ИТРИУМ®

Программное обеспечение интегрированной системы безопасности ITRIUM®

Драйвер SCADA

Руководство пользователя

Санкт-Петербург
2020

Содержание

1 Назначение Драйвера SCADA

ПО ITRIUM® может выступать в качестве универсального **OPC-сервера** для контроллеров охранной, пожарной сигнализации, систем контроля доступа и IP-видеонаблюдения различных производителей.

«Драйвер SCADA» позволяет:

- подключить к любой SCADA-системе любое оборудование, поддерживаемое ПО ITRIUM®;
- передавать в SCADA-систему события, возникающие в системе охранной, пожарной сигнализации, контроля доступа и IP-видеонаблюдения, в виде переменных (тегов);
- посылать команды постановки/снятия с охраны, открытия/закрытия считывателей и другие команды, доступные в ПО ITRIUM®, в виде переменных (тегов).

☑ **Примечание:** «Драйвер SCADA» поддерживает стандарт **OPC Data Access 2.05a**.

2 Конфигурирование Драйвера SCADA

Для того чтобы сконфигурировать «Драйвер SCADA», необходимо в программе «Администратор системы» (рисунок 1):

- добавить элемент **Драйвер SCADA** (см. раздел Добавление элемента Драйвер SCADA);
- добавить ссылку на элемент системы безопасности (см. раздел Добавление ссылки на элемент системы безопасности).

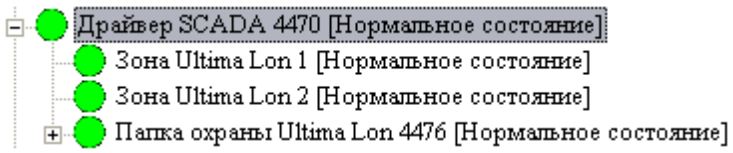

Рисунок 1 — Пример дерева элемента **Драйвер SCADA**

☑ **Примечание:** Перед конфигурированием **Драйвера SCADA** убедитесь, что в системе безопасности сконфигурированы и корректно работают драйверы и службы, с которыми необходимо работать в OPC-клиенте. Информацию по настройке драйверов и служб см. в соответствующих руководствах пользователей.

2.1 Добавление элемента Драйвер SCADA

Для добавления **Драйвера SCADA** необходимо:

1. В программе «Администратор системы» в дереве элементов выделить мышью элемент **Компьютер**, на котором установлен **OPC-клиент**.
2. Добавить элемент **Драйвер SCADA**, для этого на панели инструментов нажать на кнопку  .
3. В появившемся окне **Добавить к "Компьютер"** выделить мышью элемент **Драйвер SCADA**, нажать на кнопку **Добавить** (для поиска элемента можно воспользоваться фильтром).
4. В окне **Свойства "Драйвер SCADA"**:
   - На вкладке **Общие** в поле **Имя** введите удобное пользователю имя элемента;
   - На вкладке **Драйвер** в группе **Параметры запуска** выберите переключатель **В выделенном приложении**;
   - для того, чтобы система каждую минуту проверяла работу драйвера установите флаг **Посылать сообщение Keep-alive каждую минуту**. При этом в программе «Администратор системы» в списке сообщений каждую минуту будет выдаваться сообщение «*УУ протестировано*». Если сообщение «*УУ протестировано*» не появилось в списке сообщений, то драйвер «завис». Автоматическую перезагрузку драйвера можно настроить в «Службе автоматического управления» (руководство пользователя см. установочный диск ITRIUM®, раздел **Документация – Службы – Служба автоматического управления**).
   - На вкладке **Параметры сервера OPC**, при необходимости, задайте параметры формирования тегов (подробнее см. Параметры формирования тегов в разделе Представление элемента переменными). Вы можете позже вернуться к этой группе настроек на странице частных свойств элемента **Драйвер SCADA**.
   - нажмите на кнопку **Принять**.

2.2 Добавление ссылки на элемент системы безопасности

К **Драйверу SCADA** необходимо добавлять ссылки на те элементы системы безопасности, свойства, состояние и событие от которых должны быть переданы в виде переменных (тегов) в SCADA-систему.

Чтобы добавить ссылку на элемент системы безопасности, необходимо:

1. Выделить мышью элемент **Драйвер SCADA**.
2. Из контекстного меню элемента выбрать пункт **Добавить дочерний элемент** (рисунок 2).

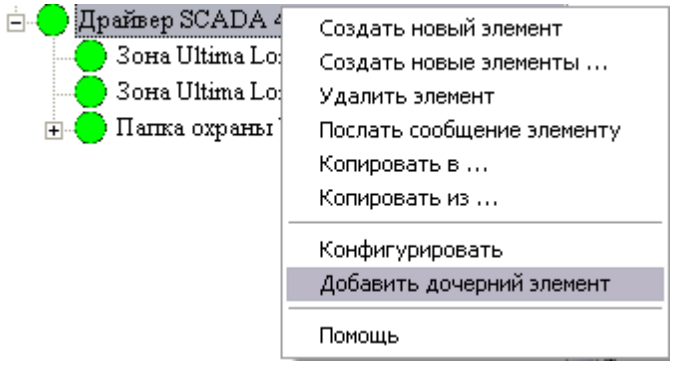

Рисунок 2 — Контекстное меню элемента **Драйвер SCADA**

3. В появившемся окне **Параметры команды "Добавить дочерний элемент" "Драйвер SCADA"** (рисунок 3) выберите элемент, с которым необходимо работать в OPC-клиенте. В нижней части окна выберите пункт **Без дочерних элементов**, если необходимо добавить элемент без ветки дочерних элементов. Нажмите на кнопку **Принять**.

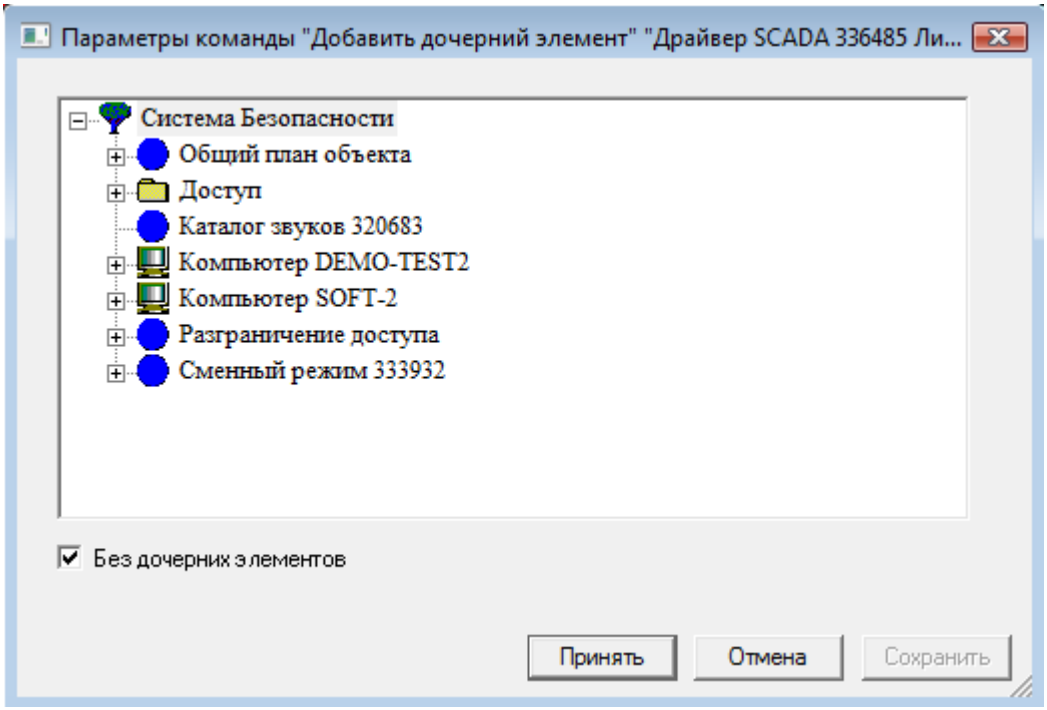

Рисунок 3 — Окно **Параметры команды "Добавить дочерний элемент" "Драйвер SCADA"**

☑ **Примечание:** В окне **Параметры команды "Добавить дочерний элемент" "Драйвер SCADA"** отображаются только те элементы, которые были раннее добавлены в систему. Поэтому, перед добавлением ссылки, необходимо добавить и сконфигурировать нужный элемент.

После этого к **Драйверу SCADA** добавится ссылка на выбранный элемент. Необходимо повторить данные действия столько раз, со сколькими элементами должна работать SCADA-система. На основании созданного дерева ссылок OPC-сервер ITRIUM® будет строить

внутреннее адресное пространство переменных (тегов), описывающее состояния, свойства и события элементов системы безопасности.

3 Настройка SCADA-системы

Чтобы настроить SCADA-систему для работы с ПО ITRIUM®, необходимо:

1. В программе SCADA-системы добавить **OPC-сервер ItriumOPCServer.DA**;
2. Из SCADA-системы подключиться к серверу, создать группу и добавить в нее нужные теги (имена которых можно предварительно получить с помощью интерфейса **IOPCBrowseServerAddressSpace**, который должен поддерживаться SCADA-системой).
3. В программе «Администратор системы» в частных свойствах элемента **Компьютер** в поле **Автоматический старт службы под именем** выбрать значение **Администратор системы**.

OPC-сервером ПО ITRIUM® поддерживается синхронная/асинхронная запись тегов, синхронное/асинхронное чтение тегов, а также выдача изменившихся значений тегов по подписке **IOPCDataCallback** (то есть без запроса со стороны SCADA-системы об изменении состояний всех тегов сервера).

☑ **Примечание:** В данном разделе указаны особенности настройки SCADA системы. Подробное описание настройки см. в документации к SCADA системе..

4 Настройка работы SCADA-системы через DCOM

Для работы SCADA-системы с ПО ITRIUM® по сети, необходимо:

1. Создать на компьютере-клиенте и на компьютере-сервере нового пользователя с одинаковым именем и паролем и добавить его в группу администраторов. Для этого:
   - В меню **Пуск** выберите пункт **Панель управления**;
   - Выберите элемент **Учетные записи пользователей**;
   - Выберите пункт **Управление учетными записями пользователей**;
   - В открывшемся окне **Учетные записи пользователей** на вкладке **Пользователи** нажмите на кнопку **Добавить**;
   - В поле **Пользователь** введите имя пользователя, в поле **Домен** введите имя компьютера;
   - Нажмите на кнопку **Далее**;

- Выберите пункт **Администратор** и нажмите на кнопку **Готово**.

2. На время настройки отключите **Windows Firewall (Брандмауэр Windows)**. См. раздел Отключение Брандмауэра Windows.

3. В Windows 7, Windows XP и Windows Vista необходимо настроить локальную политику безопасности. См. раздел Настройка Локальной политики безопасности. В этом нет необходимости для Windows 2000 или более ранних версий.

4. Настройте DCOM. См. раздел Настройка DCOM.

5. Включите и настройте **Windows Firewall (Брандмауэр Windows)**. См. раздел Настройка Брандмауэра Windows.

6. На компьютере-сервере в программе «Администратор системы» в частных свойствах элемента **Компьютер** в поле **Автоматический старт службы под именем** выберите **Администратор системы**.

7. Настройте приложение DCOM **ItriumOPCServer**. См. раздел Настройка приложения DCOM ItriumOPCServer.

8. Настройте службу **OpcEnum** с помощью оснастки **Службы Консоли управления Microsoft**. См. раздел Настройка службы OpcEnum.

9. Настройте **Драйвер OPC-сервера**. См. Настройка Драйвера OPC.

10. Запустите командный интерпретатор **cmd**. В командной строке введите **runas /user:userOPC "C:\Program Files\Common Files\ICONICS\DataSpy.exe"**, где **userOPC** - имя пользователя, **C:\Program Files\Common Files\ICONICS\DataSpy.exe** - путь к файлу **DataSpy.exe**. Нажмите на кнопку **Enter**. Введите пароль пользователя. Запустится клиент **OPC DataSpy**. В дереве элементов необходимо выбрать сервер (Ag – имя рабочей группы, в которую входит сервер) и проверить корректность настройки.

Для диагностики неполадок можно использовать утилиту **OPC Security Analyzer**. **При работе с OPC Security Analyzer** для более полной диагностики проблем нужно запустить службу **Удаленный реестр** на сервере.

☑ **Примечание**: На некоторых версиях Windows возможны проблемы при работе с **Crypto API**. Это приводит к тому, что невозможно вычитать закодированный пароль в реестре (этот пароль сохраняется в закодированном виде, когда производится запуск службы под именем и сохранение). Для этих случаев была добавлена возможность задавать нужный пароль доступа к ПО ITRIUM® в открытом виде в реестре. Для этого необходимо в **KeeperConnection** создать строковой параметр **OPCLogonPassword** и в значение вписать пароль.

4.1 Отключение Брандмауэра Windows

Чтобы отключить **Брандмауэр Windows 7** выполните следующую последовательность шагов:

1. Откройте **Панель управления.** В окне **Поиск в панели управления** введите текст **брандмауэр**, выберите пункт **Брандмауэр Windows** (см. рисунок 4).

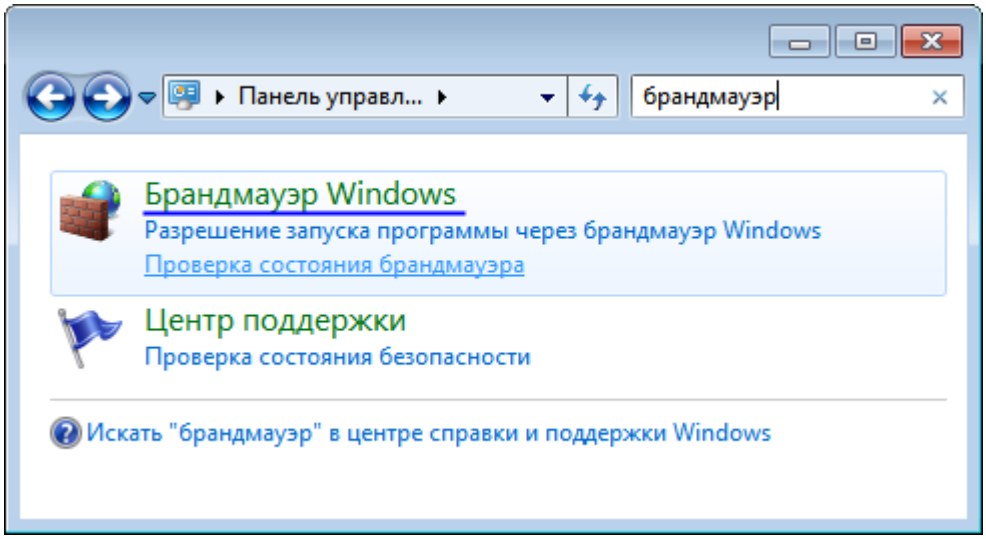

Рисунок 4 — Панель управления. Результаты поиска по запросу **брандмауэр**

2. В открывшемся окне в левом столбце выберите пункт **Включение и отключение брандмауэра Windows** (см. рисунок 5).

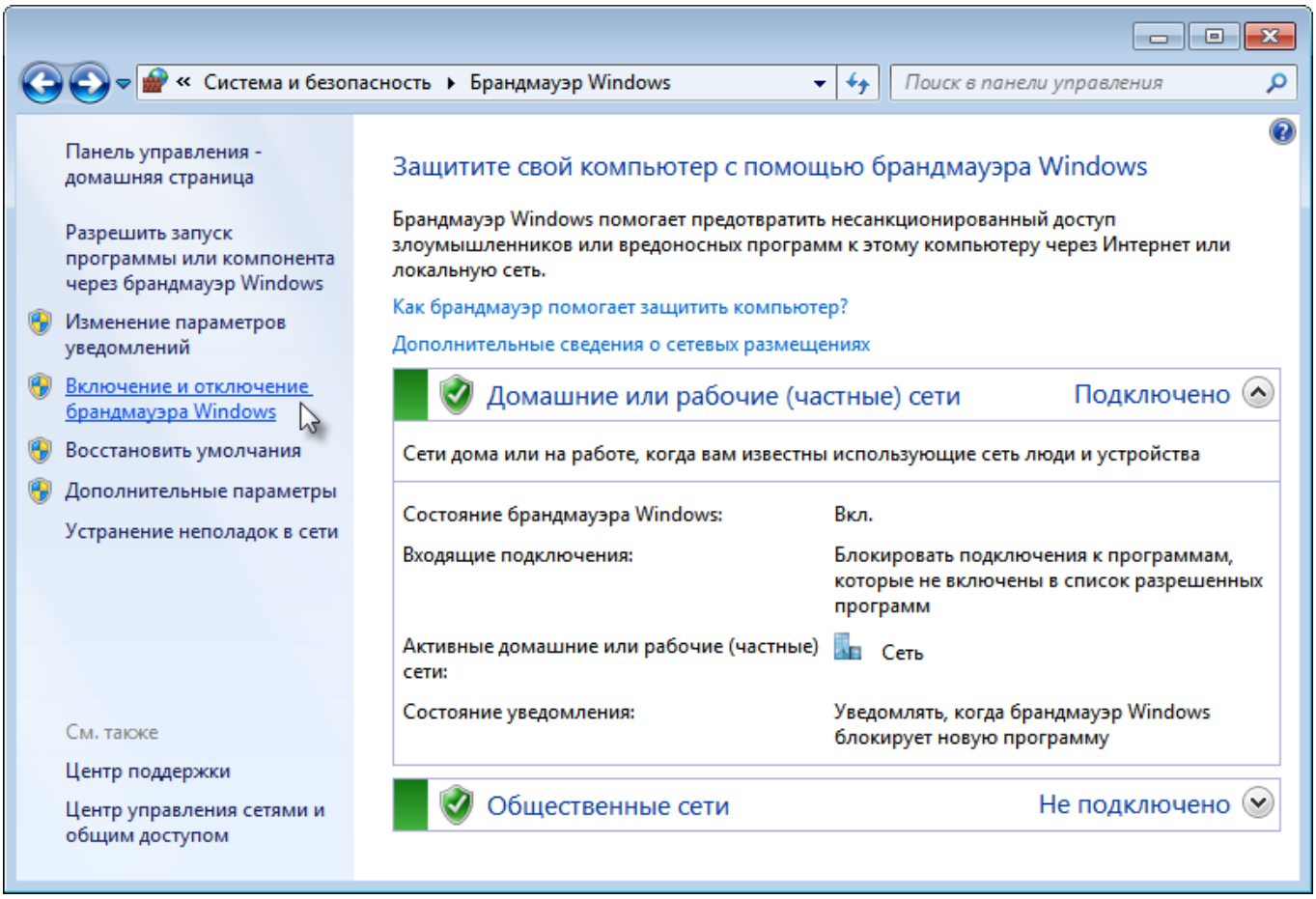

Рисунок 5 — Панель управления. Раздел **Брандмауэр Windows**

3. В открывшемся окне выберите пункт **Отключить брандмауэр Windows (не рекомендуется)** для каждого сетевого размещения, защиту которого нужно отключить (см. рисунок 6).

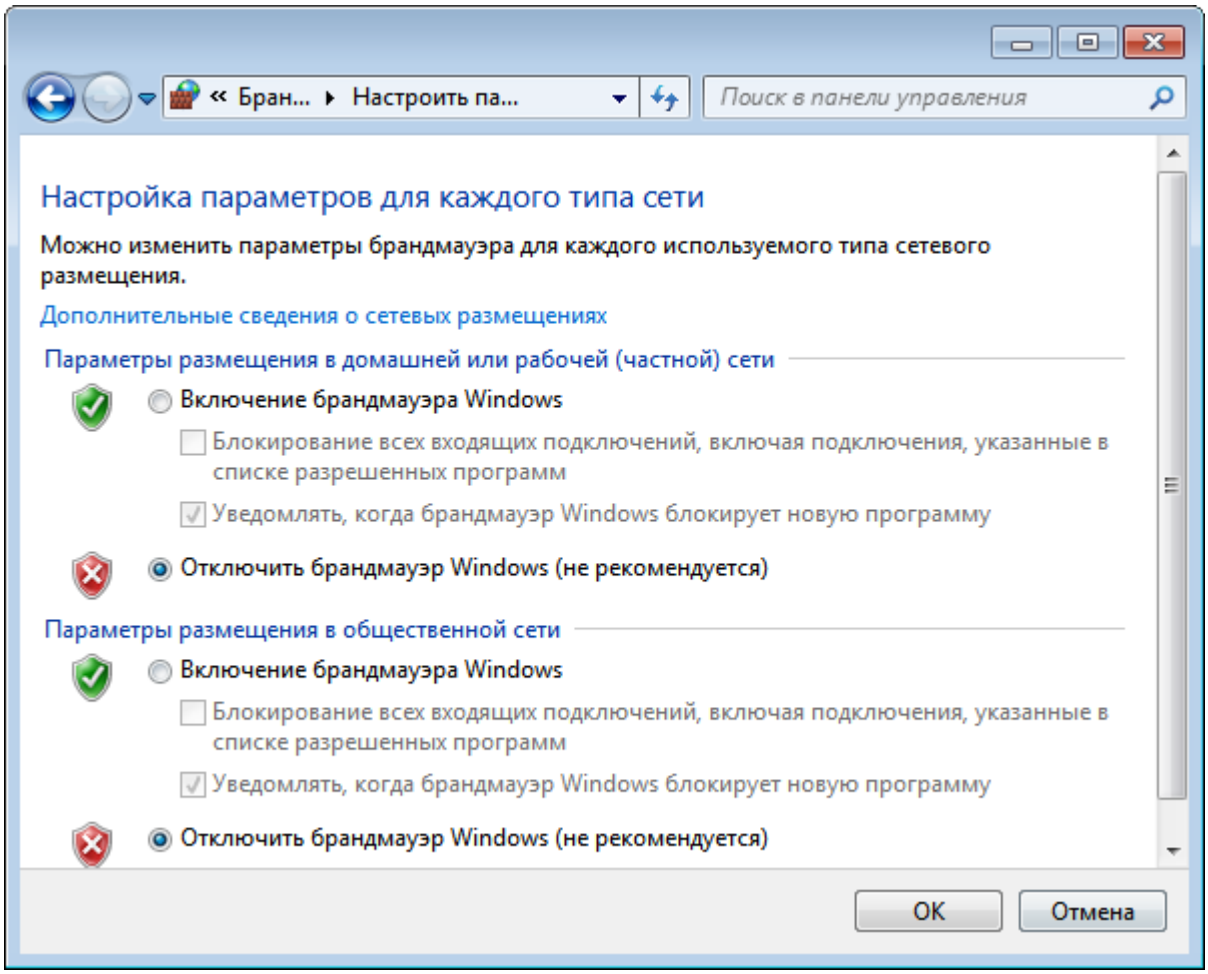

Рисунок 6 — Панель управления. Окно **Настроить параметры**

4. Нажмите кнопку **ОК**.

3. В окне **Брандмауэр Windows** (см. рисунок 7) в левом столбце выберите пункт **Дополнительные параметры.**

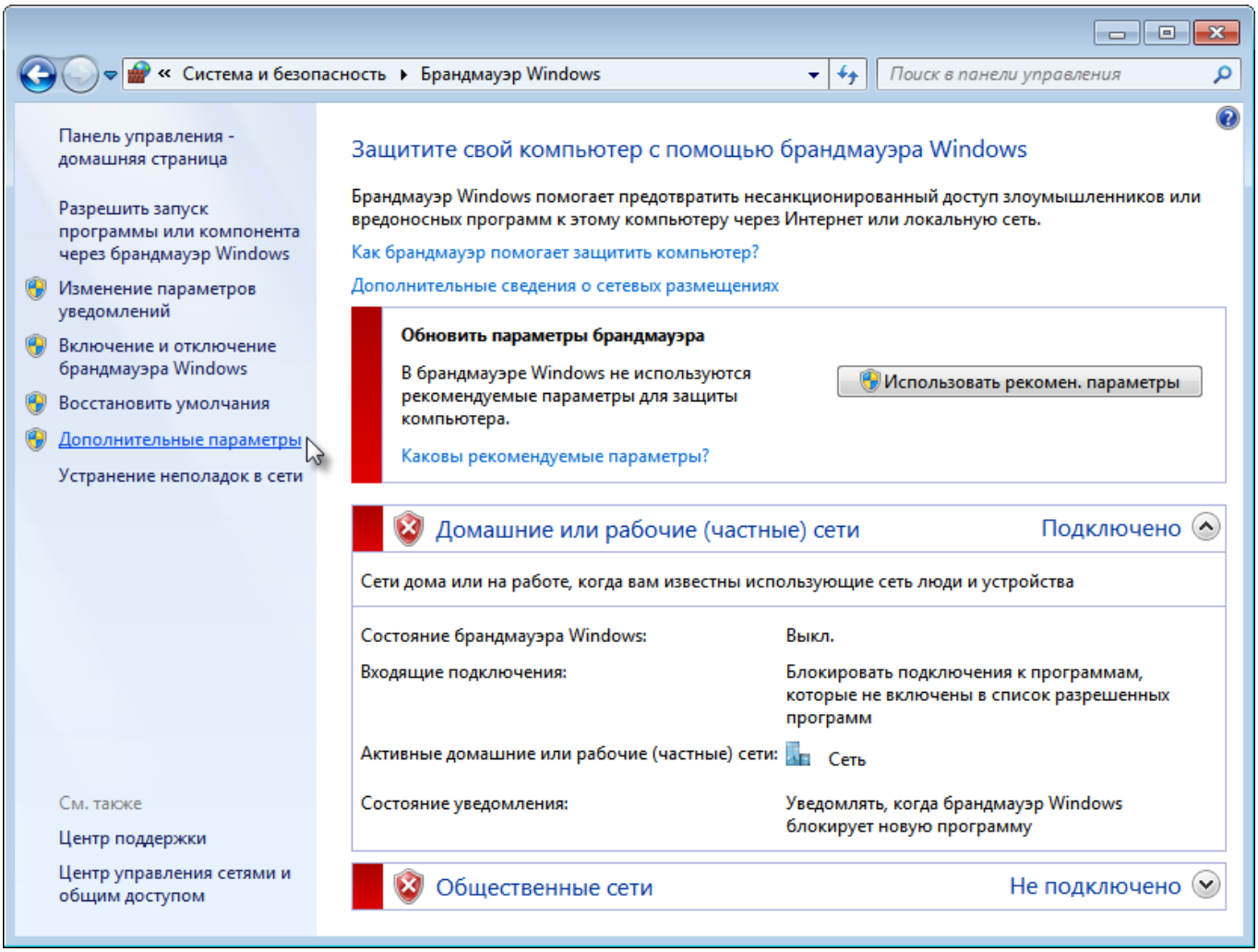

Рисунок 7 — Панель управления. Окно **Брандмауэр Windows**

6. В окне **Брандмауэр Windows в режиме повышенной безопасности** (см. рисунок 8) в группе свойств **Обзор** выберите пункт **Свойства брандмауэра Windows**.

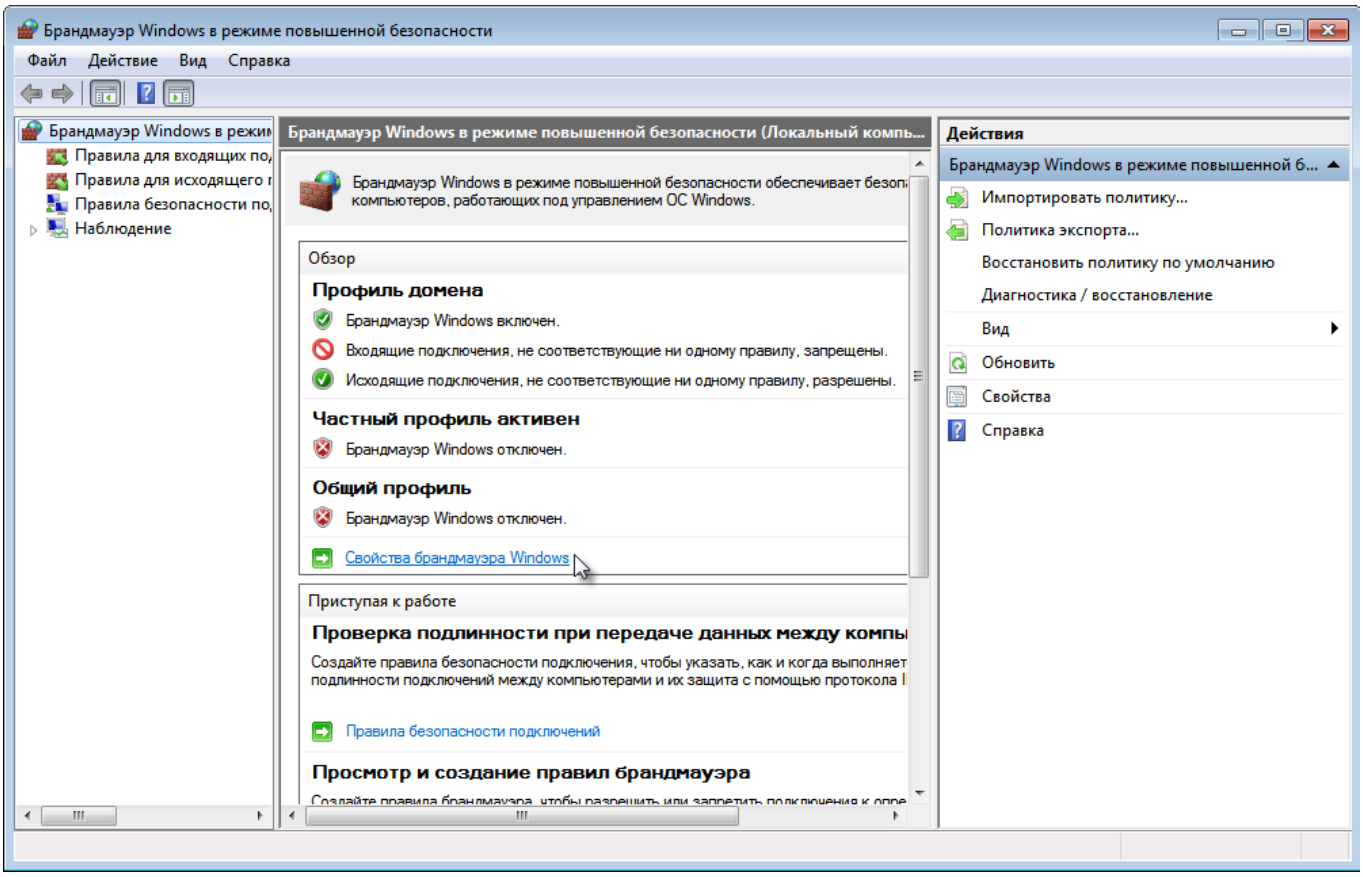

Рисунок 8 — Панель управления. Окно **Брандмауэр Windows в режиме повышенной безопасности**

7. В открывшемся окне **Свойства брандмауэра Windows в режиме повышенной безопасности** во вкладках **Общий профиль**, **Частный профиль**, **Профиль домена** в ниспадающем списке **Состояние брандмауэра** выберите значение **Отключить** (см. рисунок 9).

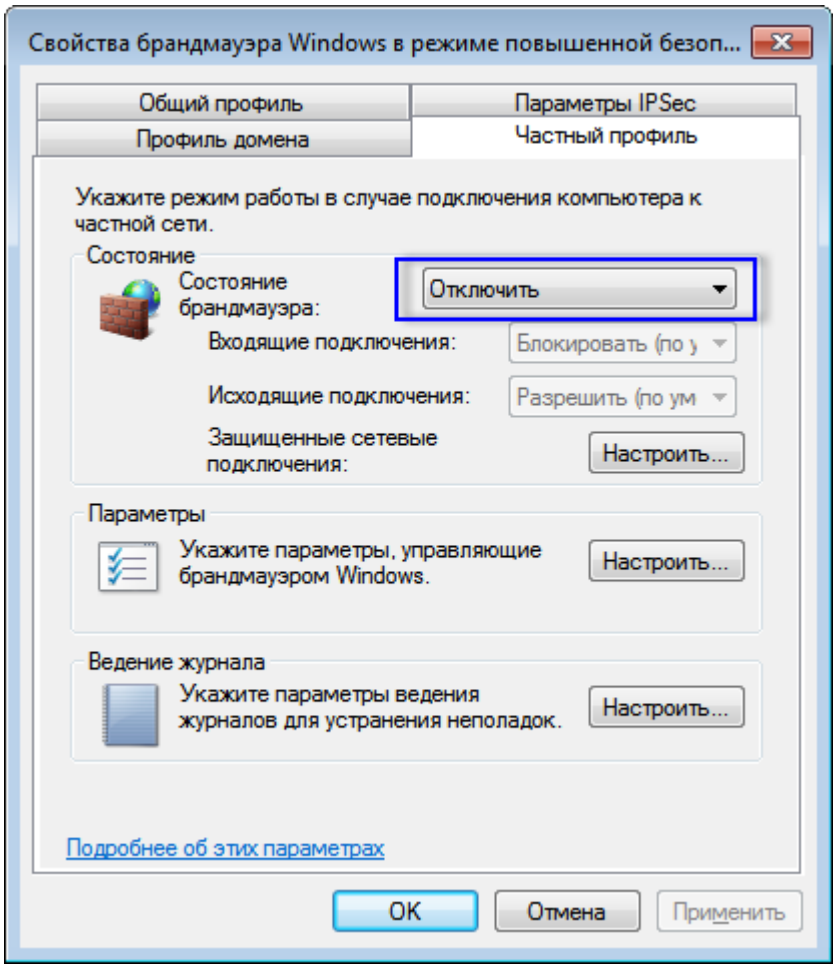

Рисунок 9 — Панель управления. Окно **Свойства брандмауэра Windows в режиме повышенной безопасности**

8. Нажмите кнопки **Применить** и **OK**.

9. В окне **Брандмауэр Windows в режиме повышенной безопасности** в группе свойств **Обзор** под названием каждого из профилей должно быть отображено **Брандмауэр Windows отключен** (см. рисунок 10).

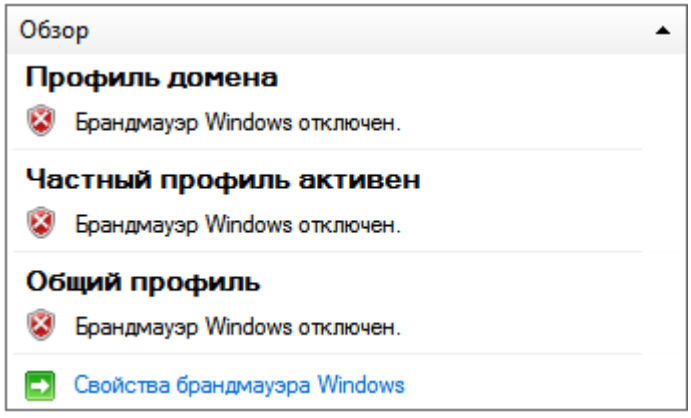

Рисунок 10 — Группа свойств **Обзор**

Чтобы отключить **Брандмауэр Windows XP** выполните следующую последовательность шагов:

- В меню **Пуск** выберите пункт **Панель управления**;
- Выберите элемент **Windows Firewall**;
- Нажмите на **Изменить параметры**;
- Выберите пункт **Выключить (не рекомендуется)**;
- Нажмите на кнопку **Принять** и **ОК**.

4.2 Настройка локальной политики безопасности

Для сетевого доступа необходимо применить параметр **Обычная** - локальные прользователи удостоверяются как они сами. Для этого:

- В меню **Пуск** выберите пункт **Панель управления**;
- Выберите элемент **Администрирование**;
- Выберите пункт **Локальная политика безопасности**;
- В открывшемся окне в дереве элементов **Параметры безопасности** выберите элемент **Локальные политики**;
- Выберите пункт **Параметры безопасности** (рисунок 11);

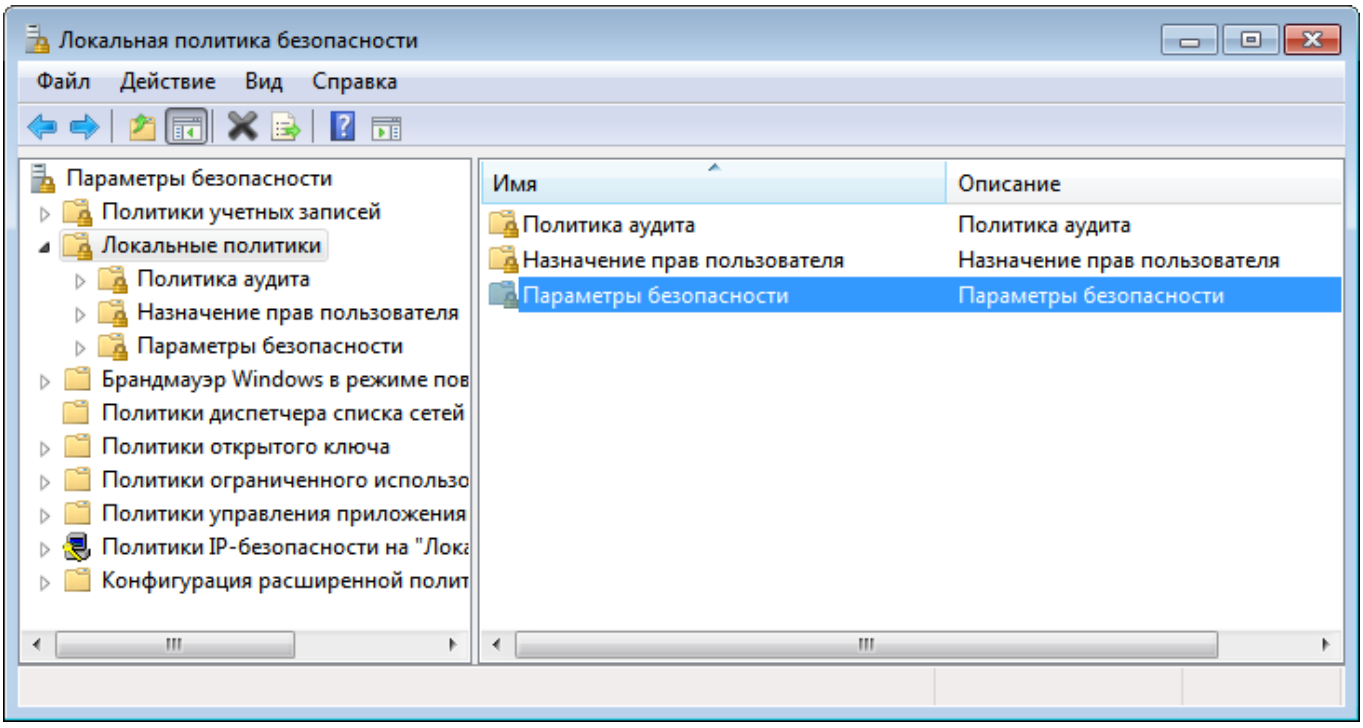

Рисунок 11 — Окно **Локальная политика безопасности**

- В открывшемся списке выберите пункт **Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей**. Двойным щелчком мыши вызовите окно **Свойства: Сетевой доступ: модель совместного доступа и безопасности для учетных записей**. Во вкладке **Параметр локальной безопасности** выберите Обычная - локальные пользователи удостоверяются как они сами (рисунок 12). Нажмите на кнопку **Принять** и **ОК**.

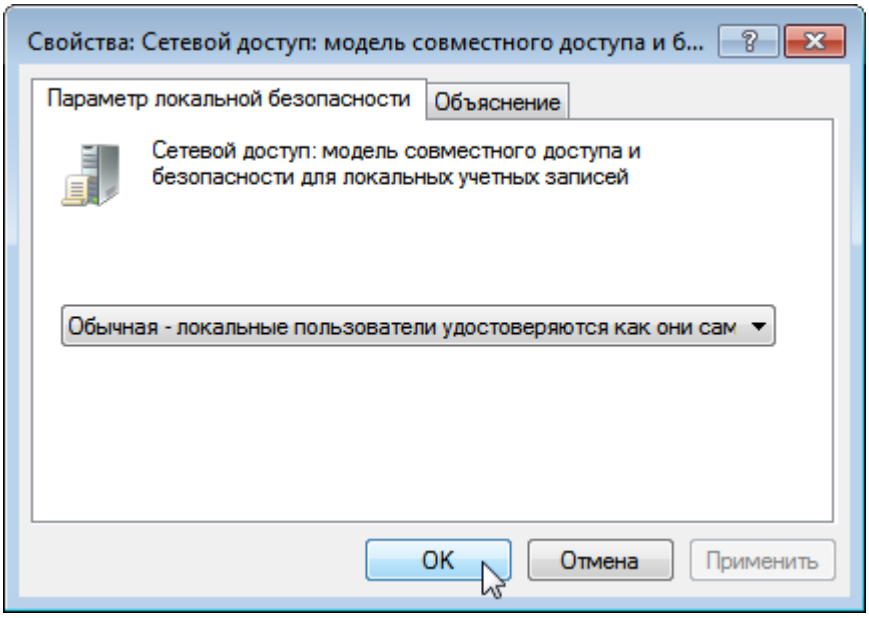

Рисунок 12 — окно **Локальная политика безопасности**

4.3 Настройка DCOM

Настроить **DCOM** можно через утилиту **DCOMCNFG**, которая поставляется как часть операционной системы. Для этого:

- В меню **Пуск** выберите команду **Выполнить...**, введите название утилиты **DCOMCNFG** и нажмите на кнопку **OK** (если команда **Выполнить...** не отображается, введите **DCOMCNFG** в строке поиска и запустите утилиту).
- В открывшемся окне **Службы компонентов** в окне слева раскройте дерево элементов и выберите элемент **Мой компьютер**;
- В окне по центру вызовите контекстное меню элемента **Мой компьютер** щелчком правой клавиши мыши и выберите пункт **Свойства** (рисунок 13);

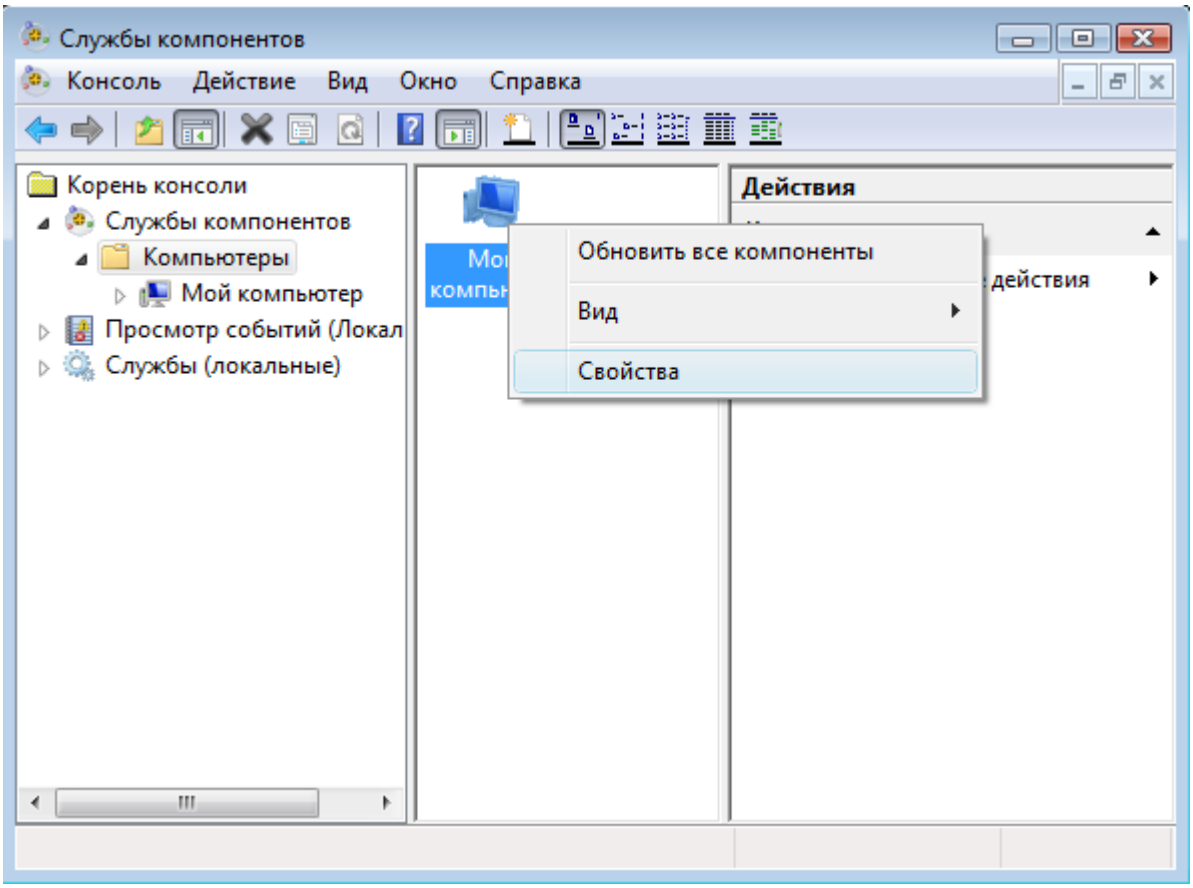

Рисунок 13 — Окно **Службы компонентов**

- В открывшемся окне **Свойства: Мой компьютер** на вкладке **Свойства по умолчанию** выберите пункт **Разрешить использование DCOM на этом компьютере**, из ниспадающего списка **Уровень проверки подлинности по умолчанию** выберите **Подключиться**, из ниспадающего списка **Уровень олицетворения по умолчанию** выберите **Определить** (рисунок 14);

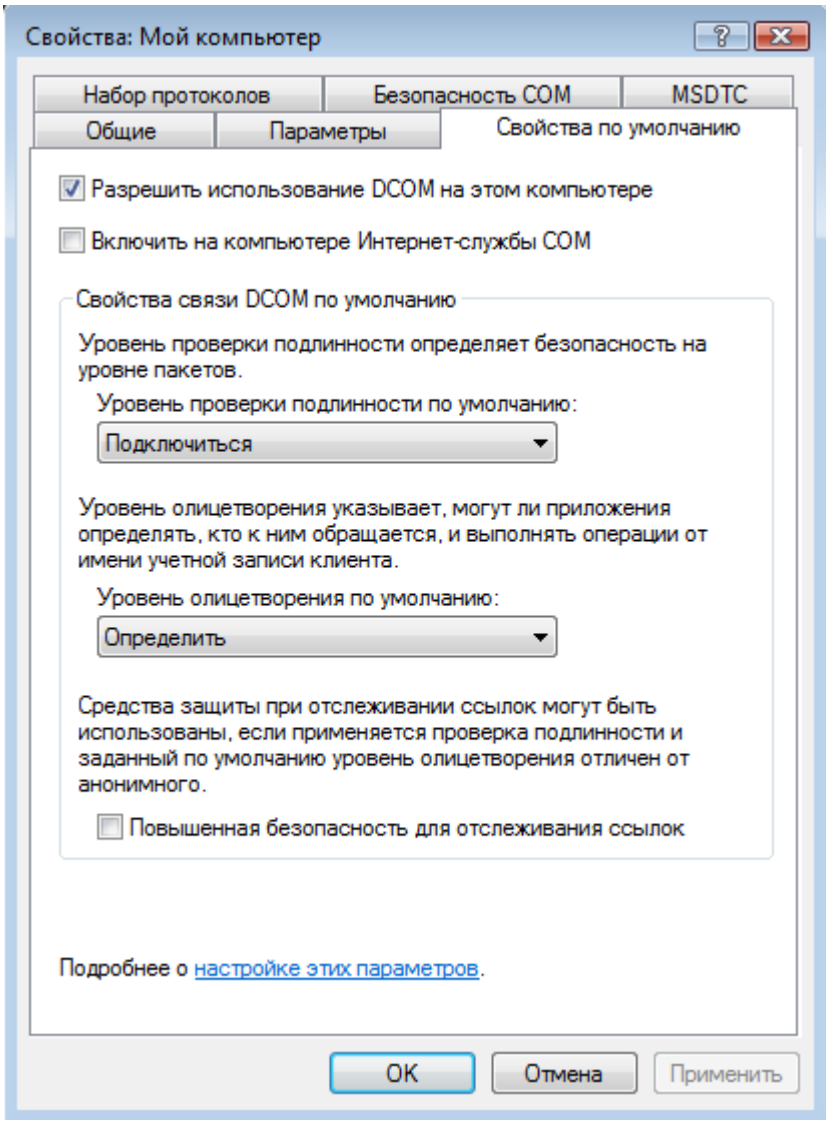

Рисунок 14 — Окно **Свойства: Мой компьютер** вкладка **Свойства по умолчанию**.

- На вкладке **Набор протоколов** в поле **Протоколы DCOM** добавьте **TCP/IP с ориентацией на подключения** (рисунок 15);

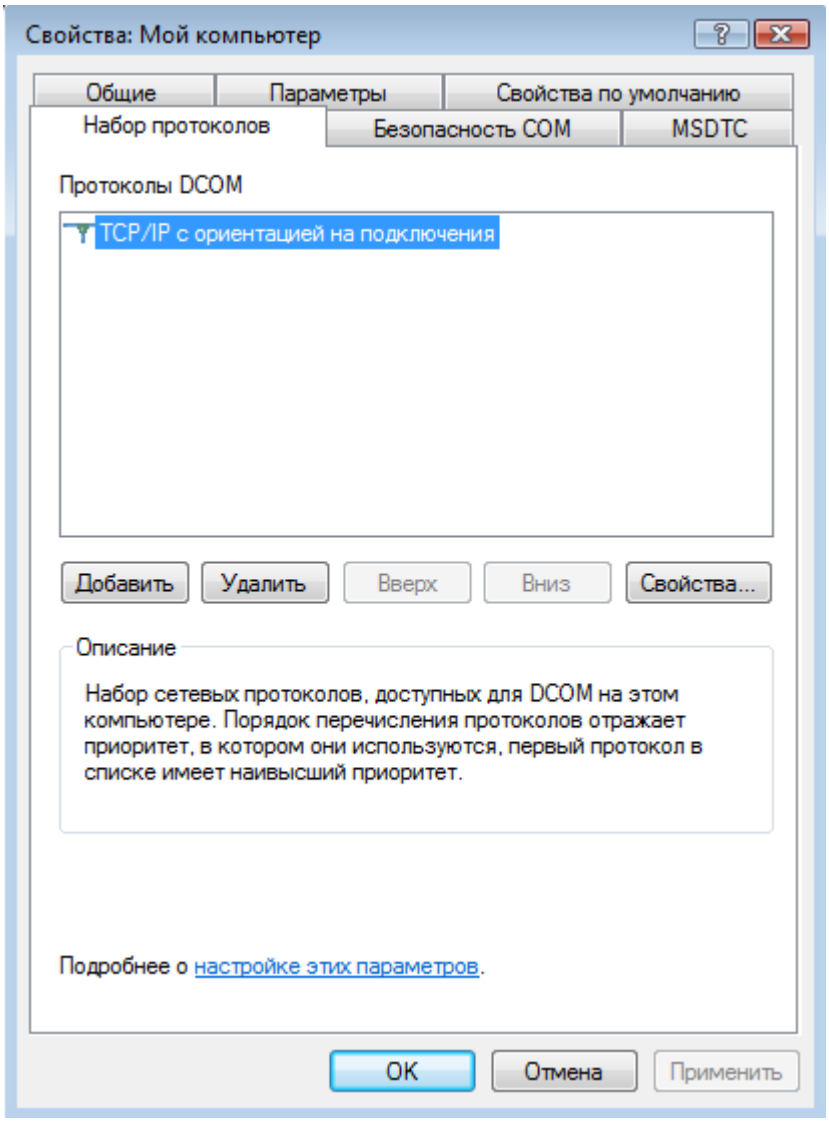

Рисунок 15 — Окно **Свойства: Мой компьютер** вкладка **Набор протоколов**

- На вкладке **Безопасность COM** в группе **Права доступа** нажмите на кнопку **Изменить ограничения** и в открывшемся окне в поле **Группы и пользователи** выберите **Все** и установите разрешения на все действия (рисунок 16). Нажмите на кнопку **ОК**;

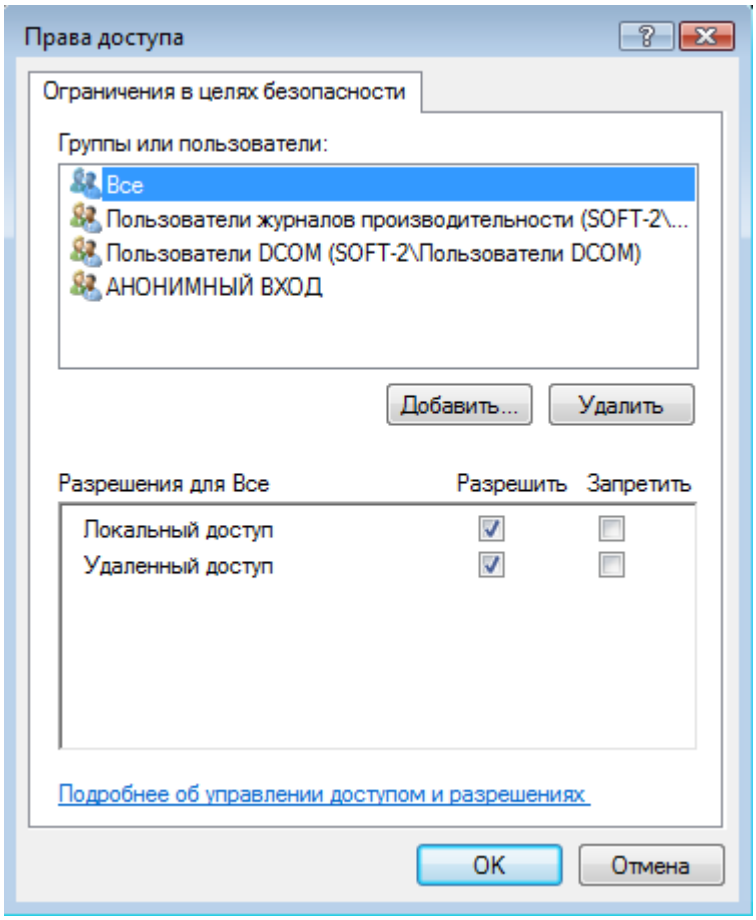

Рисунок 16 — Окно **Права доступа**

- На вкладке **Безопасность COM** в группе **Разрешения на запуск и активацию** нажмите на кнопку **Изменить ограничения** и в открывшемся окне в поле **Группы и пользователи** выберите **Все** и установите разрешения на все действия (рисунок 17). Нажмите на кнопку **ОК**;

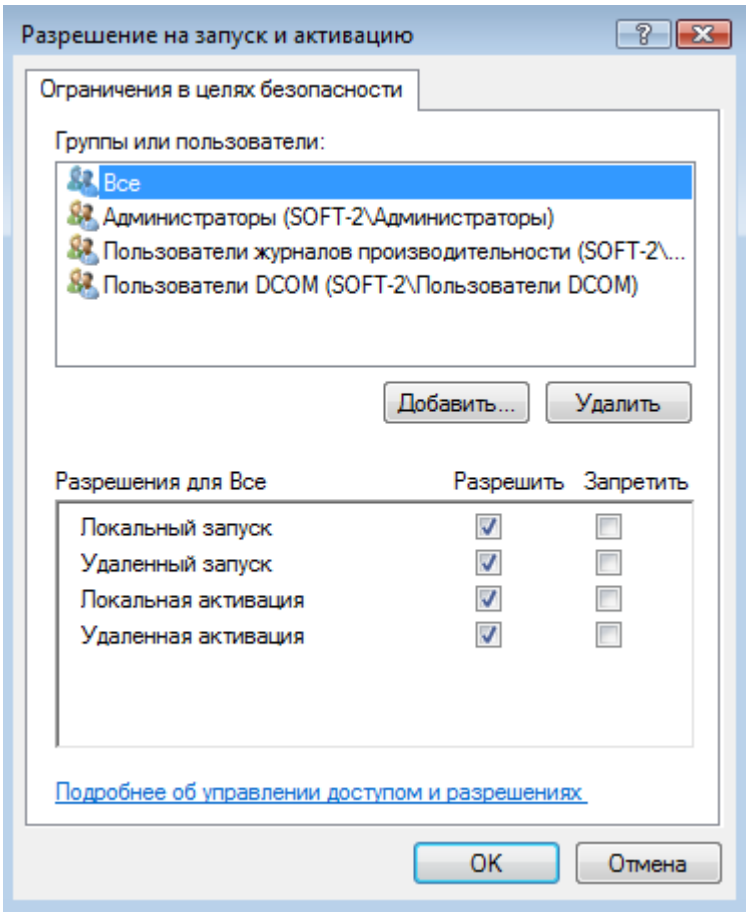

Рисунок 17 — окно Разрешение на запуск и активацию

4.4 Настройка Брандмауэра Windows

Чтобы включить брандмауэр Windows 7, выполните следующие действия:

1. Откройте **Панель управления** (см. раздел Отключение Брандмауэра Windows).
2. Слева выберите пункт **Включение и отключение брандмауэра Windows** (рисунок 18).

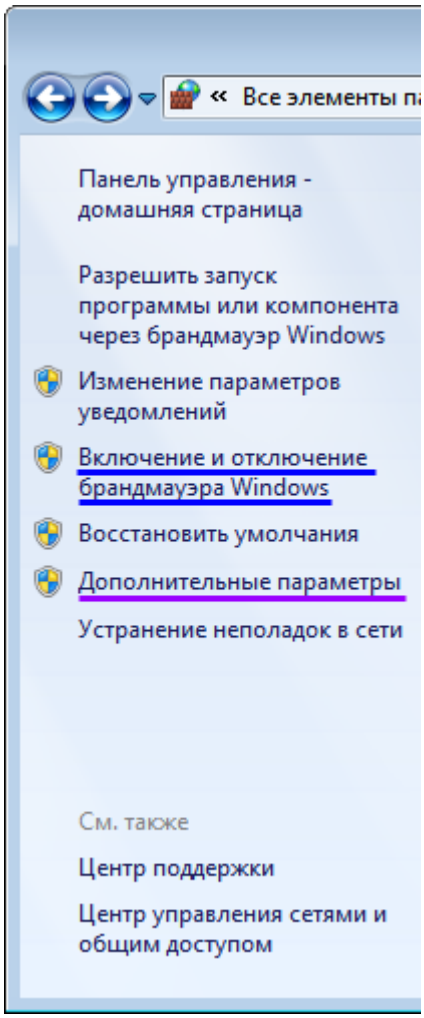

Рисунок 18 — Окно **Настройка параметров для каждого типа сети**

3. В окне **Настройка параметров для каждого типа сети** (рисунок 19) выберите **Включение брандмауэра Windows** под каждым сетевым размещением, которое следует защитить, и нажмите кнопку **ОК**.

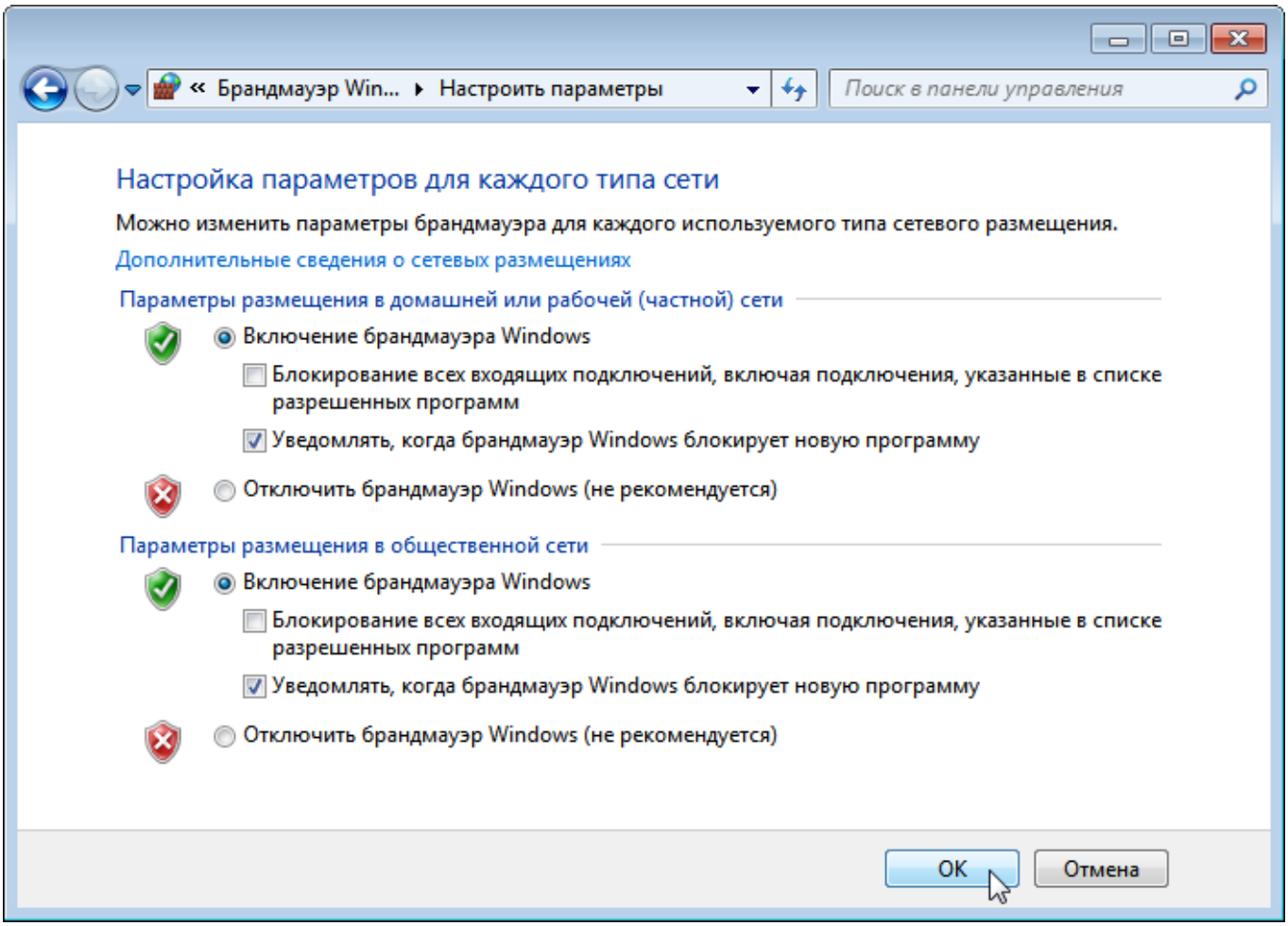

Рисунок 19 — Окно **Настройка параметров для каждого типа сети**

Добавьте в исключения все OPC-сервера и все OPC-клиенты:

OpcDbGateway.exe (OPC-сервер и OPC-клиент),
OpcDbGatewayConfigurator.exe (OPC-клиент),
SNMPRuntime.exe (OPC-сервер),
SNMPConf.exe (OPC-клиент),
OPCSimRuntime.exe (OPC-сервер)
OPCAdapter.exe (OPC-клиент),
OPCAdapterService.exe (OPC-клиент);

Для этого выберите пункт **Дополнительные параметры** (см. рисунок в пункте 2). Добавьте в папки **Правила для входящих подключений** и **Правила для исходящего подключения** требуемые правила. Для этого в разделе **Действия** воспользуйтесь командой **Создать правило...** (рисунок 20).

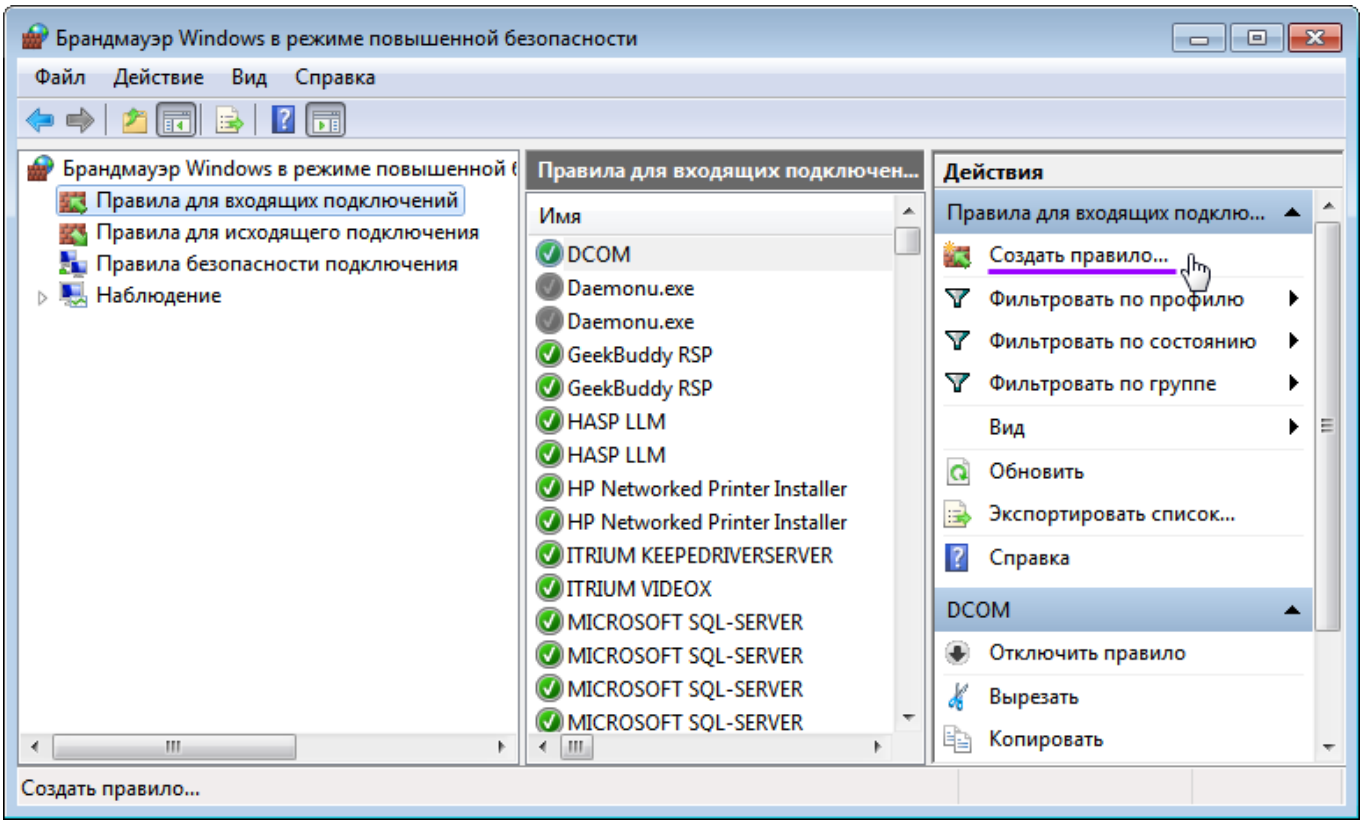

Рисунок 20 — Окно **Настройка параметров для каждого типа сети**

Создайте правило для порта 135, для этого:

1. В разделе **Действия** окна **Брандмауэр Windows в режиме повышенной безопасности** выберите команду **Создать правило...**

2. В окне мастера создания правила выберите **Тип правила** – **Для порта**, нажмите на кнопку **Далее**.

3. В следующем окне мастера (**Шаг: Протокол и порты**) выберите **Протокол TCP**, в поле **Определенные локальные порты** введите значение **135** (рисунок 21). Нажмите на кнопку **Далее**.

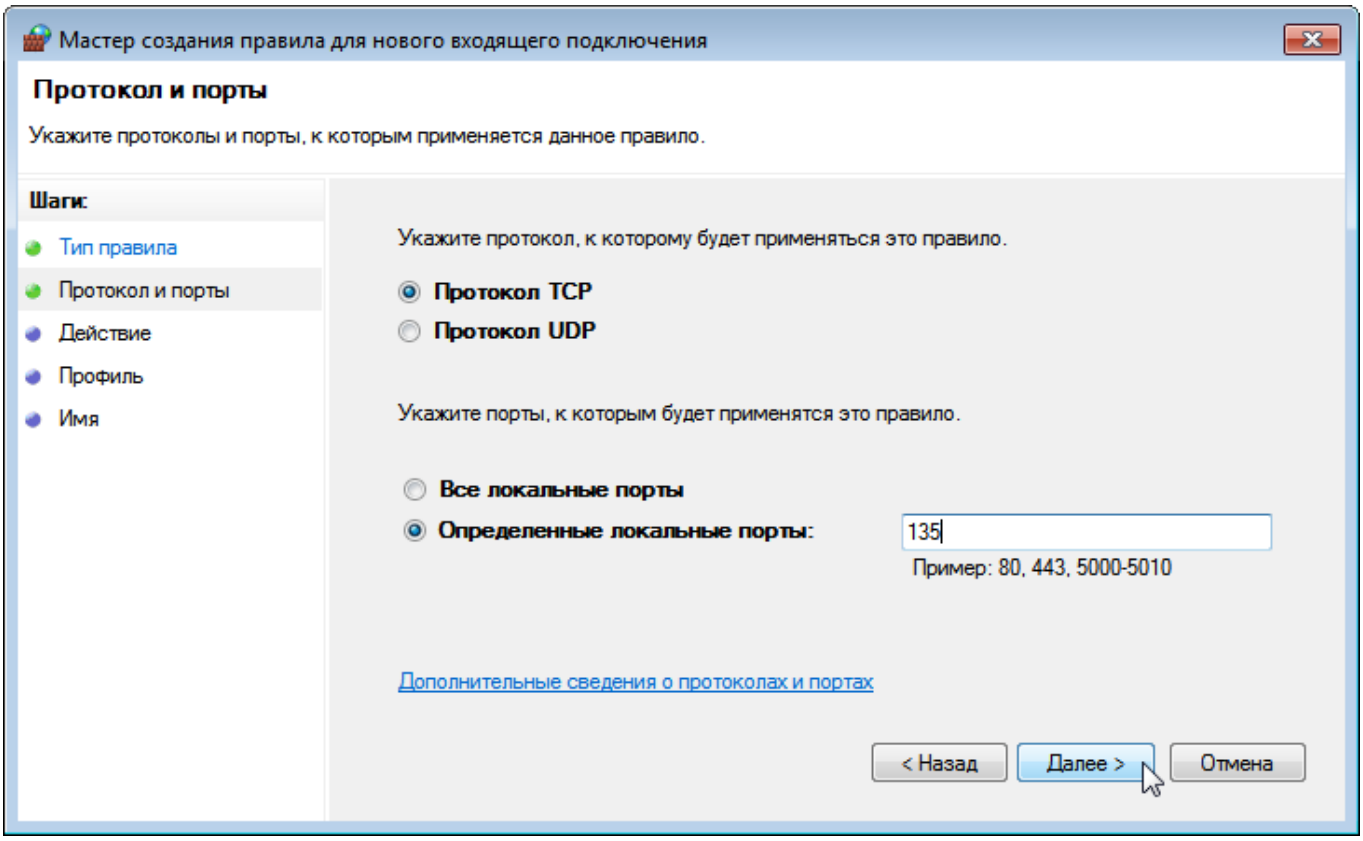

Рисунок 21 — Окно **Добавление порта**

4. На страницах шагов **Действие** и **Профиль** задайте требуемые настройки. Нажмите на кнопку **Далее**.
5. На шаге **Имя** укажите имя правила - **DCOM**. Нажмите на кнопку **Готово**.

Закройте окно **Брандмауэр Windows в режиме повышенной безопасности**.

Чтобы включить брандмауэр Windows XP, выполните следующие действия:

- В меню **Пуск** выберите пункт **Панель управления**;
- Выберите элемент **Windows Firewall**;
- Нажмите на **Изменить параметры**;
- Выберите пункт **Включить (рекомендуется)**;
- Во вкладке **Исключения** добавьте все **OPC-сервера** и все **OPC-клиенты**:

OpcDbGateway.exe (OPC-сервер и OPC-клиент),
OpcDbGatewayConfigurator.exe (OPC-клиент),
SNMPRuntime.exe (OPC-сервер),
SNMPConf.exe (OPC-клиент),
OPCSimRuntime.exe (OPC-сервер)
OPCAdapter.exe (OPC-клиент),
OPCAdapterService.exe (OPC-клиент);

- Во вкладке **Исключения** нажмите на кнопку **Добавить порт** и в открывшемся окне в поле **Имя** введите слово **DCOM**, в поле **Номер порта** введите число **135**, выберите **TCP** протокол (рисунок 22);

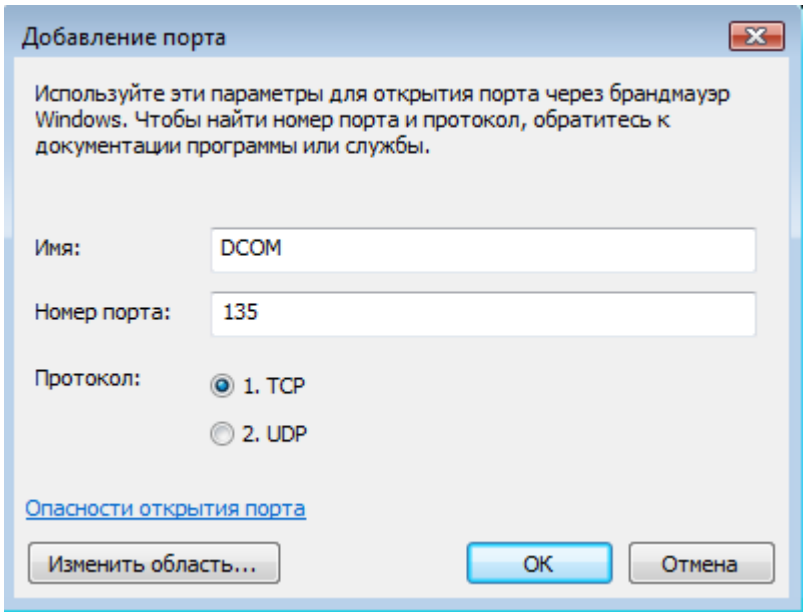

Рисунок 22 — Окно **Добавление порта**

- Нажмите на кнопку **ОК;**
- Нажмите на кнопку **Принять** и **ОК** в окне **Параметры брандмауэра Windows**.

4.5 Настройка приложения DCOM ItriumOPCServer

Запустите утилиту **DCOMCNFG** (см. раздел Настройка DCOM). Выполните следующие действия:

- В открывшемся окне **Службы компонентов** в окне слева раскройте дерево элементов, выберите элемент **Настройка DCOM**, в окне по центру выделите элемент **ItriumOPCServer** (рисунок 23).

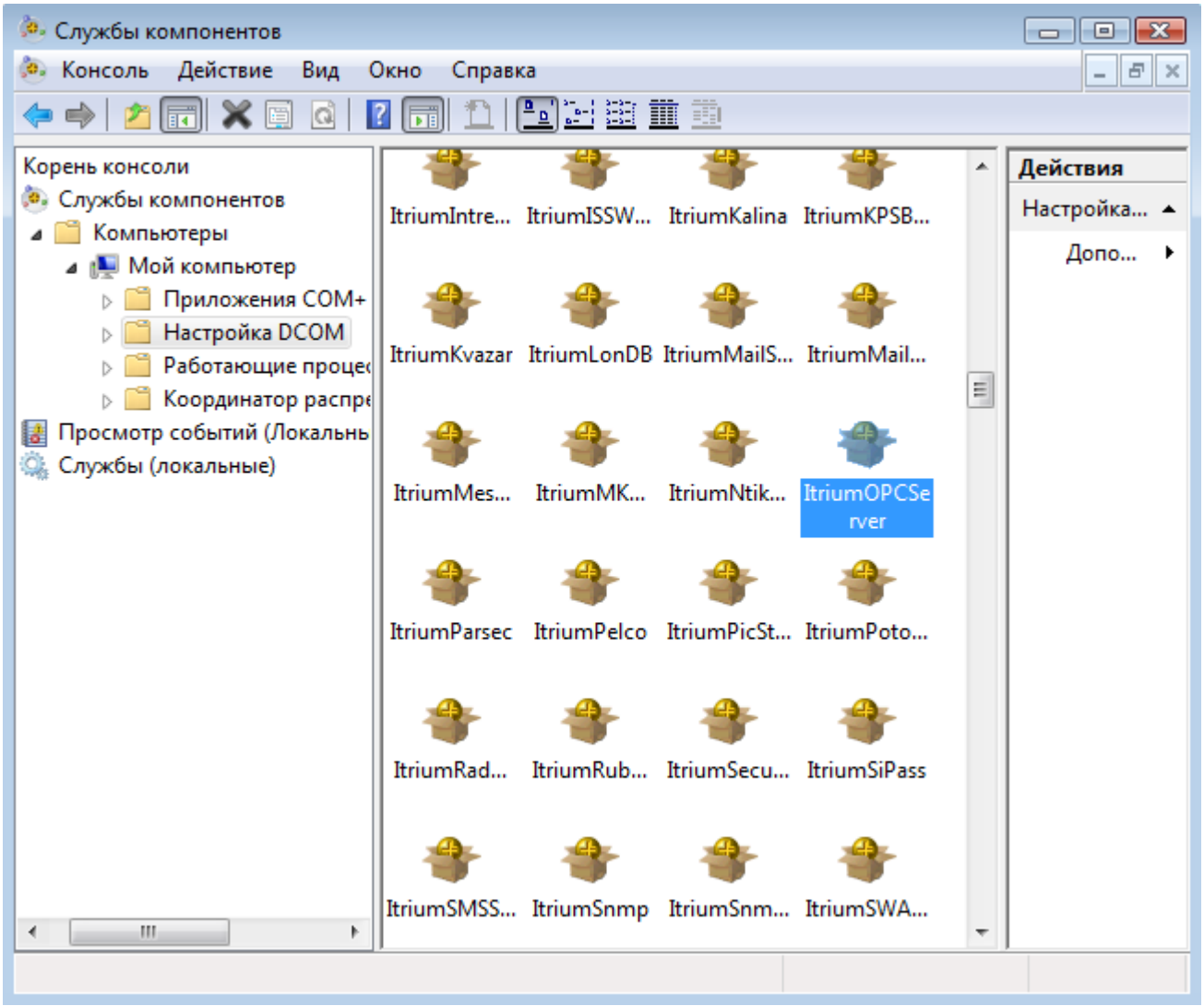

Рисунок 23 — Окно **Службы компонентов**, список компонентов

- Вызовите контекстное меню элемента **ItriumOPCServer** щелчком правой клавиши мыши и выберите **Свойства**;
- В открывшемся окне во вкладке **Общие** в раскрывающемся списке **Уровень проверки подлинности** выберите **По умолчанию**;
- Во вкладке **Удостоверение** выберите пункт **Указанный пользователь** в поле **Пользователь** введите имя созданного пользователя, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение** (рисунок 24).

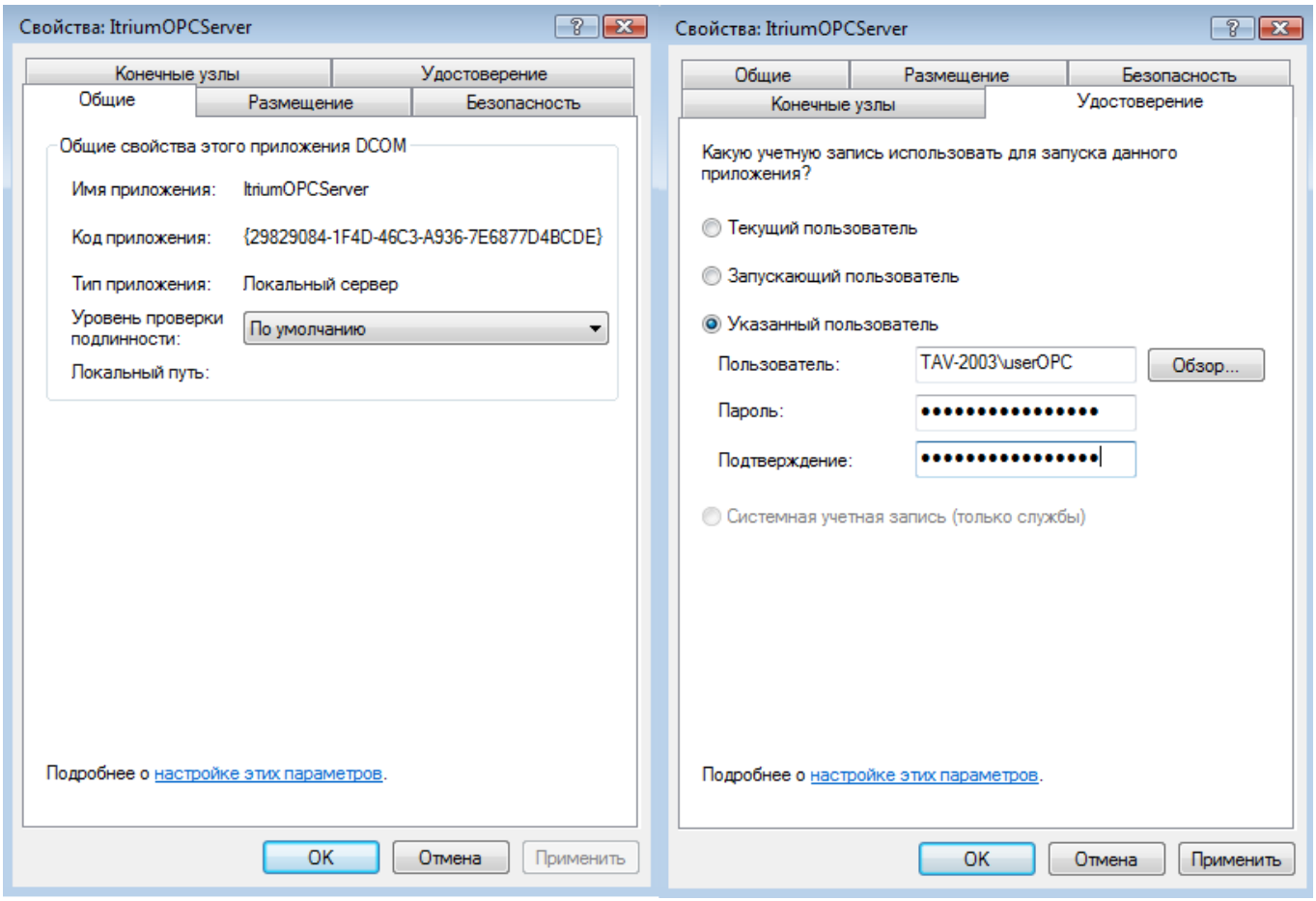

Рисунок 24 — Окно **Свойства: ItriumOPCServer**, вкладка **Общие** и **Удостоверение**

- Во вкладке **Безопасность** в группе **Права доступа** выберите пункт **Настроить** (рисунок 25), нажмите на кнопку **Изменить...** и в открывшемся окне в поле **Безопасность** выберите **Администраторы**. Нажмите на кнопку **ОК**. В группе **Разрешения на настройку** также выберите пункт **Настроить**, нажмите на кнопку **Изменить...** и в открывшемся окне в поле **Безопасность** выберите **Администраторы**. Нажмите на кнопку **ОК**.

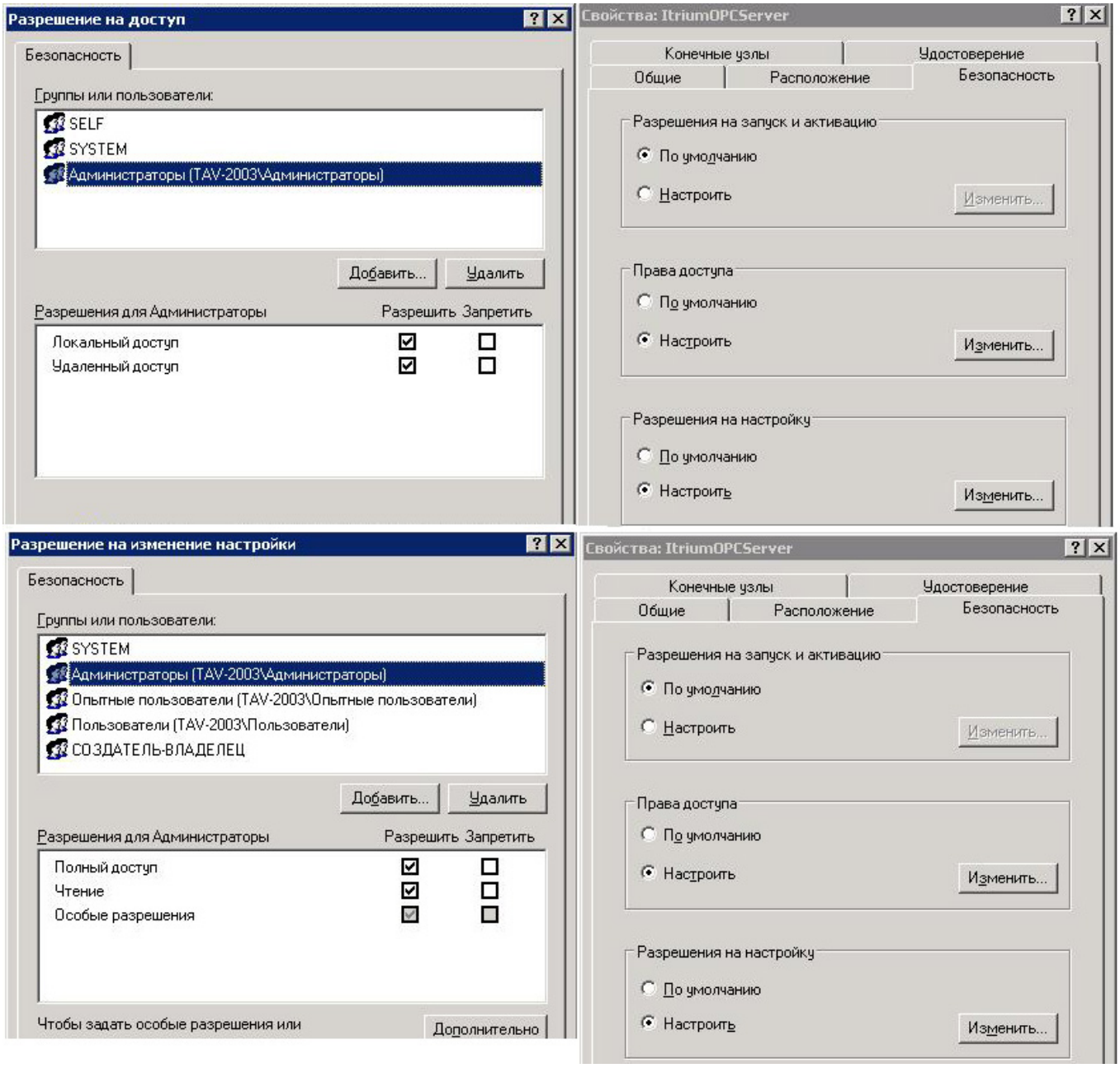

Рисунок 25 — Окно **Свойства: ItriumOPCServer**, вкладка **Безопасность**

4.6 Настройка службы OpcEnum

Запустите оснастку **Службы Консоли управления Microsoft** с помощью утилиты **services.msc**. Для этого:

- В меню **Пуск** выберите команду **Выполнить...**, введите название утилиты **services.msc** и нажмите на кнопку **OK** (если команда **Выполнить...** не отображается, введите **services.msc** в строке поиска и запустите утилиту).
- В открывшемся окне **Службы** в списке служб выберите элемент **OpcEnum.**

- Откройте контекстное меню элемента **OpcEnum** щелчком правой клавиши мыши и выберите пункт **Свойства**. Но вкладке **Вход в систему** (рисунок 26) выберите значение **С учетной записью**, введите имя пользователя. В полях **Пароль** и **Подтверждение** введите пароль. Нажмите на кнопку **Применить** и **ОК**.

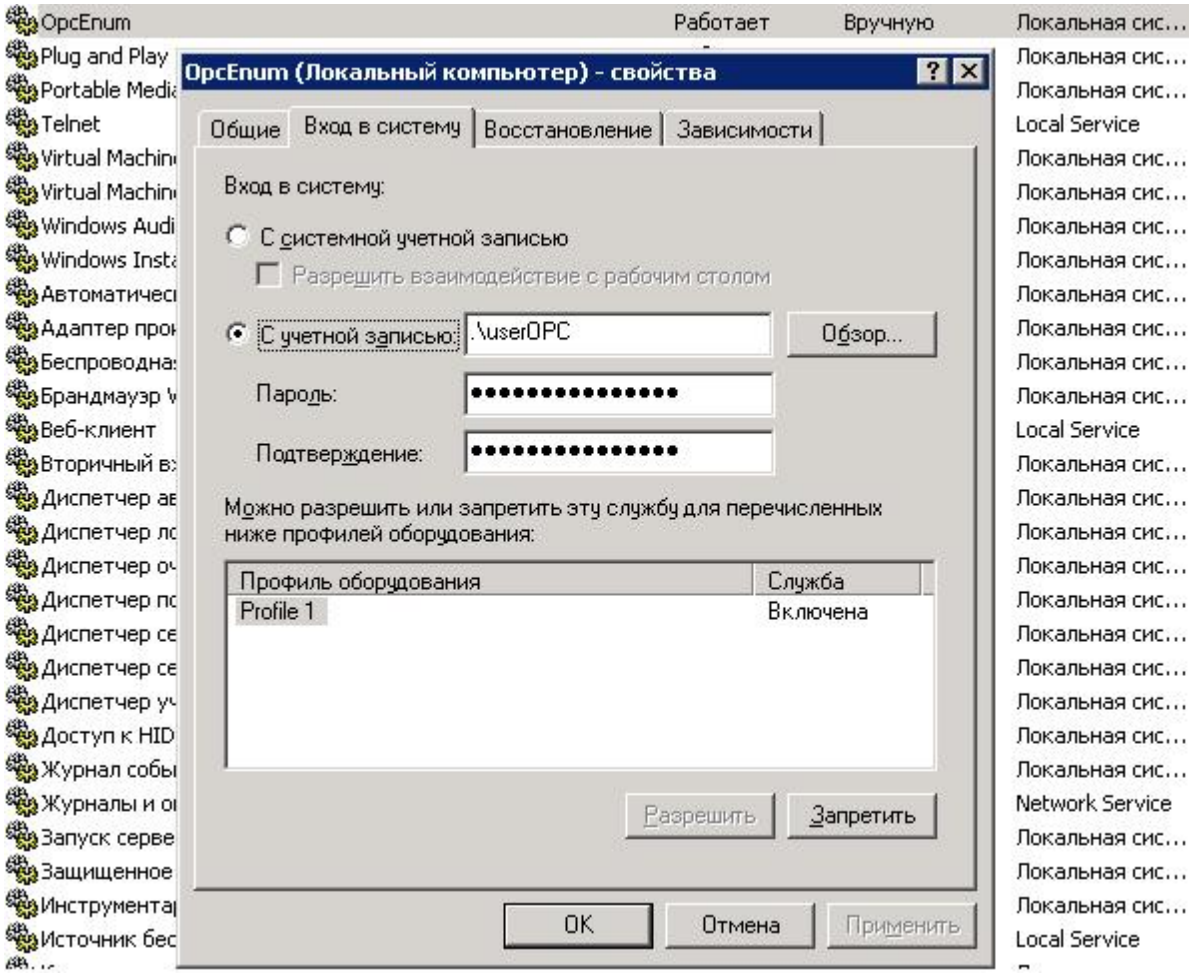

Рисунок 26 — Окно **OpcEnum (Локальный компьютер) - свойства**

4.7 Настройка Драйвера OPC

В программе «Администратор системы»:

1. В дереве элементов в выберите элемент **Компьютер**, на котором необходимо настроить SCADA систему, и добавьте к нему элемент **Драйвер OPC-сервера**;
2. К элементу **Драйвер OPC-сервера** добавьте элемент **OPC-сервер**;
3. В частных свойствах элемента OPC-сервер выполните следующие настройки (рисунок 27):
   - В раскрывающемся списке **DA OPC Сервер (ProgID)** выберите **ItriumOPCServer.DA.1**;
   - В поле **Имя удаленного компьютера** введите ip-адрес компьютера;
   - В поле **Пользователь** введите имя созданного нового пользователя (см. пункт 1 раздела Настройка работы SCADA-системы через DCOM);
   - В поле **Домен** введите имя компьютера;
   - В поле **Пароль** введите пароль;
   - В раскрывающемся списке **Способ аутентификации** выберите **RPC_C_AUTHN_WINNT**;
   - В раскрывающемся списке **Способ авторизации** выберите **RPC_C_AUTHZ_NAME**;
   - В раскрывающемся списке **Уровень доверия** выберите **RPC_C_IMP_LEVEL_IMPERSONATE**.
4. Нажмите на кнопку Сохранить  .

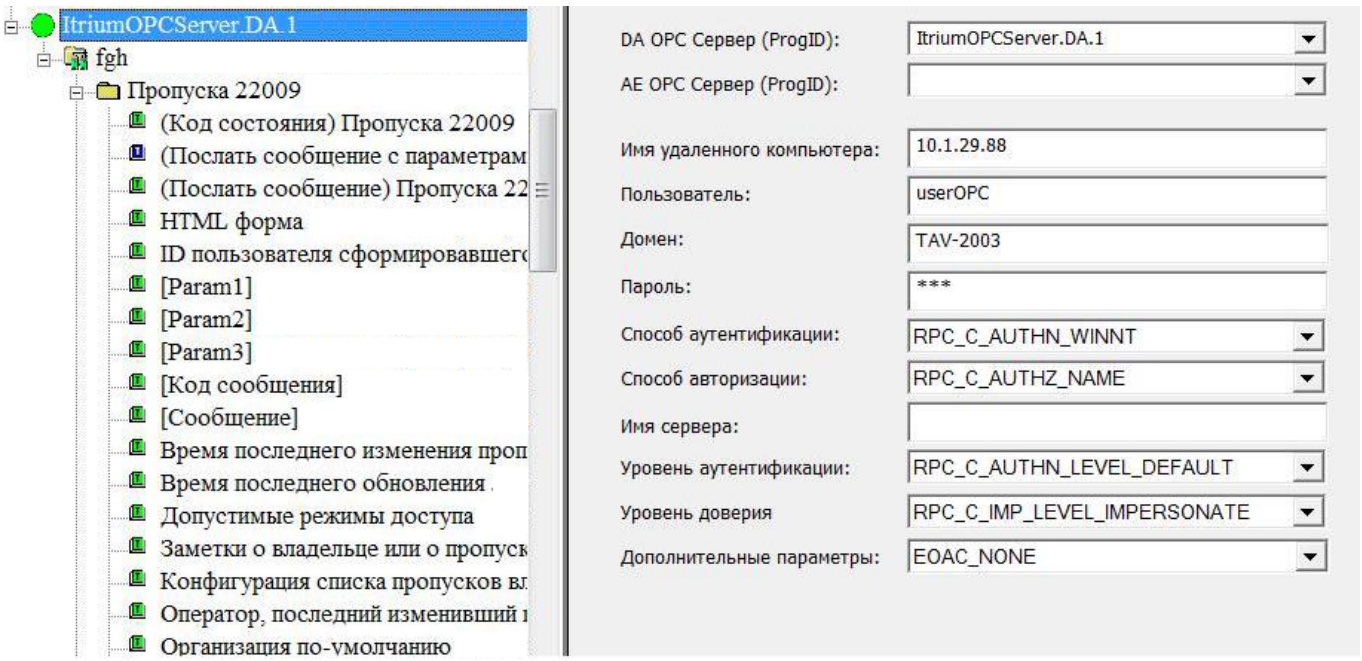

Рисунок 27 — Частные свойства элемента **OPC-сервер**

5 Пример работы Драйвера со SCADA-системой

Рассмотрим простейший пример применения **Драйвера SCADA**. Пусть требуется осуществлять мониторинг состояния зонами (например, **Драйвера ИСО Орион (Болид)**) и управлять ими из SCADA-системы. Для этого:

1. В программе «Администратор системы» к элементу **Компьютер** добавьте **Драйвер ИСО Орион (Болид)** и сконфигурируйте его дочерние элементы. Подробно о конфигурировании драйвера см. установочный диск ITRIUM®, раздел **Документация — Драйверы — Драйвер ИСО Орион (Болид)**.

2. Добавьте **Драйвер SCADA** и запустите его (см. раздел Добавление элемента Драйвер SCADA).

3. К элементу **Драйвер SCADA** добавьте ссылки на элементы **Зона ИСО Орион (Болид)** (см. раздел Добавление ссылки на элемент системы безопасности).

4. Запустите программу для настройки SCADA-системы (например, **TRACE MODE**).

5. В данной программе подключитесь к OPC-серверу **ItriumOPCServer** и добавьте переменные (теги), соответствующие свойствам элемента **Зона ИСО Орион (Болид)** (рисунок 28).

☑ **Примечание**: Список свойств каждого элемента в ПО ITRIUM® можно посмотреть, выделив данный элемент и нажав на кнопку  на панели инструментов программы «Администратор системы». Все свойства, кроме строкового представления состояния элемента, доступны как для чтения, так и для записи (read-write).

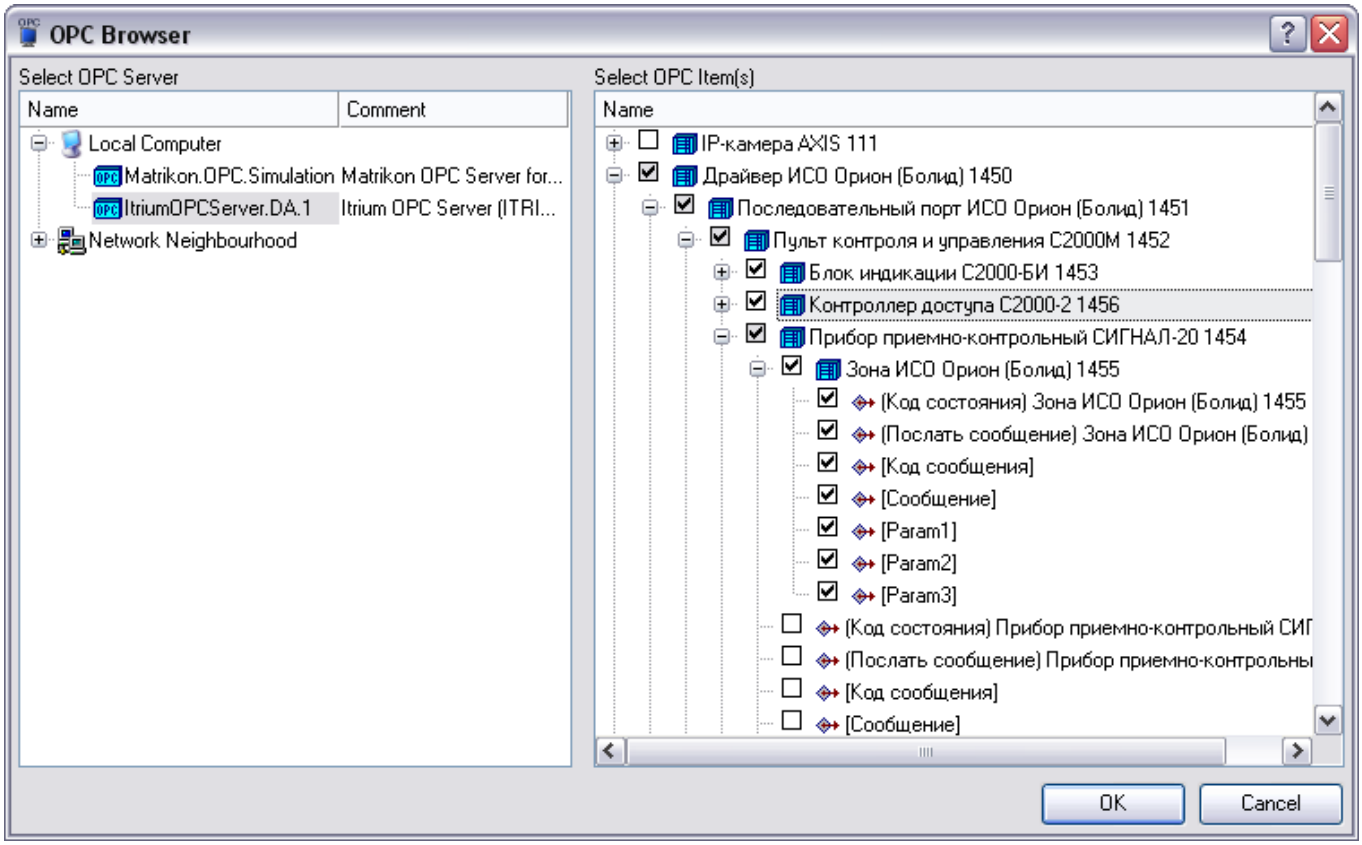

Рисунок 28 — Добавление OPC-сервера **ItriumOPCServer** и тегов в SCADA систему. Программа **TRACE MODE 6**

6. После этого появляется возможность наблюдать изменения состояний и свойств выбранных элементов, передавать сообщение элементам из ПО ITRIUM® в OPC-клиент, а также изменять состояния и свойства и отправлять сообщения элементам из OPC-клиента.

☑ **Примечание**: В SCADA-системе теги, которые предназначены для посылания команды или сообщение (например, тег с префиксом (Послать сообщение)), должны иметь направление "Output".

☑ **Примечание**: Подробная инструкция по настройке SCADA-системы см. в соответствующем руководстве пользователя.

6 Представление элемента переменными

OPC-сервер **ItriumOPCServer** представляет свойства элемента и сообщения от него переменными (тегами). В ПО ITRIUM® свойства элемента можно посмотреть, выделив данный элемент и нажав на кнопку **Показать свойства** на панели инструментов программы «Администратор системы». Все свойства, кроме строкового представления состояния элемента и параметров сообщения от элемента, доступны как для чтения, так и для записи (read-write).

Приведем **пример представления элемента тегами:**

Для элемента **Элемент 1** со свойствами **Свойство 1, Свойство 2** будут сформированы следующие теги (в угловых скобках пояснение и права доступа: **R** - чтение, **W** - запись; формат представления: **Имя тега** = **Значение тега**):

<тег R> Элемент 1 = "Потеряна связь"

<папка> Элемент 1

--- <тег RW> (Код состояния) Элемент 1 = 4

--- <тег RW> (Послать сообщение) Элемент 1 = 0

--- <тег R> [Код сообщения] Элемент 1 = 0

--- <тег R> [Сообщение] Элемент 1 = 0

--- <тег R> [Param1] Элемент 1 = 1244

--- <тег R> [Param2] Элемент 1 = 0

--- <тег R> [Param3] Элемент 1 = "message"

--- <тег RW> Свойство 1 = 555

--- <тег RW> Свойство 2 = "qwe"

Теги **(Код состояния), (Послать сообщение), [Param1], [Param2], [Param3], [Код сообщения], [Сообщение]** являются обязательными и отображаются для любого элемента. Теги **Свойство 1, Свойство 2,..., Свойство N** являются необязательными и отображаются только при наличии дополнительных свойств у элемента в ПО ITRIUM®.

Записав числовое значение в тег с префиксом **(Код состояния)**, можно изменить состояние элемента. Записав числовое значение в тег с префиксом **(Послать сообщение)**, можно отправить элементу сообщение. Записав значение в остальные RW-теги можно изменять соответствующие свойства элемента. Тег с названием элемента содержит строковое представление кода состояния элемента. Теги **[Param1], [Param2], [Param3], [Код сообщения]** и **[Сообщение]** отображают сообщения, возникающие от элемента в ПО ITRIUM®.

Список сообщений, которые оператор может подавать элементу (команд), можно просмотреть с контекстном меню элемента, в программе «Администратор системы». Список сообщений, источником которых является элемент, указаны во вкладке **Сообщения** (которая вызывается нажатием кнопки  на панели инструментов). На рисунке 29 представлен список команд, которые оператор может подать элементу **Зона**.

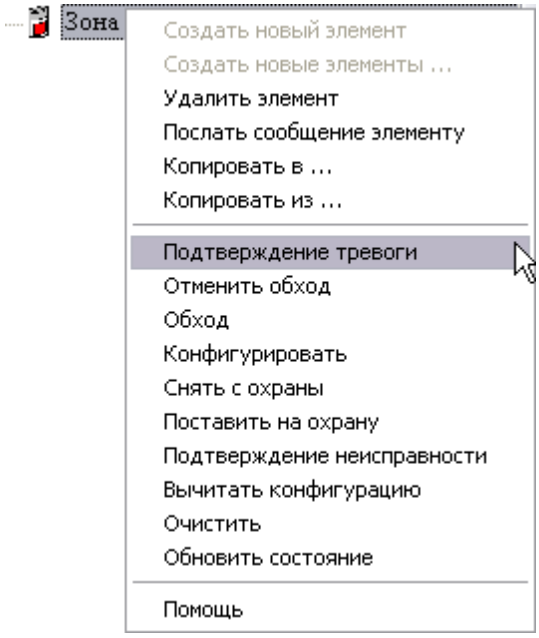

Рисунок 29 — Команды элемента Зона

Чтобы узнать код, соответствующий какой-либо команде (сообщению), необходимо подать данную команду элементу (инициировать приход сообщения). Затем, в списке событий, которое находится в нижней части окна программы «Администратор системы», выбрать данную команду(сообщение), и в ее контекстном меню выбрать пункт **Подробнее...** (рисунок 30).

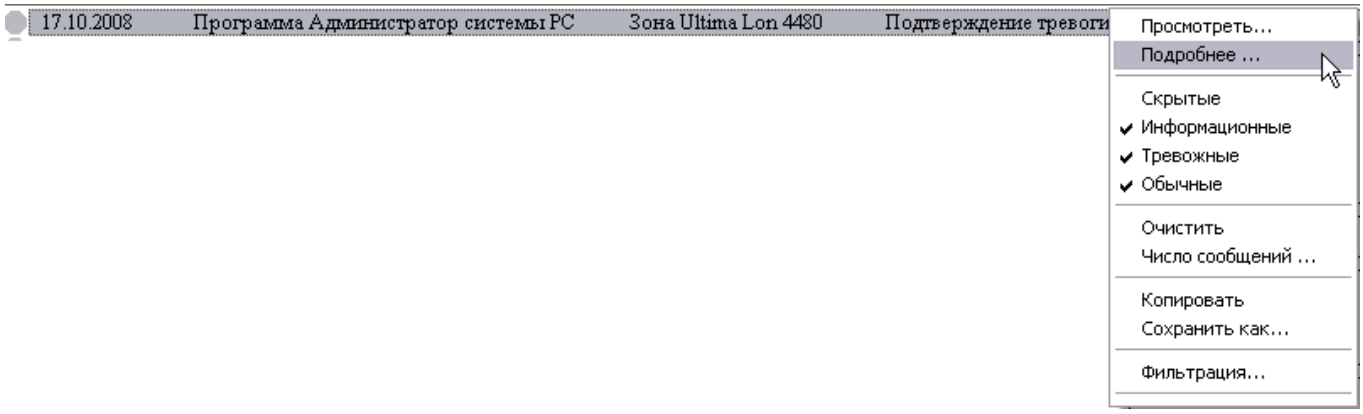

Рисунок 30 — Контекстное меню команды **Подтверждение тревоги**

Затем, в открывшемся окне **Описание сообщения** нажать на кнопку **Подробнее**. В разделе **Описание** появится идентификатор сообщения и дополнительные параметры, которые описывают данную команду (сообщение).

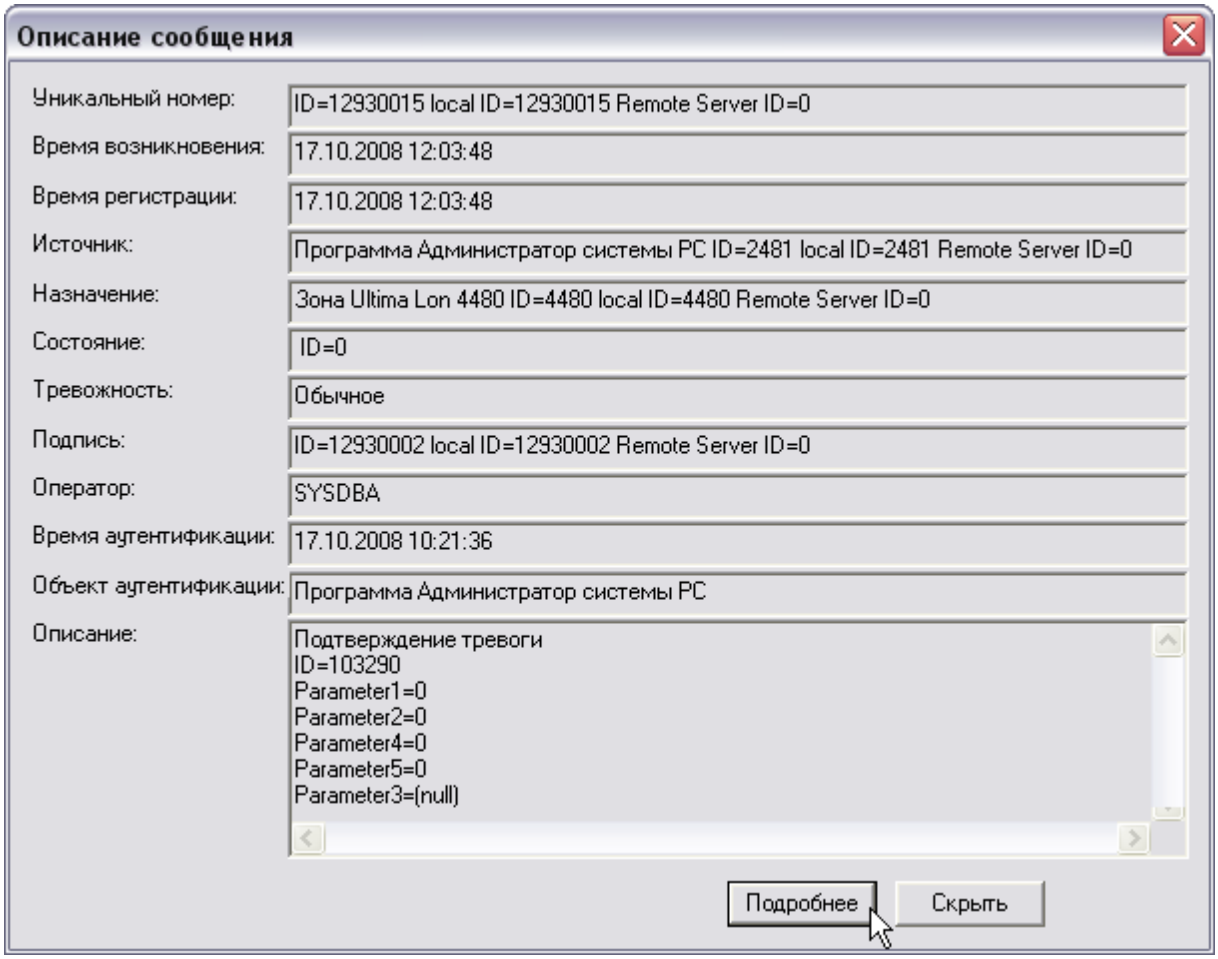

Рисунок 31 — Окно Описание сообщения команды «Подтверждение тревоги»

На рисунке 31 представлено описание команды **Подтверждение тревоги**, из которого видно, что для того, чтобы послать данную команду элементу, необходимо ввести в тег с префиксом **(Послать сообщение)** значение **103290**.

Параметры формирования тегов:

На странице частных свойств элемента **Драйвер SCADA** можно задать параметры формирования тегов. Для этого:

1. Откройте страницу частных свойств элемента **Драйвер SCADA** помощью кнопки **Частные свойства** на Панели инструментов.
2. На вкладке **Параметры драйвера OPC** (рисунок 32):

- **Транслитерировать теги и заменять следующие символы символом подчеркивания** – Установите флажок, если требуется заменить символы русского алфавита на символы английского алфавита при помощи транслитерации. Если флажок не установлен. теги будут иметь префикс, указанный слева (в скобках) в разделе **Формировать теги**. Если флажок установлен, теги будут иметь префикс, указанный справа в разделе **Формировать теги.**
  В поле ниже введите символы, которые по требованию OPC-клиента должны быть заменены символом подчеркивания;

- **Формировать теги** – По умолчанию формируется полный набор тегов. При необходимости ограничить набор формируемых тегов снимите флажки для тех тегов, которые не должны быть предоставлены OPC-клиенту.

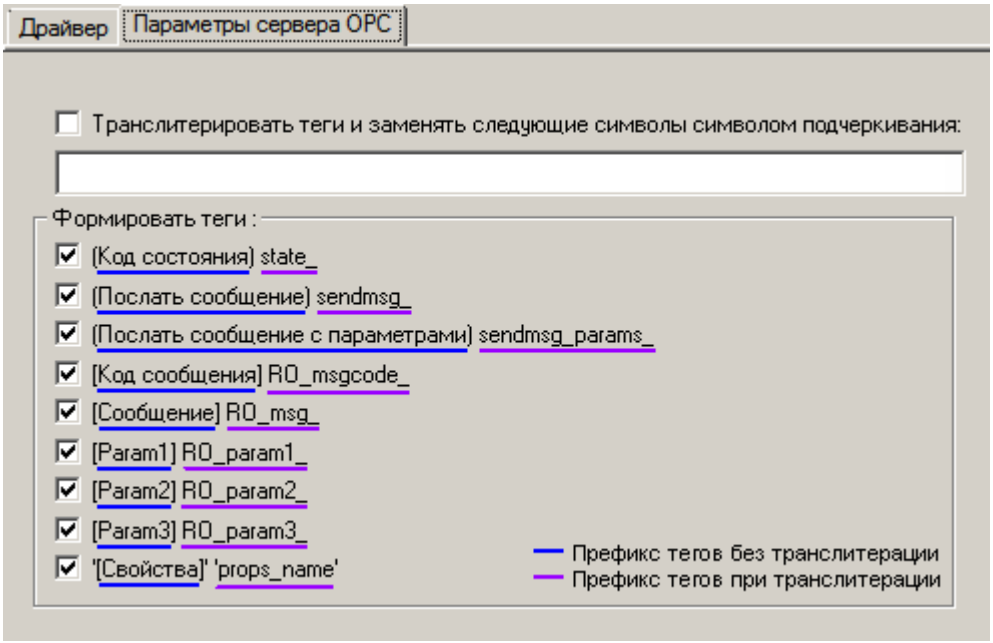

Рисунок 32 — Окно частных свойств элемента **Драйвер SCADA**. Вкладка **Параметры сервера OPC**

ООО «ИТРИУМ СПб»

194100, Санкт-Петербург, ул. Харченко, д. 5, Литер А.
interop@itrium.ru
www.itrium.ru