Руководство по настройке DCOM

Фирма „ТРЭИ ГМБХ" постоянно совершенствует и развивает свою продукцию. В связи с этим информация, содержащаяся в данном документе, может изменяться без дополнительного предупреждения пользователей.

Россия,
440028, Пенза, ул. Титова, 1Г
Телефон (fax): +7 (8412) 55-58-90, 49-95-39
fax: +7 (8412) 49-85-13
e-mail: trei@trei-gmbh.ru

Содержание

Общие сведения

ПО Unimod Pro имеет в составе несколько (D)COM-серверов, которые могут работать как локально и удалённо. Это TREI plc gate, TREI OPC DA server и TREI OPC HDA server. Настраиваются они абсолютно идентично, поэтому далее будет просто указываться «сервер», что подразумевает любой из вышеперечисленных компонентов.

Настройка DCOM необходима только в случае удалённого использования сервера. Если COM-сервер используется **только** локально, специальной настройки DCOM не требуется.

Вся настройка DCOM заключается в настройке параметров безопасности для сервера и системы в целом. Система защиты ОС Windows® подразумевает, что каждый процесс действует от имени определённого пользователя (пользователей).

В рамках настройки DCOM необходимо обеспечить возможность двунаправленного обмена данными между процессами клиента и сервера, что обеспечивается правами соответствующих учётных записей, от имени которых будут работать процессы клиента и сервера. Здесь возможны два варианта:

- полностью отключить защиту;
- явно регламентировать права отдельных учётных записей и групп.

Первый способ прост, однако неприемлем с точки зрения безопасности всей системы, поскольку полное отключение защиты открывает беспрепятственный доступ в систему любому принципалу.

Второй способ более трудоёмок, однако обеспечивает минимальное вмешательство в работу системы защиты на уровне операционной системы и сетевых взаимодействий.

Данный раздел рассматривает только второй способ – явную настройку

параметров безопасности с использованием отдельных учётных записей пользователей и групп.

Прежде всего, немного теории. Имеем несколько станций, объединённых общей сетью. Посмотрим, что происходит, когда станция А (процесс А) обращается к станции В (процессу В). Процесс А выполняет операцию требующую обращения к ресурсам станции В. Станция А проверяет право процесса А на выполнение этой операции. При наличии прав, выполняется обращение к станции В. Теперь станция В, её система безопасности, проверяет право процесса А на доступ к требуемым ресурсам. При наличии такого права, процесс А получает требуемые ресурсы.

При проверке прав пользователя или группы, система безопасности конкретной станции должна иметь доступ к учётной записи этого пользователя или группы. Возможны два варианта расположения учётных записей:

- *локально*, для каждой станции;
- *удалённо*, на выделенной станции.

В первом случае – локальное расположение учётных записей – каждая станция должна содержать все учётные записи пользователей, которые должны иметь доступ к ресурсам станций.

В случае удалённого расположения учёных записей, одна из станций выступает в качестве хранилища общей БД учётных записей. Все прочие станции обращаются к этой общей БД.

Возможны следующие варианты сетевой конфигурации станций (работающих под управлением ОС Windows®):

a. все станции принадлежат одному домену.
b. станции принадлежат разным доменам;
c. станции принадлежат одной рабочей группе, либо не входят в

общую группу/домен.

В случае (a) можно использовать как локальное, так и удалённое расположение БД учётных записей. Т. е. либо использовать доменные учётные записи, хранящиеся на контроллере домена, БД которого доступна всем станциям домена, либо дублировать учётные записи для каждой станции.

Случай (b) отличается от (a) следующим моментом: между доменами обязательно должны быть установлены двусторонние доверительные отношения. Здесь также можно использовать локальное расположение БД учётных записей (тогда доверительные отношения не нужны).

В случае (c) **каждая** станция должна иметь полный набор учётных записей.

Исходя из вышесказанного, задача сводится к выбору способа хранения учётных записей и соответствующей настройке.

Настройка DCOM

Программа установки Unimod Pro Solution выполняет автоматическую настройку DCOM для всех компонентов, создавая отдельную учётную запись для работы. Если по каким-то причинам не удаётся подключиться к удалённому серверу или автоматическая настройка не прошла успешно, то все нижеописанные действия необходимо выполнить вручную.

Настройка будет производиться на примере ПК под управлением ОС Windos7. На остальных системах семейства Windows NT процедура похожая и все операции почти аналогичны.

Общие настройки для станций клиента и сервера

На данном этапе, прежде всего, следует создать необходимые учётные записи.

> **Примечание:** для работы с учётными записями пользователей и

групп следует использовать стандартные средства, входящие в состав ОС Windows®.

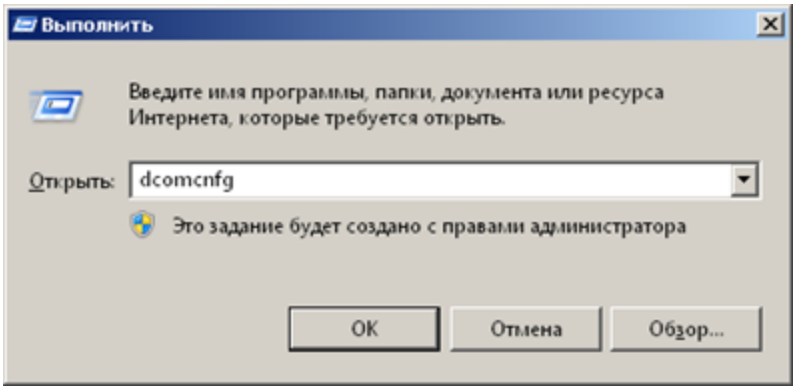
Можно обойтись единственной учётной записью, от имени которой будет работать и COM-сервер и клиенты. Либо можно создать отдельные учётные записи для каждого клиента. В любом случае, для COM-сервера необходимо указать учётную запись.

Примечание: если предполагается доступ к серверу нескольких пользователей (разных учётных записей), имеет смысл создать для них общую группу. Это немного упростит настройку.

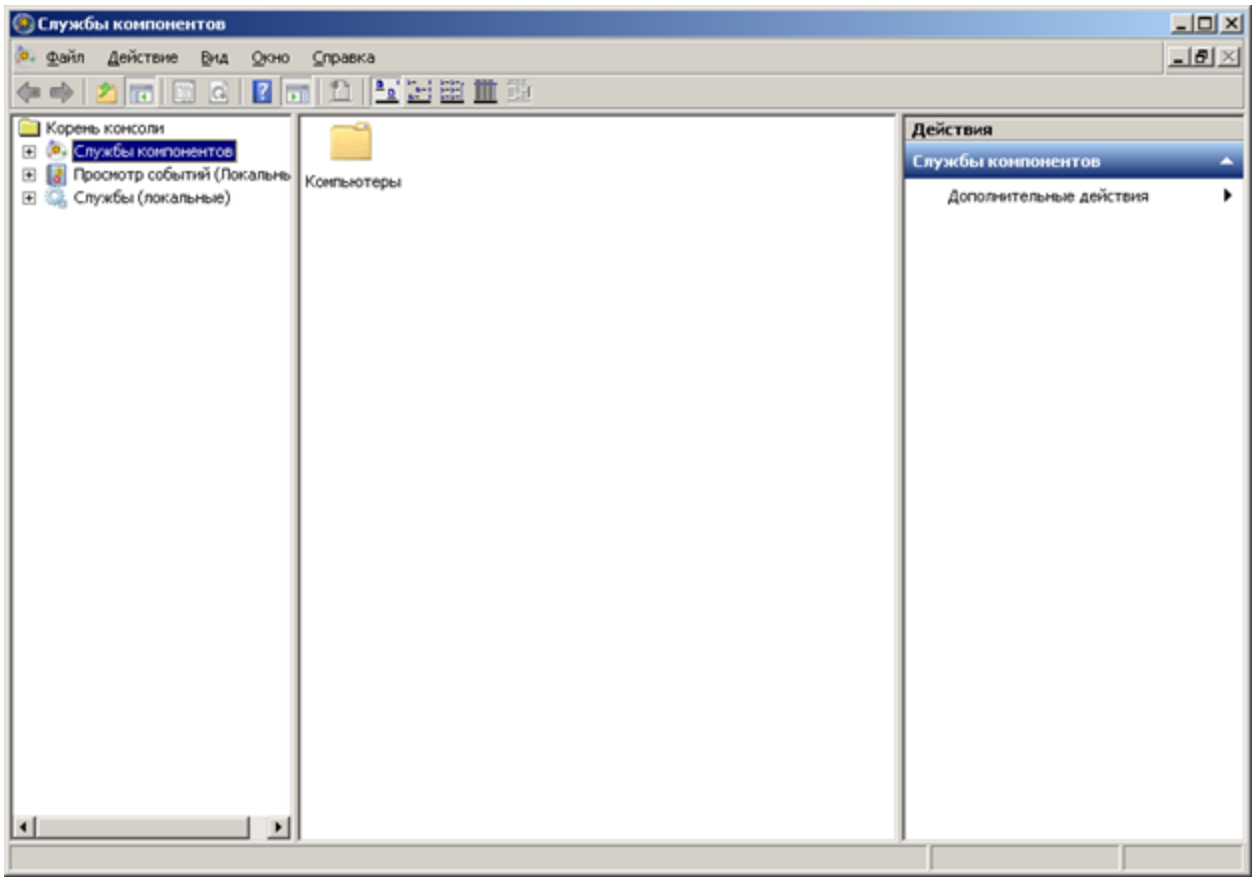
Учётная запись, от имени которой будет работать процесс COM-сервера «Шлюз», должна обеспечивать серверу права на доступ к файлам конфигурации и устройствам в/в. (Эта учётная запись *необязательно* должна принадлежать к группе «администраторы системы»).

1) Запустить утилиту dcomcnfg

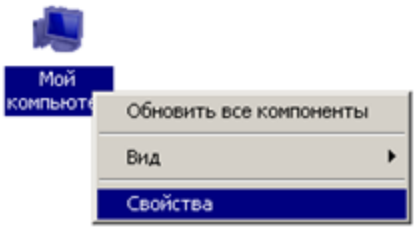
Чтобы запустить утилиту настройки DCOM, необходимо нажать Win +R или Пуск -> выполнить и ввести команду «dcomcnfg» .



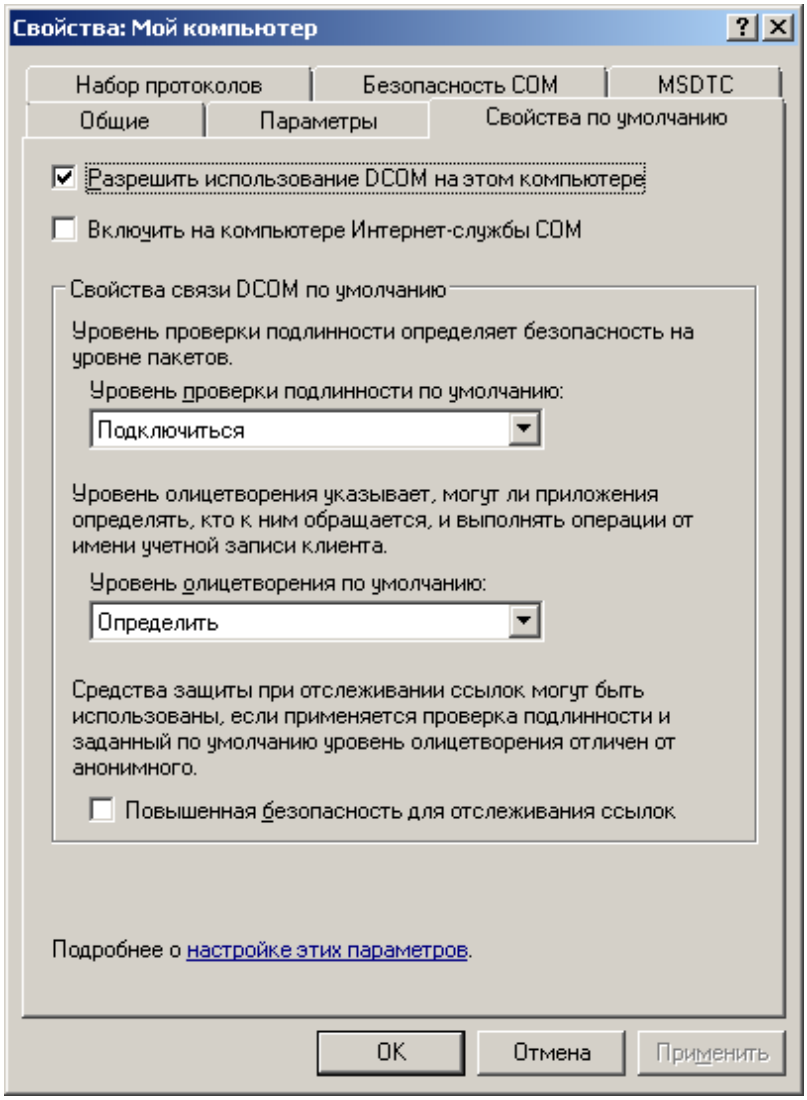
На экране появится окно стандарт ной утилиты наст ройки параметров DCOM.



Щелкаем по значку Компьютеры, выбираем «мой компьютер» и правой кнопкой мыши вызываем контекстное меню, пункт свойства



2) Закладка «Свойства по умолчанию»

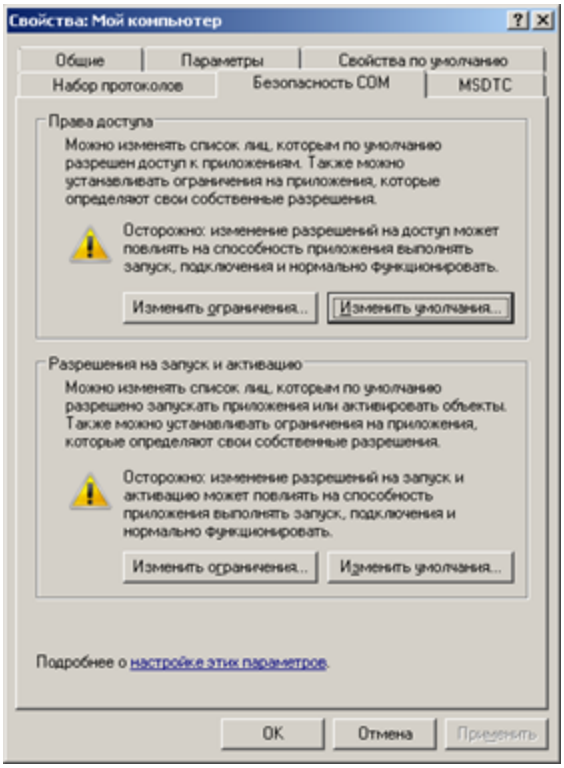


Флажок «разрешить использование DCOM на этом компьютере» должен быть установлен.

Кроме того, в поле «Уровень проверки подлинности по умолчанию» должно стоять «Подключиться». В поле «Уровень олицетворения по умолчанию» должно стоять «Определить».

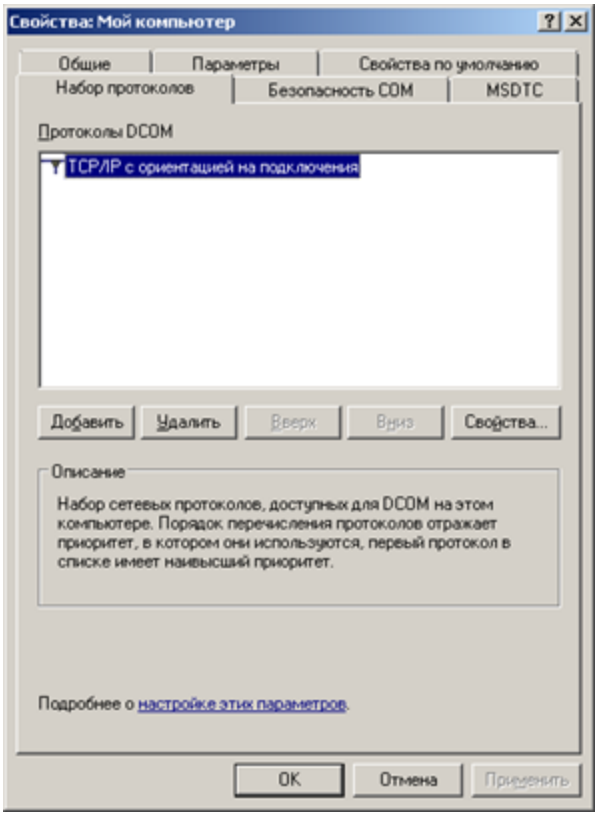
Флажок «Повышенная безопасность для отслеживания ссылок» должен быть снят.

3) Закладка «Безопасность COM»



Убедитесь, что списки пользователей, доступные по кнопкам «Изменить умолчания» и «Изменить ограничения» не содержат запретов для выбранных учётных записей на доступ и запуск COM-серверов.

4) Закладка «Набор протоколов».



Первым в списке должен стоять протокол «TCP/IP с ориентацией на подключения».

Настройка параметров на станции сервера

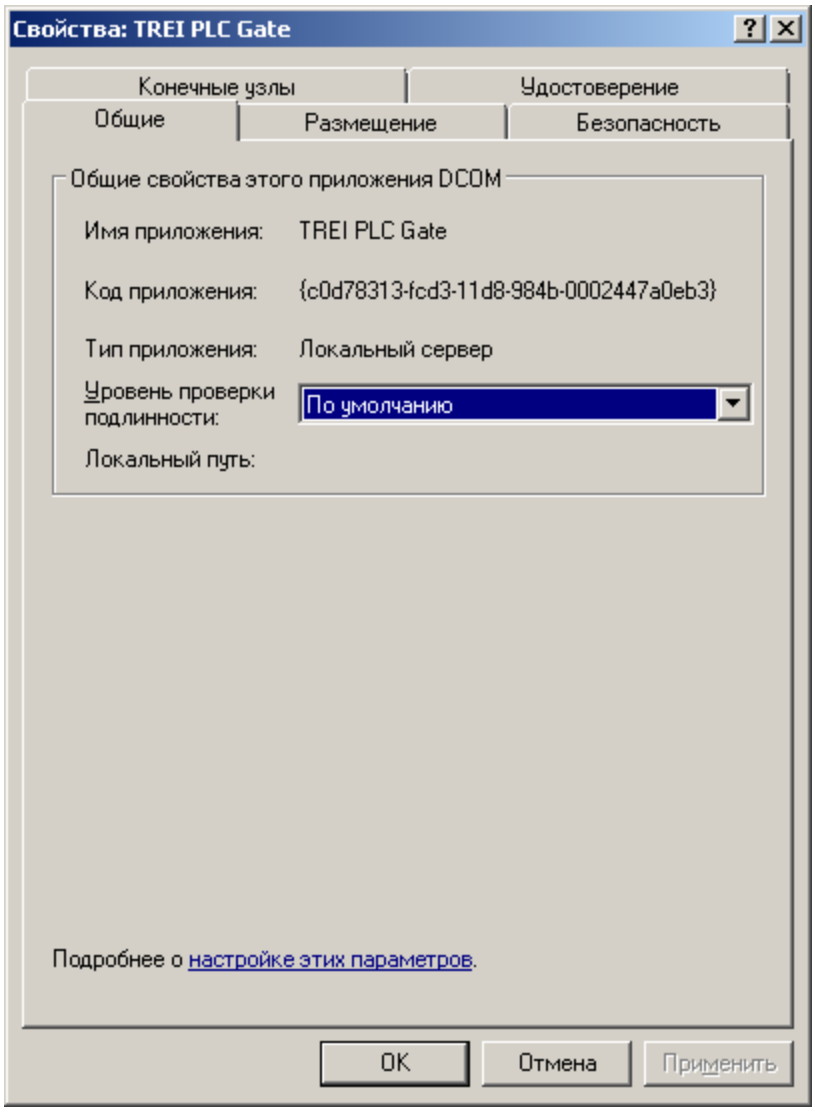
1) Запустите утилиту dcomcnfg и откройте окно стандартных параметров необходимого COM-сервера.

   Для этого необходимо дважды щелкнуть на значке «мой компьютер», затем «настройка DCOM» и выбрать из списка нужный сервер (сервера обозначены как «TREI PLC Gate», «TREI OPC DA server» и «TREI OPC HDA server»). Диалог параметров сервера доступен через контекстное меню «Свойства».


ThirdPartyE...
ThirdPartyE...
Thumbnail Cache Out...
timedate. cpl
TlntSvr
Transforms
TrayDeskto...
TREI PLC Gate
treiOPCDA
treiO
Вид
Свойства
Trusted Instal...
TSTheme
TSWbPrxy. exe
UIAutomati... Class
UICOM

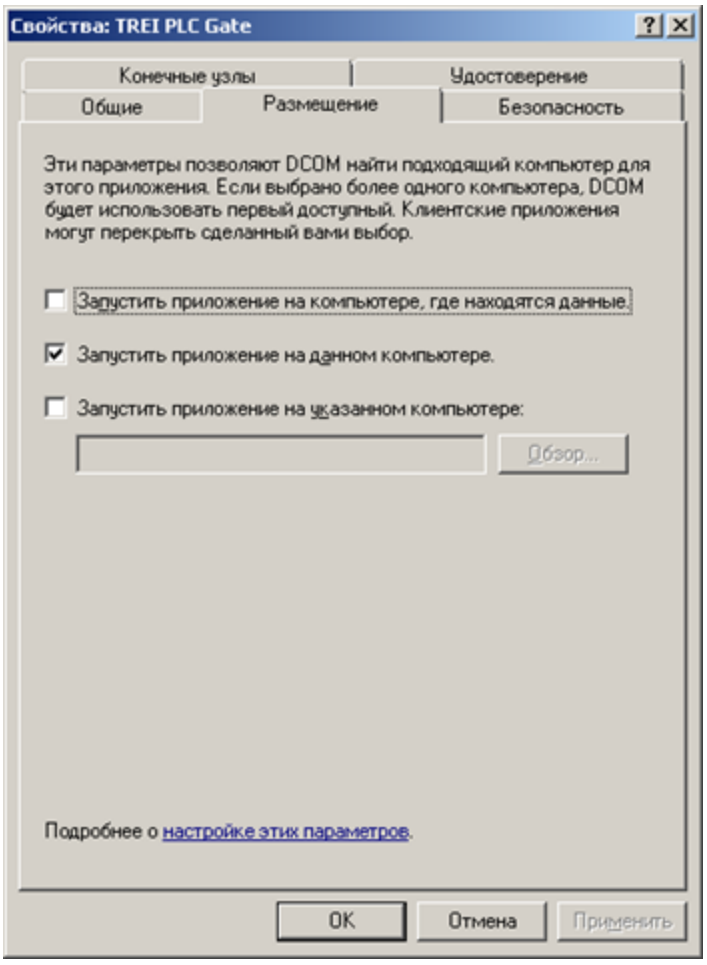
2) Закладка «Общие».

Оставьте все параметры без изменений. По умолчанию, в поле «Тип приложения» должно стоять значение «локальный сервер», а в поле «уровень проверки подлинности» должно стоять значение «по умолчанию».

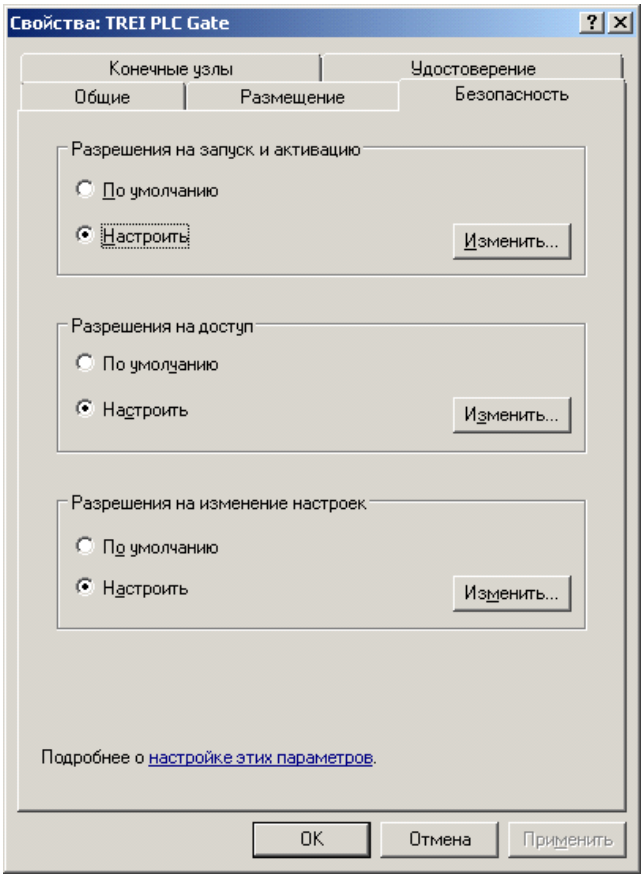


3) Закладка «размещение».

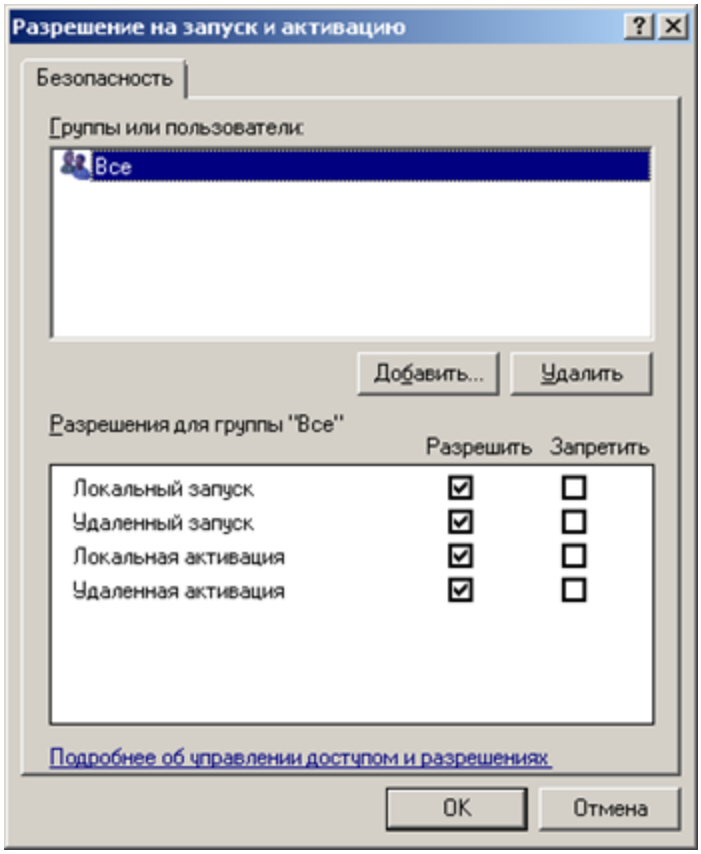
Здесь должен быть установлен только флажок «Запустить приложение на данном компьютере», означающий, что COM-сервер будет запускаться локально, на данной станции.



4) Закладка «Безопасность».



Здесь необходимо отредактировать права на доступ и запуск COM-сервера.



Для этого, выберите «Настроить» и нажмите кнопку «Изменить…» в группе «Разрешение на запуск и активацию». В ответ на это, на экране появится список учётных записей, которым разрешён доступ к серверу.

Список должен содержать следующие элементы:

- Администраторы – доступ разрешается всем пользователям из группы «Администраторы»;
- Интерактивные – доступ разрешается текущему пользователю зарегистрированному в системе;
- Сеть – разрешается доступ к серверу со стороны удалённых

пользователей;

- Система – разрешается доступ к серверу со стороны системной учётной записи.

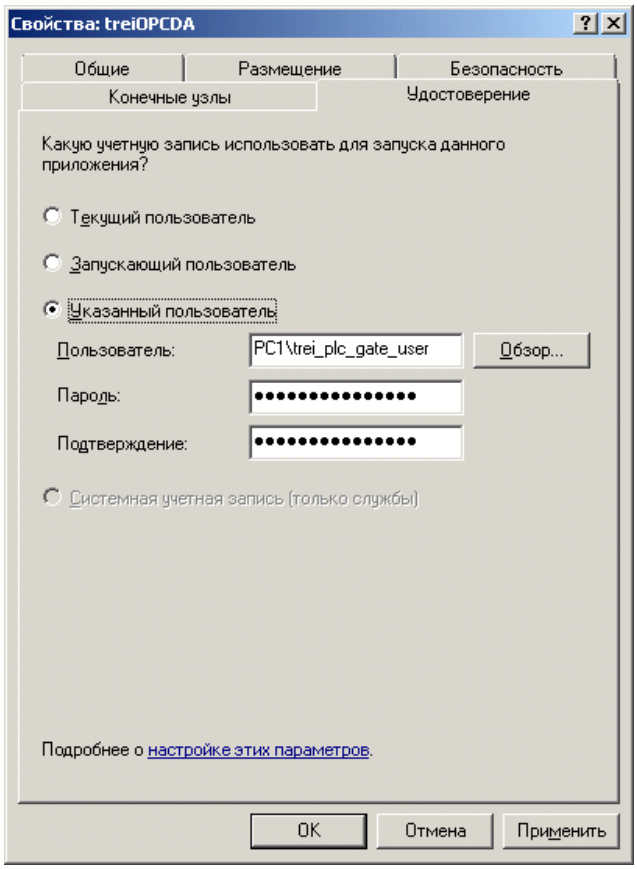
список также должен содержать группу или конкретного пользователя, которым разрешён доступ и работа с данным COM-сервером.

Аналогично настроить разрешения на разрешения на доступ.

Список учётных записей, имеющих право на редактирование параметров («Разрешения на изменение настроек») следует оставить без изменений.

5) Закладка «Удостоверение».

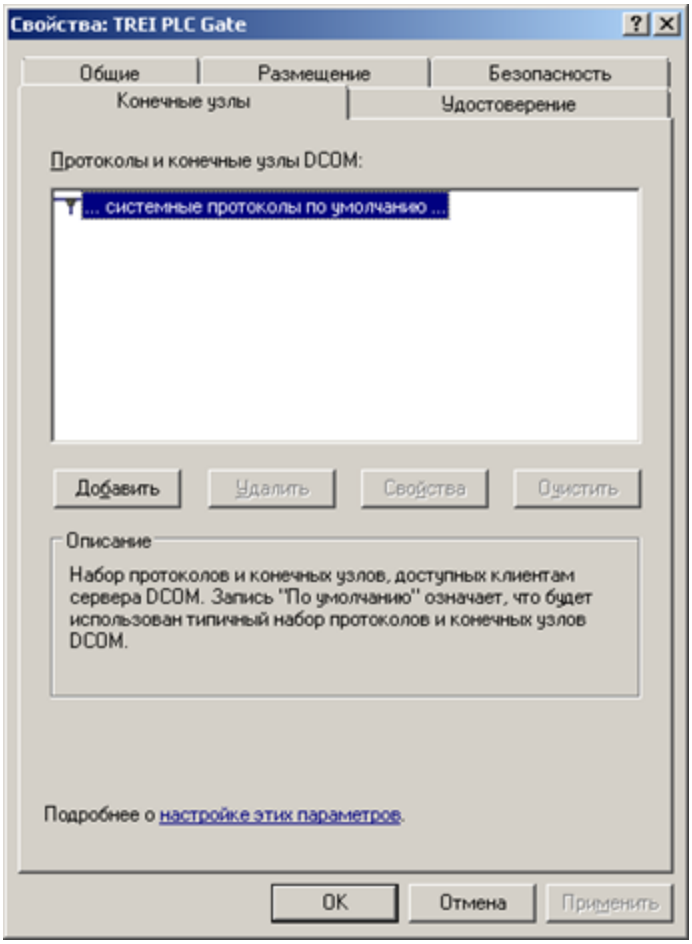
Здесь необходимо явно указать имя и пароль учётной записи (созданной ранее) от имени которой будет работать COM-сервер. Об этой учётной записи должна «знать»(см.выше) как клиентская, так и серверная станция.



Примечание: если учётная запись пользователя принадлежит другому домену, здесь также следует указать имя домена.

6) Закладка «Конечные узлы».

В списке должен присутствовать только элемент «… системные протоколы по умолчанию…», означающий использование системных настроек по умолчанию.



Примечание: если станция расположена в другом домене (рабочей группе), здесь также следует указать имя домена (рабочей группы).

Такие параметры гарантируют запуск COM-сервера на указанной

удалённой станции.

Остальные параметры следует оставить без изменений.

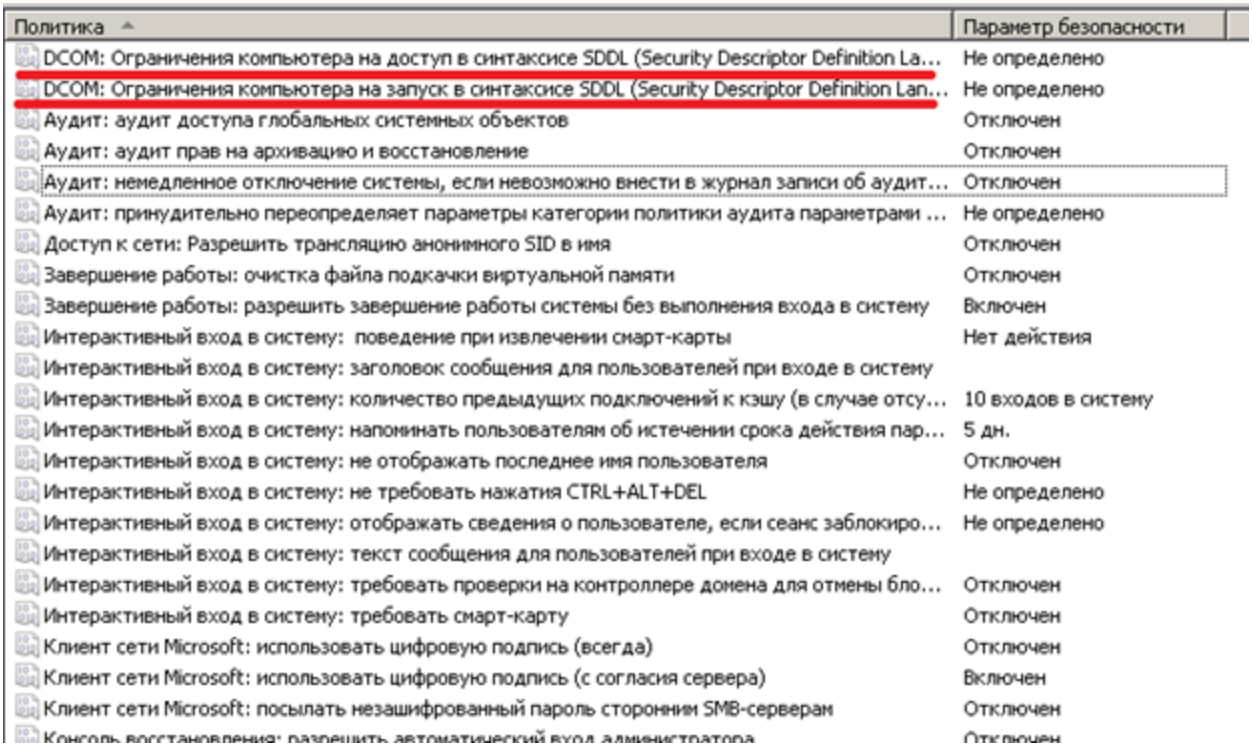
Настройка политики безопасности и отключение брандмауэра Windows

Далее описаны действия, которые необходимо выполнить лишь в том случае, если удалённое подключение так и не удалось установить.

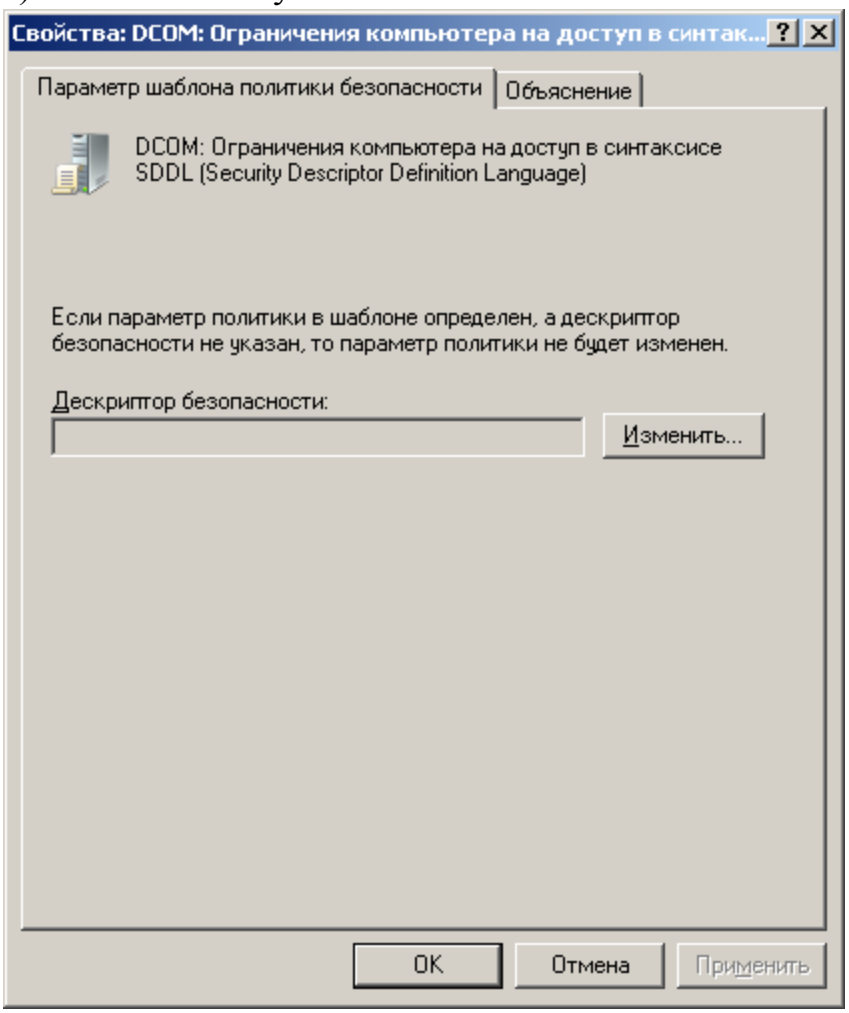
Политика безопасности

Зайти в Панель управления\Администрирование\Локальная политика безопасности

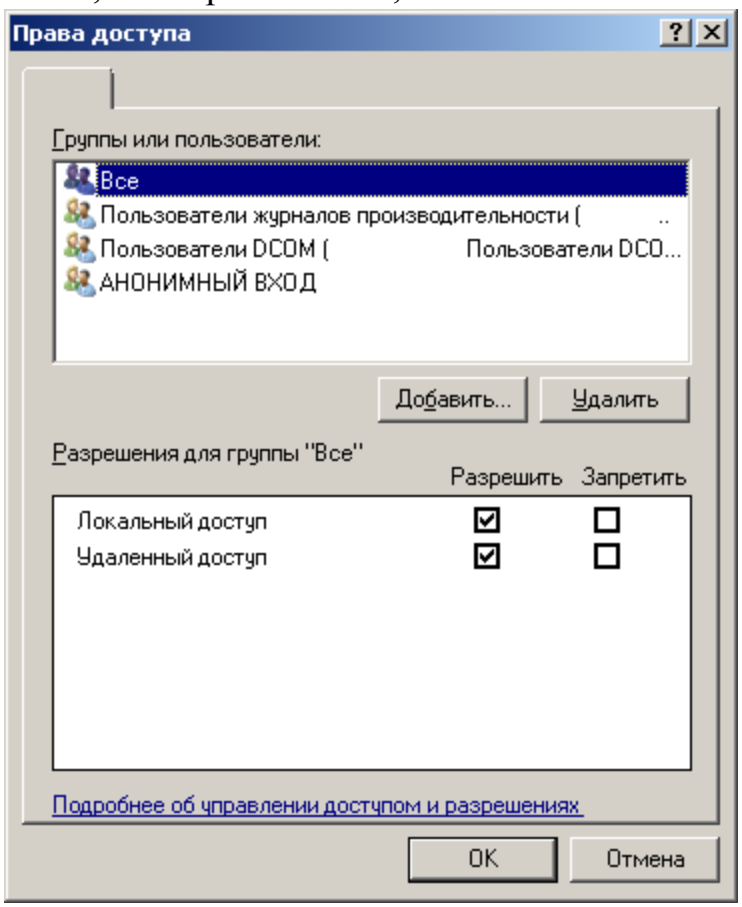
1) Выбрать «Параметры безопасности\Локальные политики \Параметры безопасности» Нажать правую кнопку мыши на «DCOM: Ограничения компьютера на доступ в синтаксисе SDDL» и выбрать «Свойства»



2) Нажать кнопку «Изменить безопасность»



3) В появившемся окне выставить следующие разрешения: разрешить "Локальный доступ", "Удаленный доступ" для пользователей: "Все", "Интерактивные", "Сеть" и "Система":



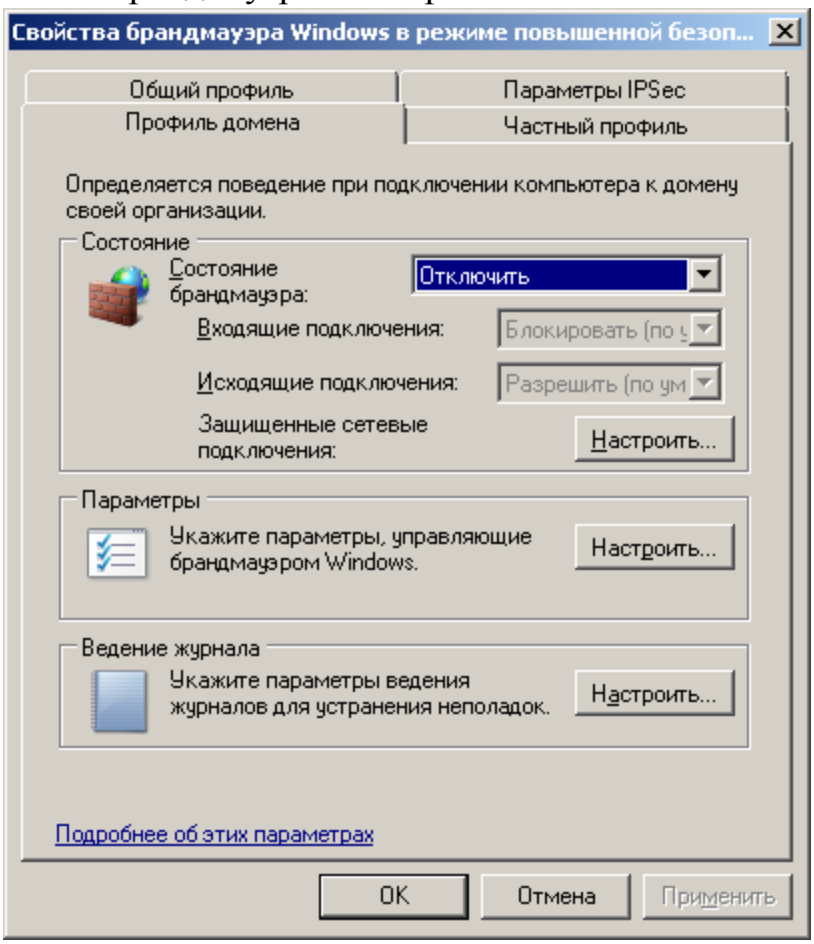
4) Повторить операцию на пункту «DCOM: Ограничения компьютера на запуск в синтаксисе SDDL». Разрешения: «Локальный запуск», «Удаленный запуск», «Локальная активация», «Удаленная активация» для пользователей: «Все», «Интерактивные», «Сеть», «Система» и «Интерактивные».

6) «Сетевой доступ: разрешить применение разрешений для всех к анонимным пользователям» установить в положение «Включено».

7) Задать политике «Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей» параметр: «Обычная - локальные пользователи удостоверяются как они сами».

Настройка брандмауэра Windows

1) «Брандмауэр Windows»->«Дополнительные параметры»-> «Свойства брандмауэра Windows». На закладках «Профиль домена»\ «Частный профиль» \«Общий профиль»
пункт «Состояние брандмауэра» выберите «Отключить».



2) Вкладка Включение и отключение брандмауэра: везде установить галочки «отключить».