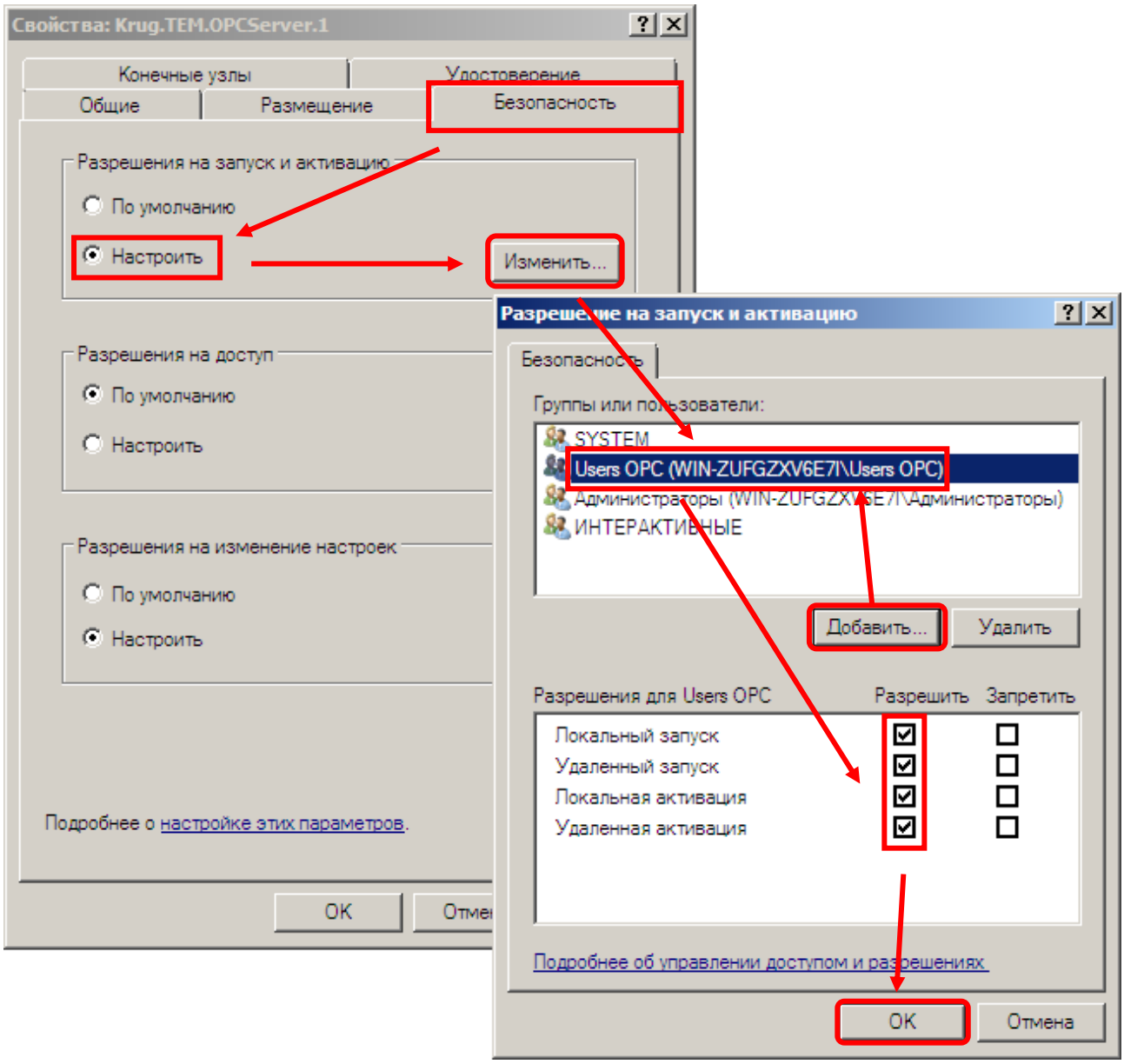

Рисунок 5.42 - Окно настройки «Разрешение на запуск» для OPC-сервера

5 На секции «**Разрешения на доступ**» (вкладка «Безопасность») выбрать «**Настроить**» и нажать на кнопку «**Изменить…**». В открывшемся окне «**Права доступа**» (рисунок 5.43) нажать кнопку «**Добавить**» и добавить группу «**Users OPC**».

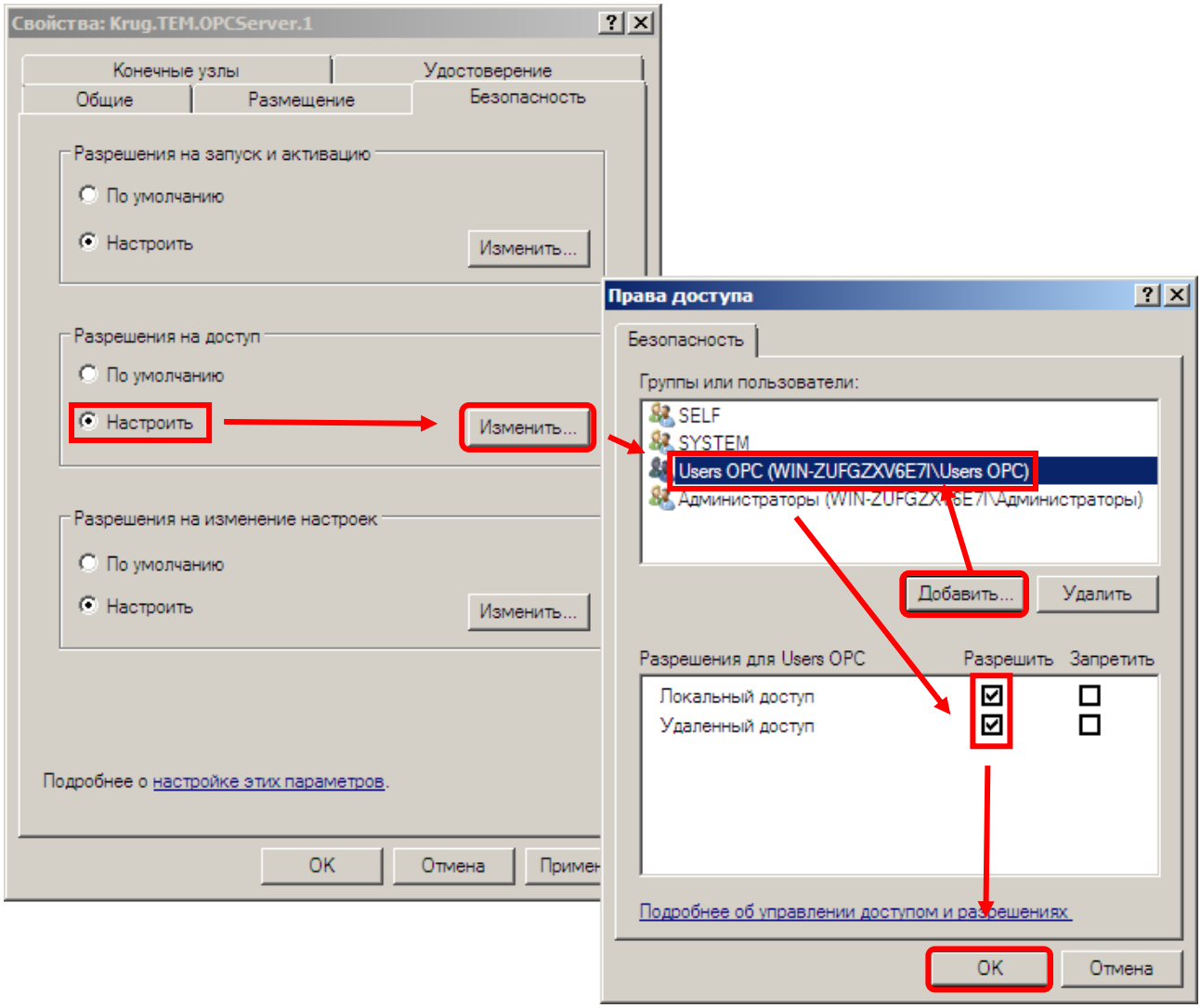

Рисунок 5.43 - Окно настройки «Разрешение на доступ» для OPC-сервера

Для этой группы («**Users OPC**») поставьте галочки «**Разрешить**» для всех вариантов доступа. Если Пользователи группы должны получить только удаленный доступ к OPC-серверу, поставьте галочку «**Разрешить**» только для пункта «**Удаленный доступ**».

6 Для того, чтобы указать под какой учетной записью будет запускаться OPC-сервер, нужно перейти на вкладку «**Удостоверение**» (рисунок 5.44).

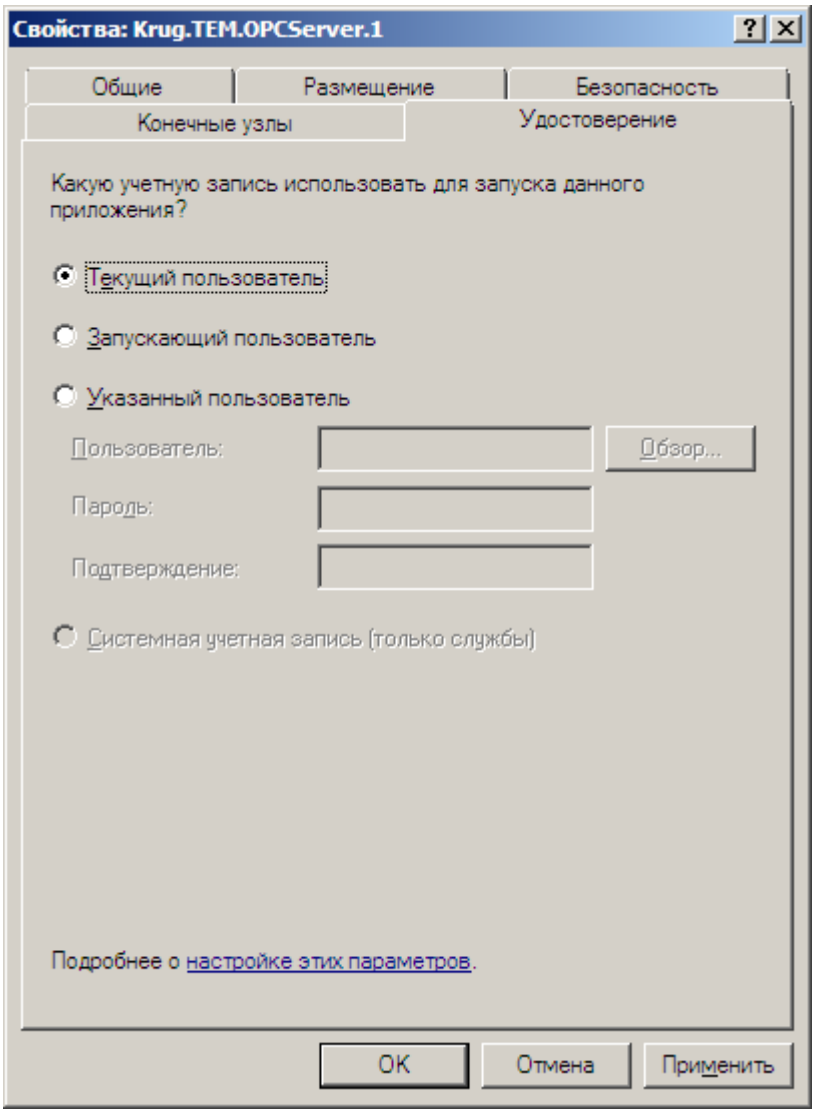

Рисунок 5.44 - Свойства OPC-сервера, закладка «Удостоверение»

Выбор учетной записи для запуска данного приложения зависит от реализации данного OPC-сервера. Следует воспользоваться документацией к OPC-серверу, чтобы выбрать тип Пользователя.

Общие рекомендации по выбору Пользователя для запуска OPC-сервера приведены в таблице 5.1.

7 После выбора Пользователя для запуска OPC-сервера необходимо проверить, есть ли у него доступ к исполняемому файлу OPC-сервера.
Например, если exe-файл OPC-сервера помещен в папку, к которой запрещен доступ учетной записи, используемой для запуска OPC-сервера, тогда при запуске OPC-сервера клиент получит сообщение об ошибке «**Отказ в доступе**».

Чтобы проверить разрешения на доступ к исполняемому файлу OPC-сервера, нужно выполнить следующую последовательность действий:

- Открыть контекстное меню для папки, в которой находится exe-файл OPC-сервера, и выбрать пункт «**Свойства**» («Properties»).
- В открывшемся окне «**Свойства:**…» перейти на вкладку «**Безопасность**» (рисунок 5.45).

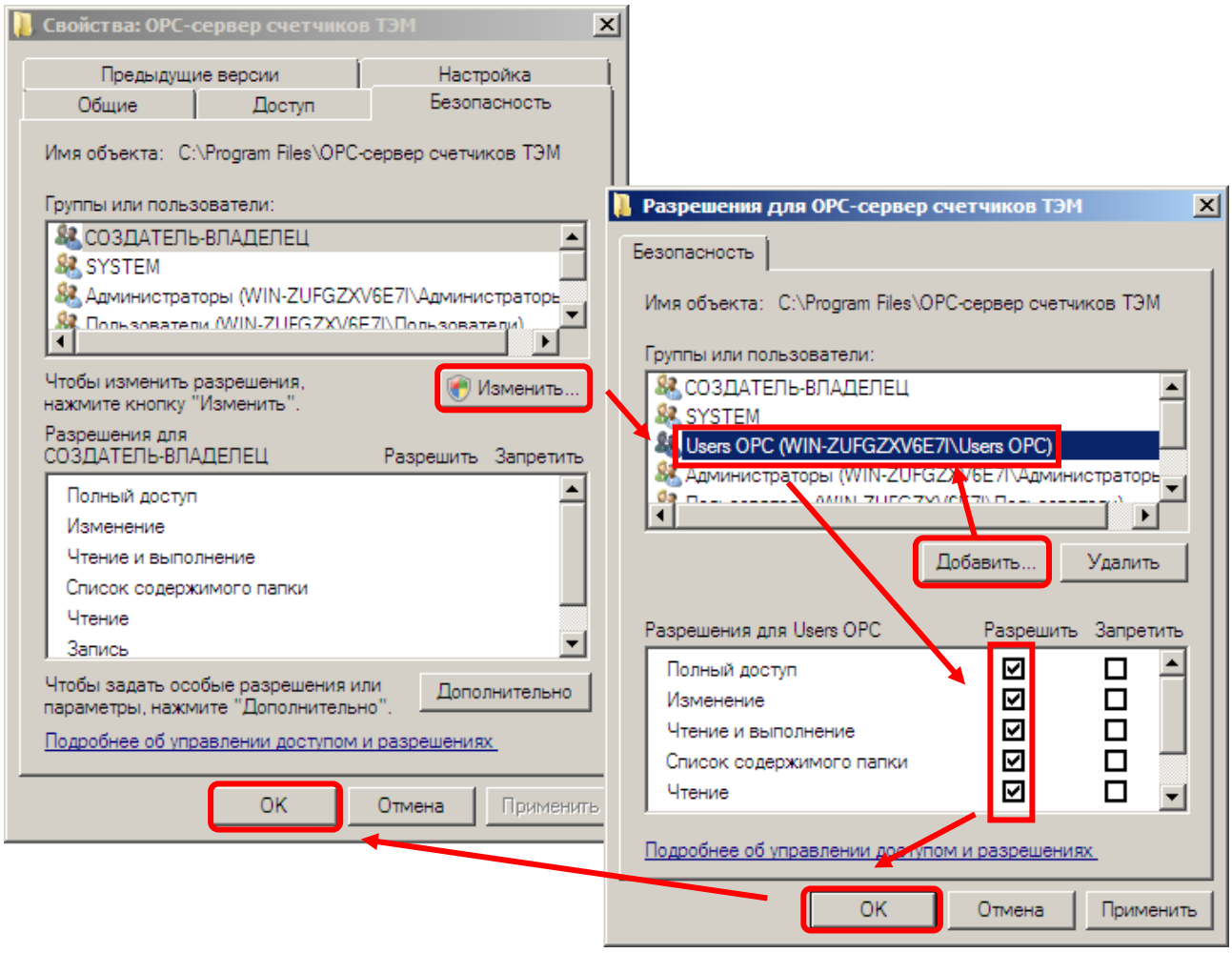

Рисунок 5.45 - Свойства папки, закладка «Безопасность»

- В списке «**Группы или Пользователи**» должен быть Пользователь, который используется для запуска OPC-сервера, или группа, в которую он включен. Если Пользователь отсутствует, нажать кнопку «**Изменить...**», после чего в новом окне нажать кнопку «**Добавить**» и добавить требуемого Пользователя или группу, в которую он включен. Если для выбранного Пользователя не установлен вариант доступа «**Полный доступ**», поставить галочку «**Разрешить**» для этого варианта.
- Нажать кнопку «**OK**» для сохранения сделанных изменений.

8 Для сохранения изменений нажать кнопку «**OK»**.
Чтобы изменения были применены к OPC-серверу, его необходимо перезапустить (если он был запущен ранее).

☝**ВНИМАНИЕ!!!**

Без перезапуска OPC-сервера измененные настройки не будут применены к нему.

Если OPC-сервер не имеет интерфейса Пользователя, с помощью которого он может быть перезапущен, завершить процесс OPC-сервера можно следующей последовательностью действий:

- открыть **Диспетчер задач Windows** и перейти на вкладку «**Процессы**»;
- выбрать процесс настраиваемого OPC-сервера и нажать кнопку «**Завершить процесс**».

После нового подключения OPC-клиента, OPC-сервер будет загружен уже с новыми настройками.

5.3.4 Настройка параметров DCOM для утилиты поиска OPC-серверов

Внимание!!!

Настройки параметров DCOM для утилиты OPCEnum.exe производятся только на компьютере, где установлены удаленные OPC-серверы.

При доступе к данным удаленного OPC-сервера используется стандартная OPC-утилита **OPCEnum.exe,** которая формирует список доступных OPC–серверов. Для использования этой утилиты необходимо настроить параметры DCOM.

Настройка разрешений осуществляется аналогично настройке OPC-серверов, описанной выше. Отличие заключается в том, что в списке приложений (компонент) необходимо выбирать **OpcEnum** (рисунок 5.46).

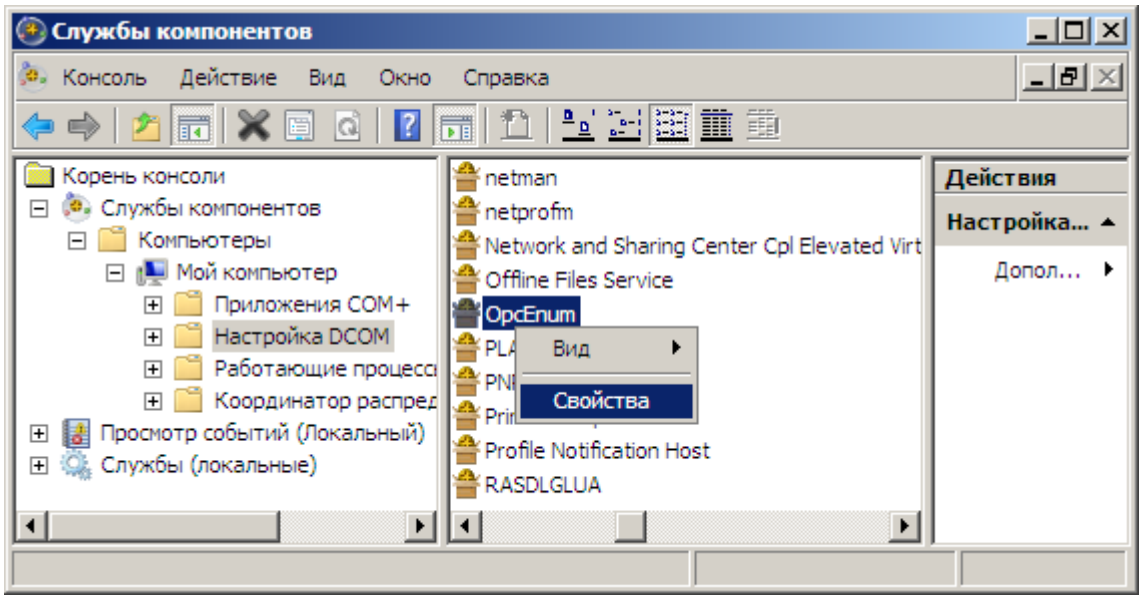

Рисунок 5.46 - Выбор свойств утилиты OPCEnum