СИСТЕМА КОНТРОЛЯ
И УПРАВЛЕНИЯ ДОСТУПОМ
PERCo-SYS-15000

Руководство администратора

СОДЕРЖАНИЕ

ВВЕДЕНИЕ **2**
1. ПОРЯДОК ПОДГОТОВКИ СИСТЕМЫ К РАБОТЕ **2**
2. ИНСТАЛЛЯЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ **3**
2.1. Инсталляция базового пакета программного обеспечения 3
2.1. Инсталляция модуля «Сервер аппаратуры серии 600» 4
2.2. Инсталляция модуля «Сервер аппаратуры серии 12000» 4
3. НАСТРОЙКА КЛЮЧЕЙ ЗАЩИТЫ GUARDANT **5**
3.1. Настройка драйвера GUARDANT (LPT) 5
3.2. Проверка работоспособности локальных ключей защиты 8
3.3 Настройка сетевых ключей защиты GUARDANT (Net) 9
4. НАСТРОЙКА DCOM **11**
4.1. Настройка DCOM в операционной системе Windows 2000 11
4.2. Настройка DCOM в операционной системе Windows XP 18
4.3. Настройка DCOM в операционной системе Windows Server 2003 26
4.4.Настройка DCOM на Microsoft Windows XP SP2 26
5. НАСТРОЙКА БАЗЫ ДАННЫХ **33**
5.1. Создание файла базы данных 33
5.2. Работа с консолью администратора БД 36
5.3. Выбор места расположения резервных копий базы данных 36
5.4. Резервное копирование базы данных 38
5.5. Восстановление базы данных из резервной копии 38
5.6. Удаление из БД данных по мониторингу 38
5.7. Удаление из БД данных о проходах 39
5.8. Удаление событий и кадров видеоидентификации 39
5.9. Работа с сохраненными в архиве данными о проходах и данными мониторинга 40
5.10.Оптимизация индексов базы данных 40
5.11. Очистка кэша конфигурации базы данных 40
5.12. Дополнительные настройки базы данных 40
6. Задание прав доступа пользователей к подразделам программного обеспечения системы 43
6.1. Формирование групп доступа к подразделам программного обеспечения 43
6.2. Ввод, редактирование и удаление данных о пользователях 45
6.3. Задание прав доступа к разделам программного обеспечения 47
6.4. Задание прав доступа к подразделениям 47
7. НАСТРОЙКА СЕРВЕРА СИСТЕМЫ **48**
7.1. Задание компьютера, на котором установлен сервер управления данными 48
7.2. Задание компьютеров, на которых установлены серверы аппаратуры 50
7.3. Включение и отключение серверов аппаратуры 50
7.4. Изменение места расположения аппаратуры 51
7.5. Удаление сервера аппаратуры 51
8. КОНФИГУРИРОВАНИЕ СИСТЕМЫ **52**
8.1. Автоматизированное определение аппаратного состава системы 52
8.2. Задание параметров работы подключенных устройств 53
8.3. Формирование дерева объектов доступа 57
8.4. Формирование точек доступа 58
8.5. Установление связи между подключенным оборудованием и объектами доступа 61
8.6. Задание диапазонов карт доступа 62
9. УДАЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ **63**
9.1. Удаление базового пакета программного обеспечения 63
9.2. Удаление модуля «Сервер аппаратуры 600» 65
9.3. Удаление модуля «Сервер аппаратуры серии 12000» 66
ПРИЛОЖЕНИЕ 1 ..... **67**
ПРИЛОЖЕНИЕ 2 ..... **73**

ВВЕДЕНИЕ

Система контроля и управления доступом PERCo-SYS-15000 с бесконтактными пластиковыми картами в качестве пропусков и ключей (далее — система) предназначена для обеспечения безопасности объектов, повышения контроля трудовой дисциплины и автоматизации учета рабочего времени на предприятии.

Данное руководство предназначено для администраторов системы. В него включены следующие описания:

- инсталляция программного обеспечения
- особенности работы с программным обеспечением
- порядок подготовки системы к работе
- задание первоначальных установок функционирования системы
- задание прав доступа пользователей к программному обеспечению системы
- настройка сервера системы
- запуск программы «Консоль управления»
- работа с сервером системы

Перед началом работы администратору системы рекомендуется ознакомиться с техническими описаниями подсистем контроллеров, входящими в комплект документации.

1. ПОРЯДОК ПОДГОТОВКИ СИСТЕМЫ К РАБОТЕ

Для того чтобы осуществить подготовку системы к работе, необходимо выполнить следующие действия:

1) Выбрать компьютеры, где будет подключена аппаратура системы, и будут работать модули «Сервер аппаратуры серии 600» и/или «Сервер аппаратуры серии 12000»;
2) Выбрать компьютер, на котором будет работать модуль «Сервер управления данными»;
3) Выбрать компьютер, на котором будет работать сервер БД FireBird;
4) Выбрать компьютер, на котором будет работать модуль «Сервер системы»;
5) Провести инсталляцию ПО в соответствии с разработанной схемой;
6) Настроить DCOM;
7) Вставить ключ защиты с маркировкой «PERCo-BS-15000» в LPT-порт компьютера, где установлен модуль «Сервер системы»;
8) Вставить ключ защиты с маркировкой «PERCo-HW-12000» в LPT-порт компьютера, где установлен модуль «Сервер аппаратуры серии 12000»;
9) Сконфигурировать ключи защиты и проверить их работоспособность;
10) Запустить модуль «Консоль администратора БД». На данном этапе осуществить подключение к серверу БД и создание базы данных;
11) Запустить модуль «Консоль управления» (для регистрации подразделов программы);
12) Задать права доступа пользователей к программному обеспечению системы. На данном этапе определить пользователей системы, задать их права доступа к подразделам программного обеспечения и присвоить им индивидуальные пароли;
13) Настроить серверы аппаратуры. При настройке серверов указать имя компьютера и COM-порт, к которому подключена аппаратура системы;
14) Провести автоконфигурацию системы, т.е. операцию по автоматическому определению состава подключенной аппаратуры с дальнейшим заданием параметров работы подключенных устройств и привязкой этих устройств к объектам доступа. Если автоконфигурация осуществляется не администратором системы, то данный пункт выполняется после задания прав доступа пользователей к программному обеспечению.

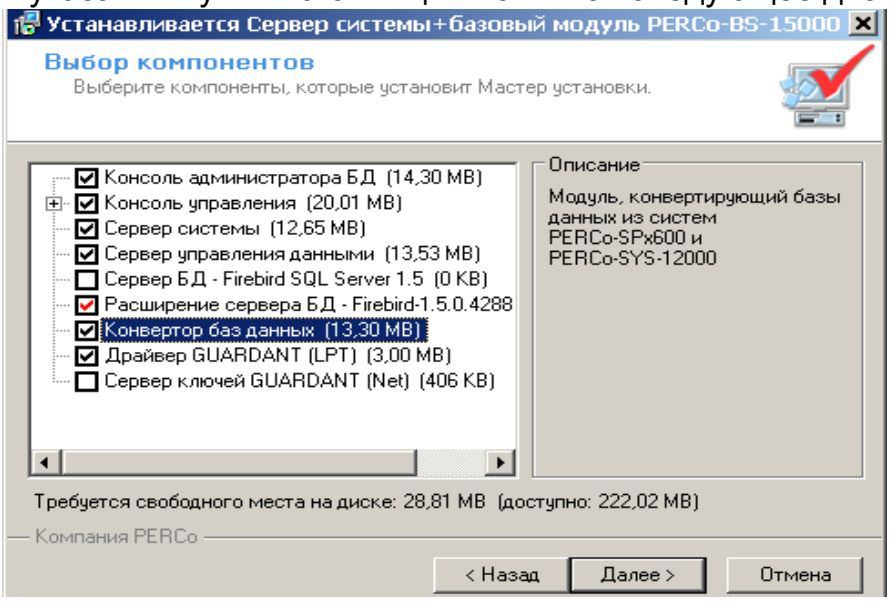
После проведения всех необходимых операций по настройке системы администратору рекомендуется задать себе пароль для входа в нее. Данная процедура необходима для установки эксклюзивного права администратора изменять настройки системы.

2. ИНСТАЛЛЯЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2.1. Инсталляция базового пакета программного обеспечения

Вставьте компакт-диск с наклейкой

в привод CD-ROM. Должен автоматически запуститься инсталляционный модуль PERCo-BS-15000.exe. Если этого не происходит — запустите данный модуль вручную. После принятия лицензионного соглашения и указания пути инсталляции появится следующее диалоговое окно:



Выберите те модули и компоненты, которые вы хотите установить на Вашем компьютере.

Модули имеют следующее назначение:

- «Консоль администратора БД» — модуль, используемый администратором БД для создания и настройки БД, а также для задания прав доступа пользователей к подразделам программного обеспечения системы
- «Консоль управления» — модуль, используемый администратором и операторами системы, состоящий из следующих компонентов:
  - «Конфигуратор» позволяет конфигурировать систему, определять объекты доступа и задавать диапазоны карт доступа
  - «Справочники доступа» предназначен для определения групп доступа и соответствующих им временных интервалов, в течение которых возможен доступ на объекты
  - «Персонал» необходим для ввода списка сотрудников с заданием каждому графика работы и занесением учетных данных. Также позволяет производить оформление пропусков
  - «Отчеты» предназначен для создания отчетов и включает подразделы «Отчет о событиях устройств» и «Дисциплина труда»
  - «Доступ на объекты» используется для выдачи постоянных и временных пропусков с назначением группы доступа
  - «Мониторинг» позволяет задавать различные режимы контроля доступом и просматривать события и информацию о них

- «Сервер системы» — модуль, отвечающий за координацию действий всей системы
- «Сервер управления данными» — модуль, отвечающий за сохранение и обработку всех данных системы
- «Сервер БД – FireBird SQL Server» — модуль, отвечающий за физическое представление и обработку данных
- «Расширение сервера БД - FireBird SQL Server» - модуль, расширяющий стандартную функциональность сервера БД - FireBird SQL Server
- «Драйвер GUARDANT (LPT)» — драйвер ключей GUARDANT для LPT-порта, используемый для работы с локальными ключами защиты
- «Сервер ключей GUARDANT (Net)» — модуль, используемый при работе с сетевыми ключами защиты
- «Конвертор баз данных» — модуль, конвертирующий базы данных из систем PERCo-S-600 и PERCo-SYS-12000

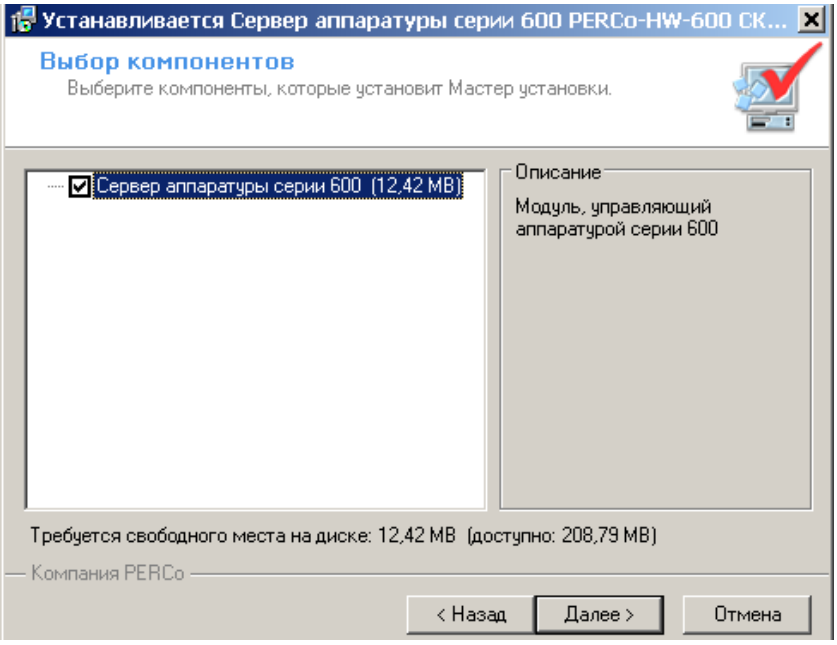
Примечание: если Вы хотите построить распределенную систему, то Вам следует инсталлировать модули базового пакета по отдельности на другие компьютеры путем повторного запуска данного инсталлятора.

Нажмите кнопку «Далее» для начала инсталляции.

2.1. Инсталляция модуля «Сервер аппаратуры серии 600»

Вставьте компакт-диск с наклейкой

в привод CD-ROM. Должен автоматически запуститься инсталляционный модуль PERCo-HW-600.exe. Если этого не происходит — запустите данный модуль вручную. После принятия лицензионного соглашения и указания пути инсталляции появится следующее диалоговое окно:



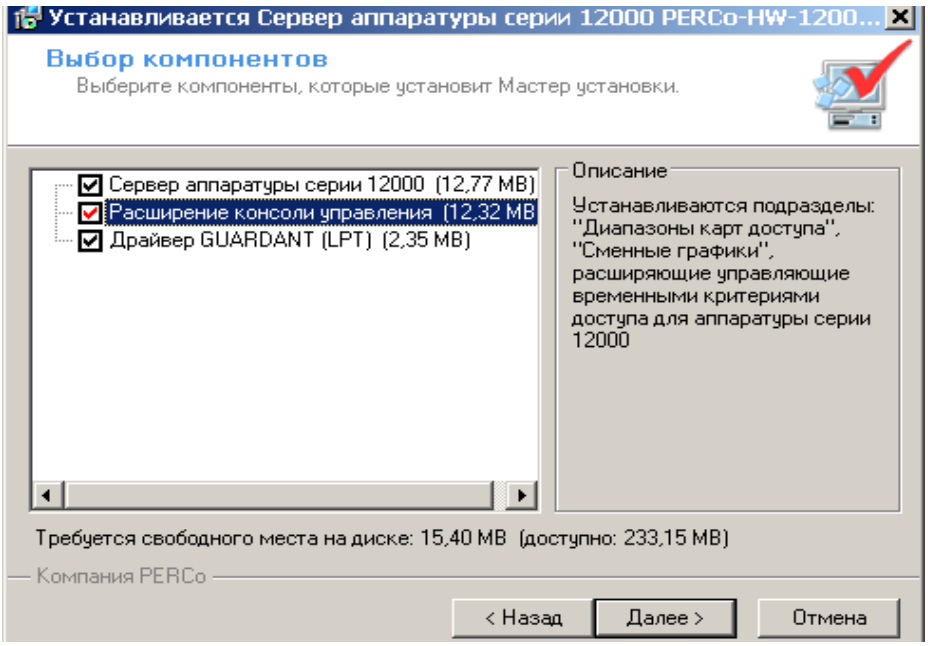
Вам предлагается инсталлировать модуль «Сервер аппаратуры серии 600»
Нажмите кнопку «Далее» для начала инсталляции.

2.2. Инсталляция модуля «Сервер аппаратуры серии 12000»

Вставьте компакт-диск с наклейкой

в привод CD-ROM.

Должен автоматически запуститься инсталляционный модуль PERCo-HW-12000.exe. Если этого не происходит — запустите данный модуль вручную. После принятия лицензионного соглашения и указания пути инсталляции появится следующее диалоговое окно:



Вам предлагается инсталлировать модуль «Сервер аппаратуры серии 12000».

Примечание: инсталляция «Расширения консоли управления» возможна только после установки базового пакета.

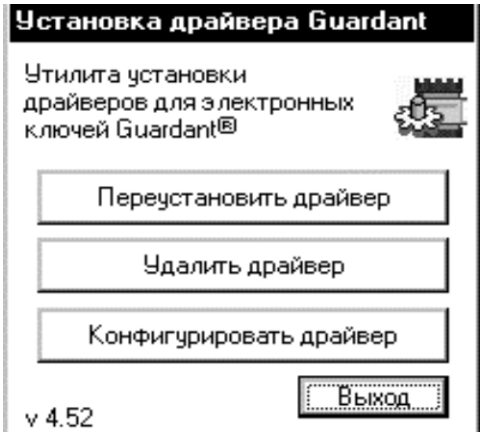
Затем нажмите кнопку «Далее» для начала инсталляции.

3. НАСТРОЙКА КЛЮЧЕЙ ЗАЩИТЫ GUARDANT

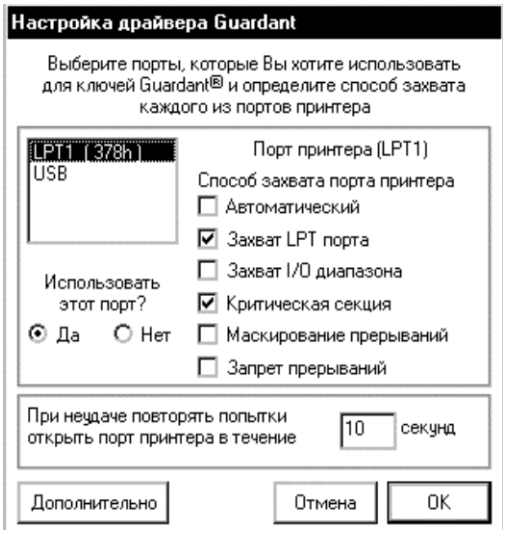
Модули «Сервер системы» и «Сервер аппаратуры серии 12000» защищены локальными ключами защиты GUARDANT. Для нормального функционирования этих модулей при их инсталляции автоматически устанавливается «Драйвер GUARDANT (LPT)», который необходимо настроить. Все компоненты системы, расширяющие возможности модуля «Консоль управления» и поставляемые отдельно, защищены сетевыми ключами (например, компонент «Учет рабочего времени», не входящий в базовый пакет). Работа с сетевыми ключами описана ниже в этом разделе.

3.1. Настройка драйвера GUARDANT (LPT)

Для настройки драйвера нажмите кнопку «Пуск» на панели задач Windows, выберите меню «Программы». В выпадающем окне найдите строку «PERCo» и наведите на нее курсор мыши. После этого выберите «СКУД PERCo-SYS-15000», затем «Управление драйвером GUARDANT(LPT)». На экране появится следующее диалоговое окно:



Нажмите на кнопку «Конфигурировать драйвер». На экране появиться следующее диалоговое окно:



для Windows 98/Me

для Windows NT/2000/XP

Процесс конфигурирования драйвера состоит из:

1) задания портов для поиска ключа;
2) задания способов захвата LPT порта;
3) установки тайм-аута;
4) задания дополнительных параметров.

Задание портов для поиска ключа

В левой верхней части окна отображается список найденных на вашем компьютере параллельных портов. В Windows 98/ME рядом с именем порта отображается и его базовый адрес. Кроме того, если на компьютере установлено аппаратное и программное обеспечение для работы с USB-устройствами, в списке портов присутствует строка «USB». Вы можете указать, на каких портах драйвер должен производить поиск ключей. Это очень полезно для уменьшения времени ответа ключа. Например, если ключ в вашем компьютере подсоединен к порту LPT2, а к LPT1 подсоединен принтер, то можно запретить использование порта LPT1 для поиска ключа. Поиск на USB-портах следует запретить. По умолчанию поиск разрешен на всех USB и LPT-портах.

Задание способов захвата LPT-порта

Захват параллельного порта необходим, во избежание конфликтов при попытке защищенного приложения обратиться к ключу в тот момент, когда другое приложение также использует порт, к которому присоединен ключ (например, происходит печать на принтер). Захват порта драйвером производится только на время общения с ключом, после чего порт освобождается. По умолчанию утилита конфигурации устанавливает автоматический способ захвата. Остальные способы имеет смысл использовать только администраторам, хорошо знакомым с тонкостями работы операционной системы и периферийных устройств. Каждому из выбранных параллельных портов можно задать свое сочетание способов захвата.

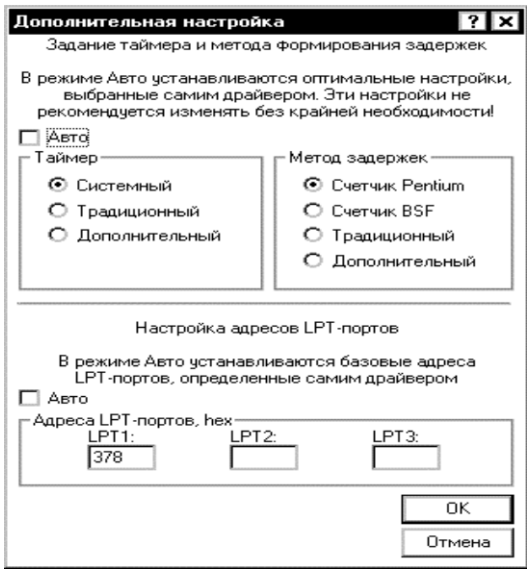
Установка тайм-аута

В случае если параллельный порт, к которому драйвер Guardant пытается получить доступ, оказывается занятым, драйвер будет ожидать освобождения порта. Время ожидания драйвера называется тайм-аутом. В течение этого времени он будет постоянно проверять состояние порта и, если порт так и остался занятым, защищенному приложению будет возвращена информация о том, что ключ не найден. Значение тайм-аута в секундах задается в нижней части диалогового окна.

Допустимые значения — от 0.001 до 600 секунд. Значение тайм-аута по умолчанию — 10 секунд. Под временем тайм-аута подразумевается общее время ожидания для всех параллельных портов, а не для каждого из них в отдельности (например, тайм-аут по умолчанию — 10 секунд всего, а не по 10 секунд для каждого из портов).

Задание дополнительных параметров

Диалоговое окно для задания дополнительных параметров вызывается нажатием кнопки «Дополнительно» в нижней части окна.



Выбор таймера и метода формирования задержек

Дополнительные параметры позволяют задать тип таймера, который будет использоваться драйверами Guardant, а также установить метод формирования задержек, необходимых при общении с электронным ключом. Это бывает нужно при работе на старых, либо ненадежно работающих (например, «разогнанных») компьютерах, у которых часто возникают проблемы с системными таймерами. На таких компьютерах можно будет добиться максимально возможной стабильности обмена с ключами Guardant. Рекомендуется выбрать автоматический режим выбора этих параметров (устанавливается по умолчанию). В этом случае драйвер сам собирает статистику, анализирует стабильность работы таймеров компьютера и выбирает оптимальный вариант настройки.

Настройка адресов LPT-портов

Настройка адресов LPT-портов необходима в тех случаях, когда компьютер оборудован дополнительными параллельными портами на платах расширения. Такие порты часто имеют нестандартные адреса. По умолчанию установлен режим автоматического определения адресов драйвером Guardant. Адреса LPT-портов, определенные драйвером, отображаются в соответствующих полях ввода. Отключение автоматического режима и корректировка адресов требуется только в случае, если драйверу не удалось верно определить базовый адрес какого-либо LPT-порта.

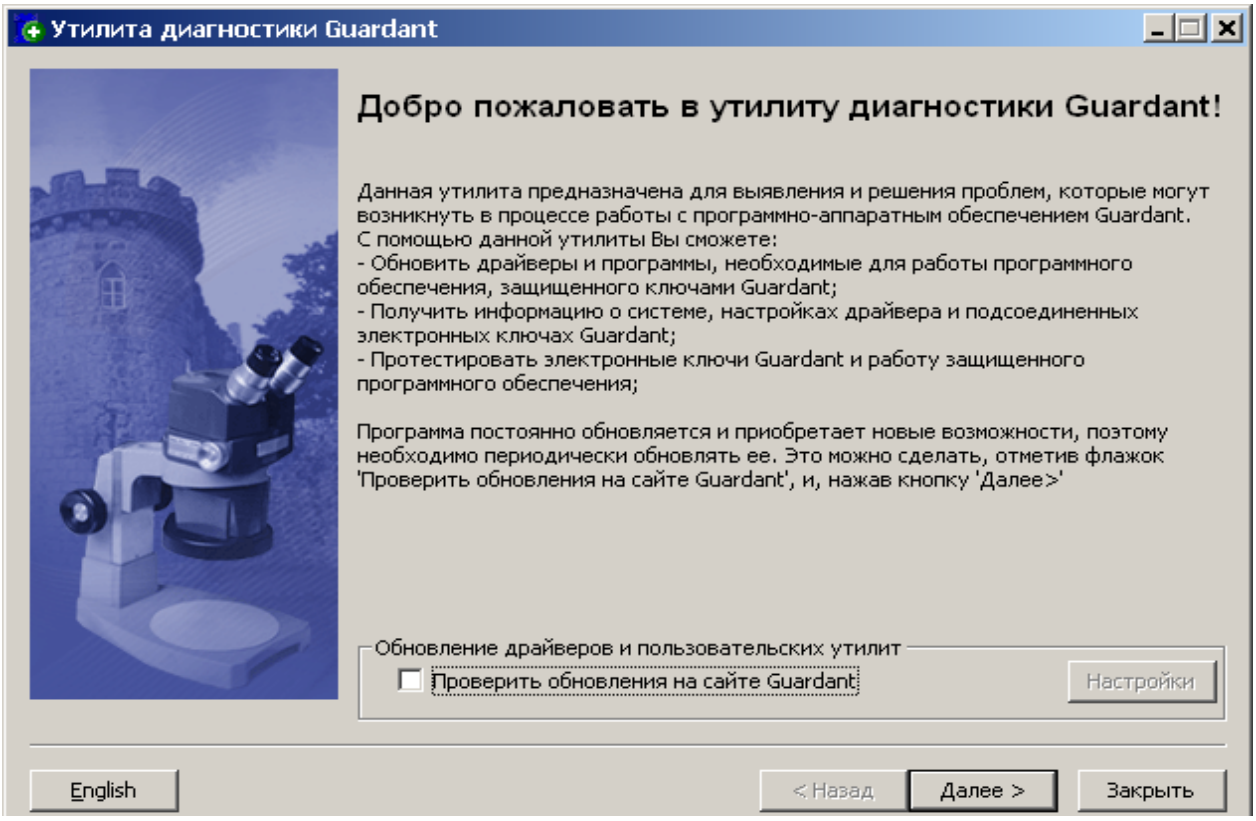
После задания всех нужных параметров нажмите кнопку «ОК», для отмены изменений — кнопку «Отмена». После конфигурирования драйвера перезагрузка системы не требуется. Все внесенные Вами изменения вступают в силу мгновенно.

Удаление драйвера

Для удаления загруженного в систему драйвера нужно нажать кнопку «Удалить драйвер» в главном окне.

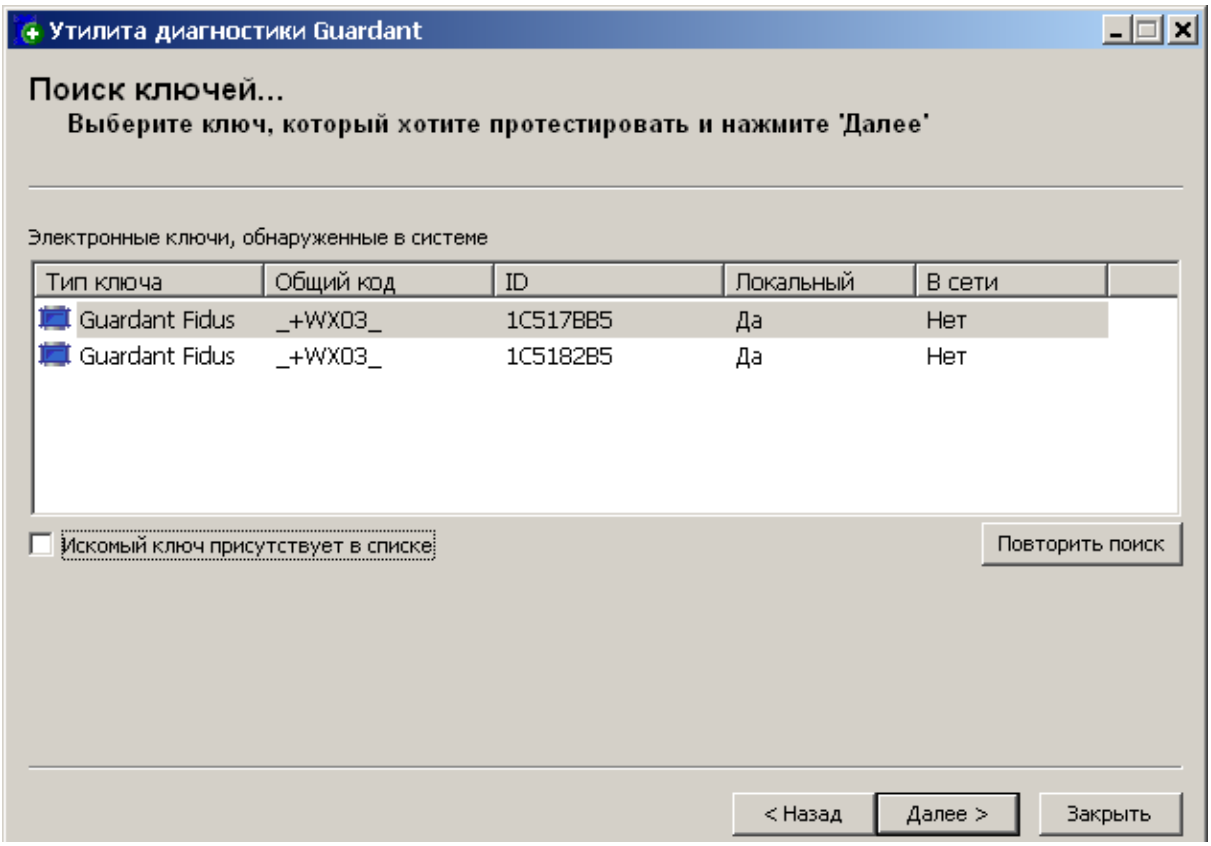
3.2. Проверка работоспособности локальных ключей защиты

Для проверки работоспособности локальных ключей защиты нажмите кнопку «Пуск» на панели задач Windows, выберите меню «Программы». В выпадающем окне найдите строку «PERCo» и наведите на нее курсор мыши. После этого выберите «СКУД PERCo-SYS-15000», затем «Диагностика ключей GUARDANT (LPT)». На экране появится следующее диалоговое окно:



Нажмите кнопку «Далее».

Появится следующее диалоговое окно:



В списке окна будут отображены все электронные ключи, найденные на локальном компьютере. Если этого не происходит, следует настроить драйвер GUARDANT (LPT) и повторить поиск. Если ключи найдены - следует нажать на кнопку «Закрыть».

3.3 Настройка сетевых ключей защиты GUARDANT (Net)

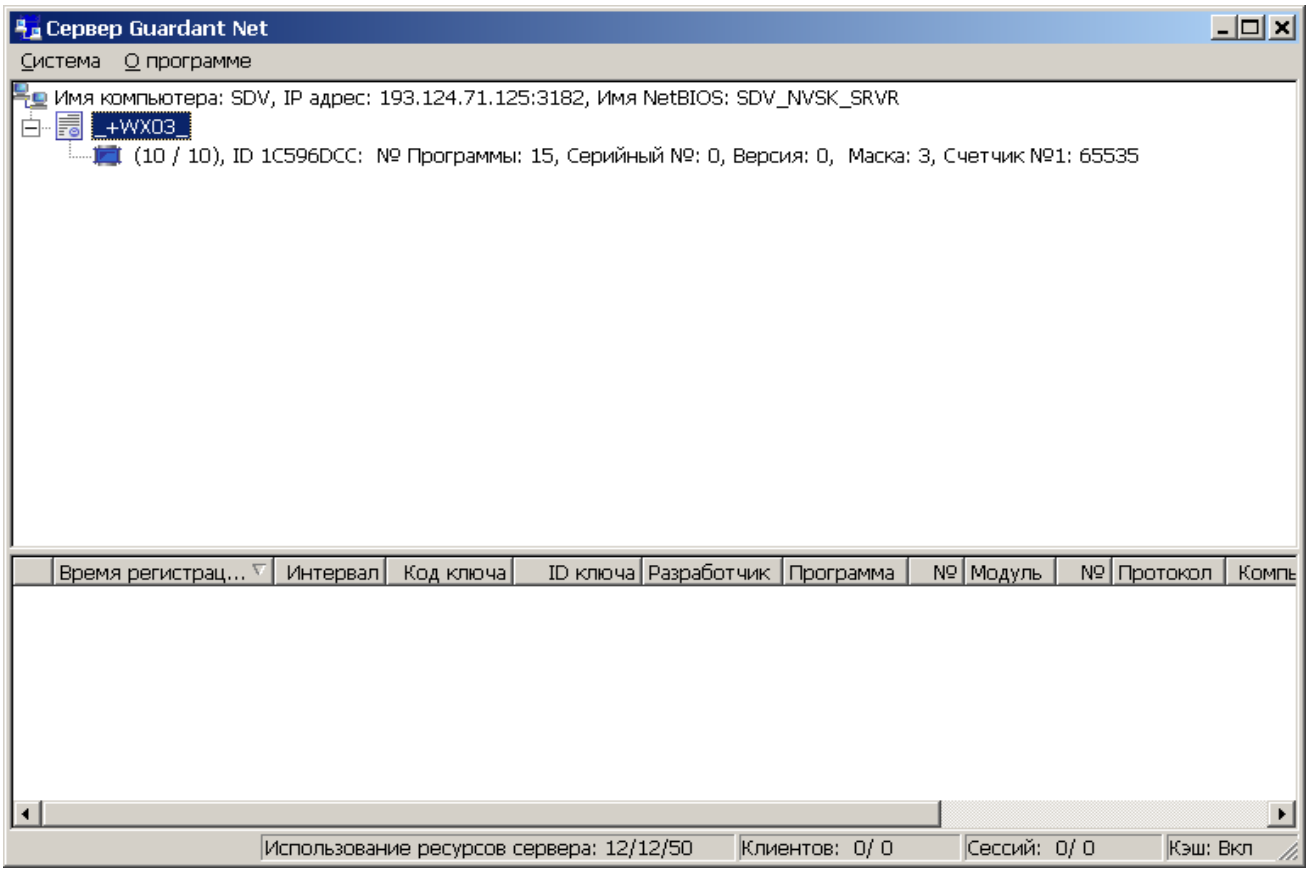
Сетевой ключ защиты отличается от локального ключа тем, что он ставиться на выделенный компьютер в сети и его видят все защищенные приложения, работающие в этой сети.

Установка сетевого ключа

Для установки сетевого ключа следует выбрать элемент «Сервер ключей GUARDANT (Net)» из базового пакета инсталляции. После инсталляции на выбранный компьютер будет установлен драйвер GUARDANT (LPT) и сервер ключей GUARDANT (Net). Далее необходимо провести настройку драйвера, как описано в п. 3.1 и 3.2, а затем запустить сервер ключей GUARDANT (Net) и оставить его работающим.

Запуск сервера ключей GUARDANT (Net)

Для запуска сервера ключей GUARDANT(Net) нажмите кнопку «Пуск» на панели задач Windows, выберите меню «Программы». В выпадающем окне найдите строку «PERCo» и наведите на нее курсор мыши. После этого выберите «СКУД PERCo-SYS-15000», затем «Сервер ключей GUARDANT (Net)». На экране появится следующее диалоговое окно:



Окно сервера разделено на две части.

В верхней части окна древовидной структурой представлена информация о компьютере, на котором установлен ключ (ключи) и сервер, а также основные данные о клиентах.

В основании «дерева» отображаются сведения о компьютере, на котором запущен сервер Guardant Net: имя компьютера (host name), IP адрес, NetBIOS имя.

На 1-м уровне вложенности находится «Общий код ключа» (Public Code).

На 2-м уровне представлена информация о ключе: значение реального сетевого ресурса (текущее/максимальное), ID ключа, номер программы, серийный номер, версия программы, значение счетчика GP.

На 3-м уровне отображается основная информация о клиенте: сетевой протокол, по которому выполнено соединение, имя и IP-адрес компьютера, на котором запущен клиент.

Статус зарегистрированного на сервере ключа отражают специальные символы рядом с пиктограммой ключа:

«замок» – ключ заблокирован операцией чтения/записи

«X» – ключ недоступен (отсоединен)

Таким образом, отсутствие пометок означает, что ключ доступен (т.е. физически подсоединен к порту компьютера) и не заблокирован.

В нижней части окна сервера в виде таблицы представлены подробные характеристики клиентов:

- Время регистрации на сервере
- Время, прошедшее с момента последнего обмена с клиентом
- Общий код и идентификационный номер (ID) ключа, который обслуживает клиента
- Разработчик программы
- Название программы и ее номер
- Название модуля и его номер (если используется таблица лицензий)
- Сетевой протокол, по которому выполнено соединение
- Имя и IP-адрес компьютера, на котором запущен клиент
- Платформа, для которой написано приложение

Данные о клиентах можно сортировать по возрастанию или убыванию по любому из параметров.

Если клиент не присылает запрос в течение 15 минут (т. е. «зависает»), то он помечается серым цветом, но не удаляется из списка клиентов. Связь с «зависшим» клиентом прерывается, только тогда, когда новому клиенту не хватает именно этой лицензии.

В строке статуса сервера отображаются статистические данные его работы:

- Использование ресурсов сервера: текущее, пиковое и максимально возможное количество служебных блоков, используемых сервером в процессе сетевого обмена для связи с клиентами
- Клиенты: текущее и пиковое количество клиентов, которых в данный момент обслуживает сервер
- Сессии: текущее и пиковое количество сессий (сеансов связи), открытых с клиентами
- Кэш: состояние кэша сервера

Регистрация нового электронного ключа

Есть возможность добавить электронный ключ к уже зарегистрированным на сервере. Однако для этого недостаточно просто подсоединить ключ к компьютеру — его надо еще и зарегистрировать. Для регистрации нового ключа служит команда меню **Система|Перечитать**. Регистрация ключа выполнена успешно, если информация о нем появилась в списке ключей этого сервера. С этого момента можно запускать программы, «привязанные» к этому ключу.

Если отсоединить зарегистрированный ключ от рабочей станции, а затем перечитать ключи при помощи команды меню **Система|Перечитать**, ключ будет помечен символом «X» — это признак того, что ключ зарегистрирован, но физически отсутствует (т.е. недоступен). С этого момента запуск новых приложений, «привязанных» к этому ключу, станет невозможным.

Восстановление регистрации ключа нужно произвести так, как описано выше. Если оно произведено успешно, символ «X» исчезнет.

4. НАСТРОЙКА DCOM

При установке ПО системы на нескольких компьютерах локальной сети необходимо настроить службу безопасности DCOM. Распределенная модель компонентных объектов DCOM (Distributed Component Object Model) используется при выполнении распределенных приложений в сети. Распределенное приложение выполняется как совокупность нескольких процессов, совместно решающих определенную задачу. Программа применяется для настройки 32-разрядных приложений, использующих модели COM и DCOM.

Чтобы использовать приложения с моделью DCOM, необходимо в программе настройки DCOM (специальная утилита, в состав программного обеспечения не входит) задать свойства приложения, определяющие их размещение и параметры безопасности.

DCOM позволяет запускать удаленные сервера на ПК с операционными системами Windows NT (WorkStation или Server), Windows 2000 и Windows XP.

Программный пакет с реализацией данной технологии как обязательный входит в состав операционных систем Windows 2000/XP/NT, а для Windows 98 может устанавливаться отдельно.

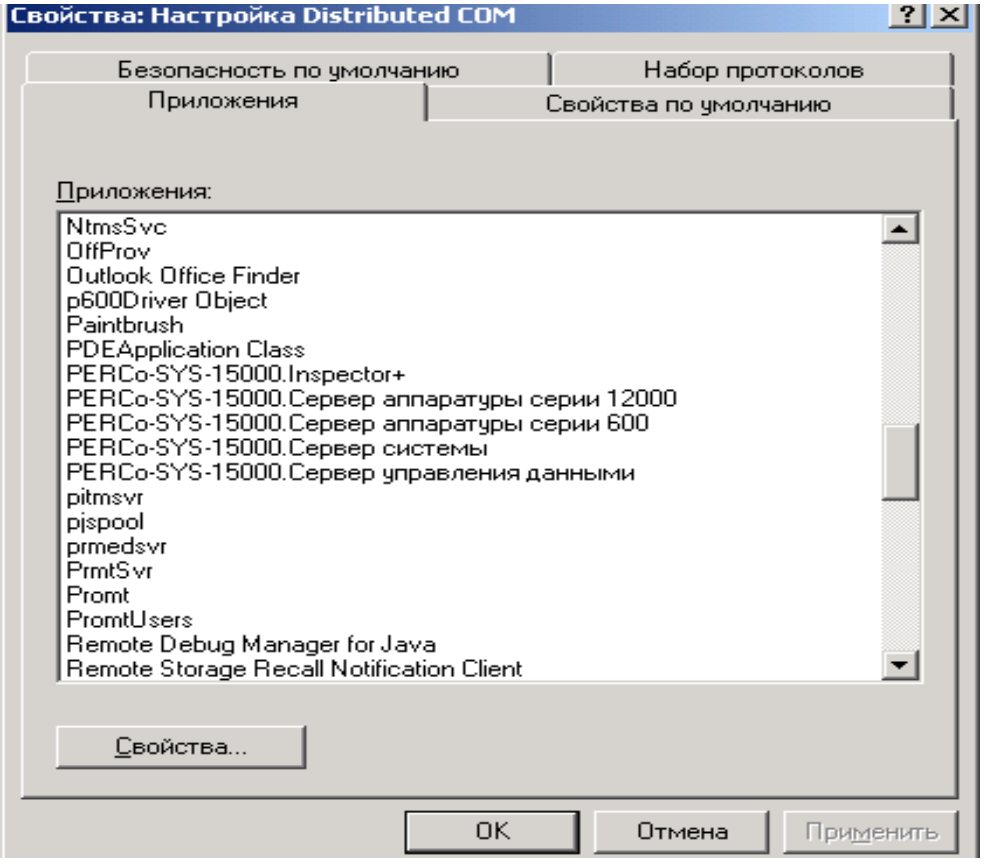
Для работы в сети создайте группу пользователей на сервере, если у вас выделенный сервер, либо на компьютере, на котором установлена аппаратура. В эту группу должны входить пользователи, которые будут работать с системой (например, группа пользователей «DCOMUser»). Более подробную информацию о создании групп пользователей можно получить в документации по Windows.

4.1. Настройка DCOM в операционной системе Windows 2000

Запустите утилиту DCOMcnfg.exe. Для этого выполните следующие действия:

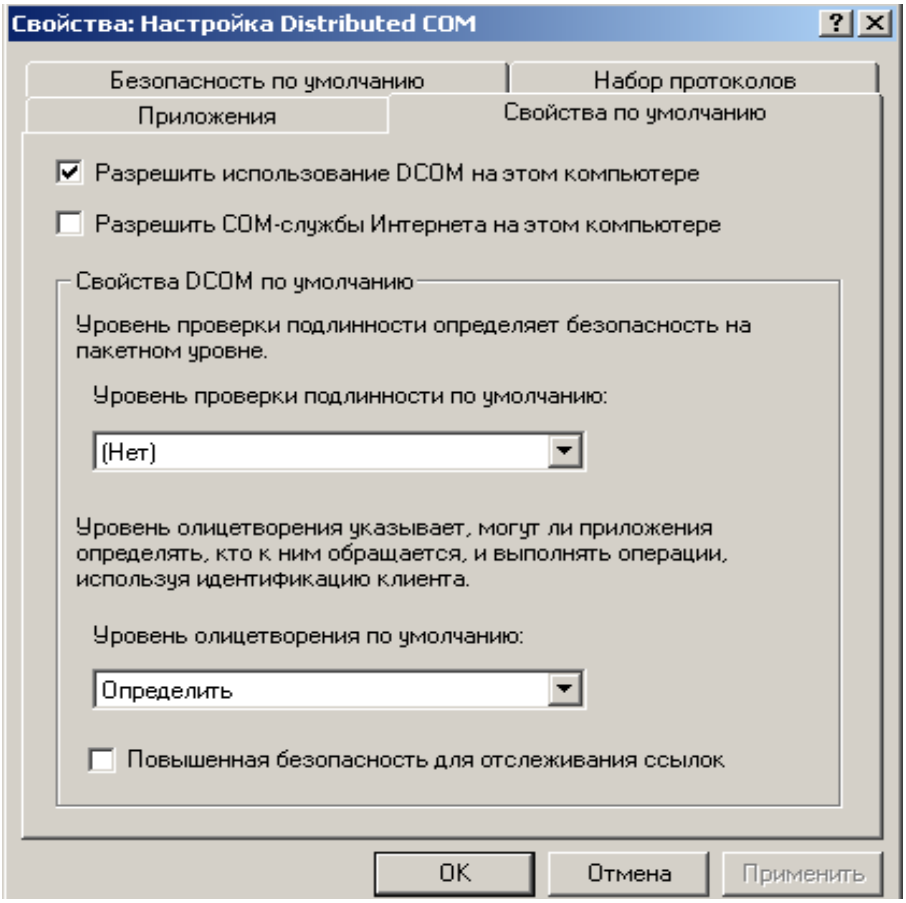
1) Нажмите кнопку «Пуск» на панели задач Windows, выберите команду «Выполнить»;
2) В появившемся окне «Запуск программы» при помощи клавиатуры введите DCOMcnfg.exe в поле «Открыть»;
3) Нажмите в окне «Запуск программы» кнопку «ОК»;

После запуска программы на экран будет выведено окно:



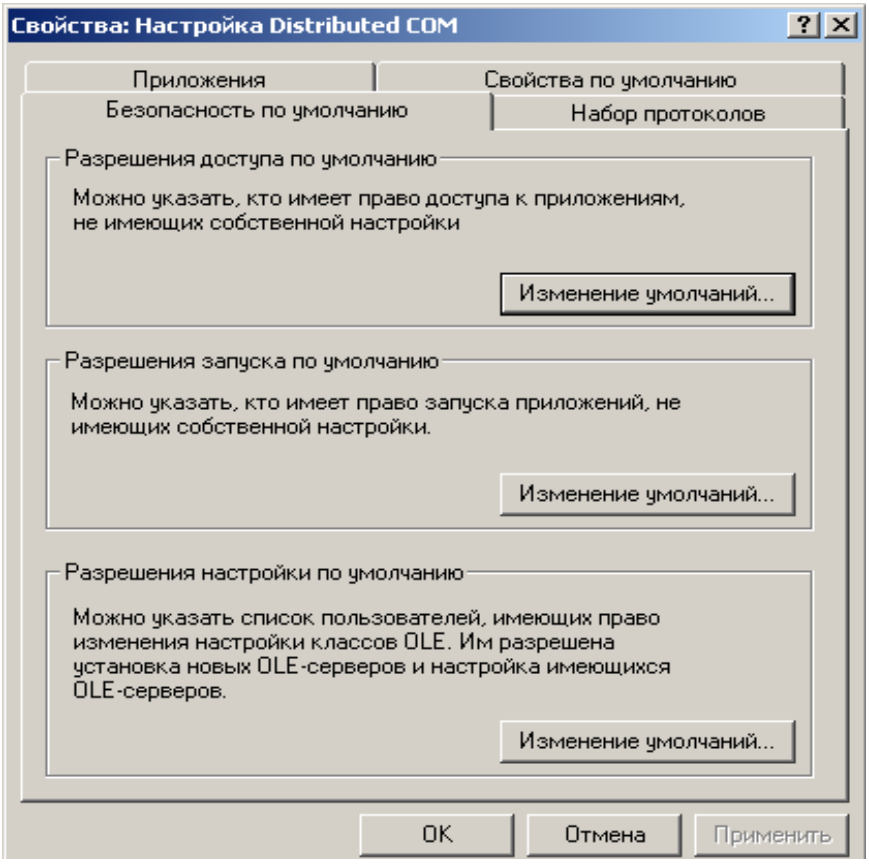
Установка свойств по умолчанию

Выберите закладку «Свойства по умолчанию» ("Default Properties") и установите параметры, указанные на рисунке:



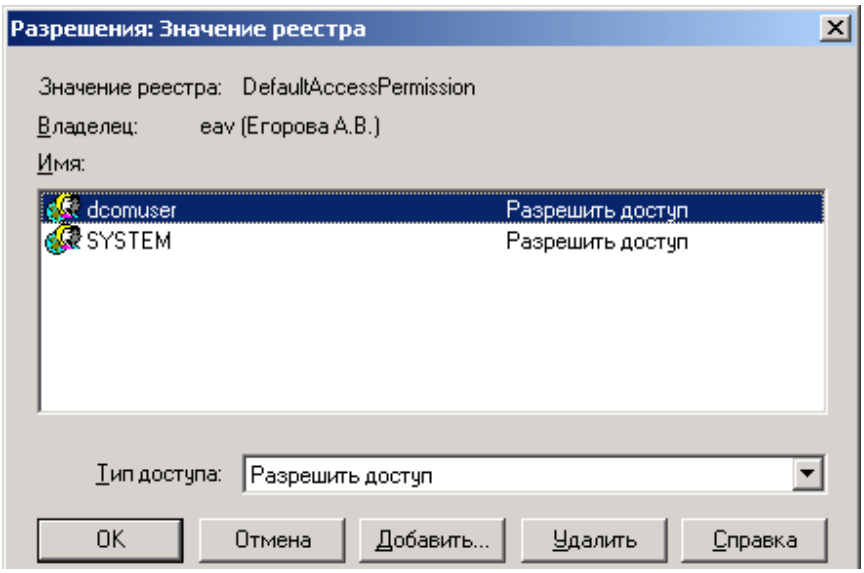
Установка безопасности по умолчанию

Выберите закладку «Безопасность по умолчанию» ("Default Security").

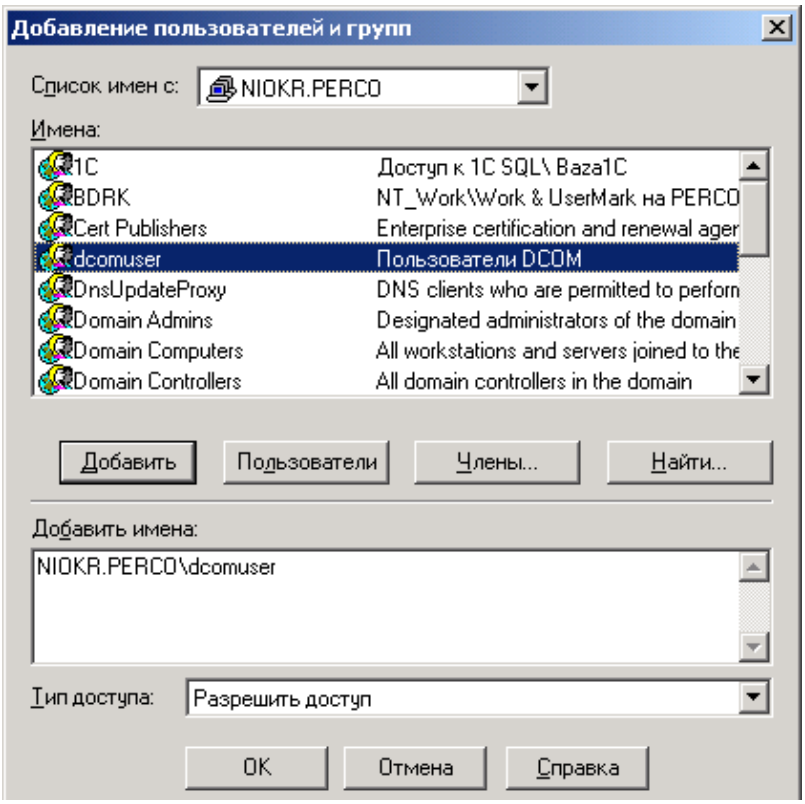


Разрешение доступа по умолчанию

Для изменения стандартных разрешений доступа в поле «Разрешения доступа по умолчанию» («Default Access Permissions») нажмите кнопку «Изменение умолчаний» («Edit default»). При этом появится диалоговое окно редактирования списка пользователей, имеющих права доступа по умолчанию.



Для добавления пользователя или группы пользователей нажмите на кнопку «Добавить» («Add») при этом откроется диалоговое окно, в котором необходимо установить права доступа:



1)В списке имен пользователей выберите «SYSTEM» и группу пользователей «DCOMUser»;

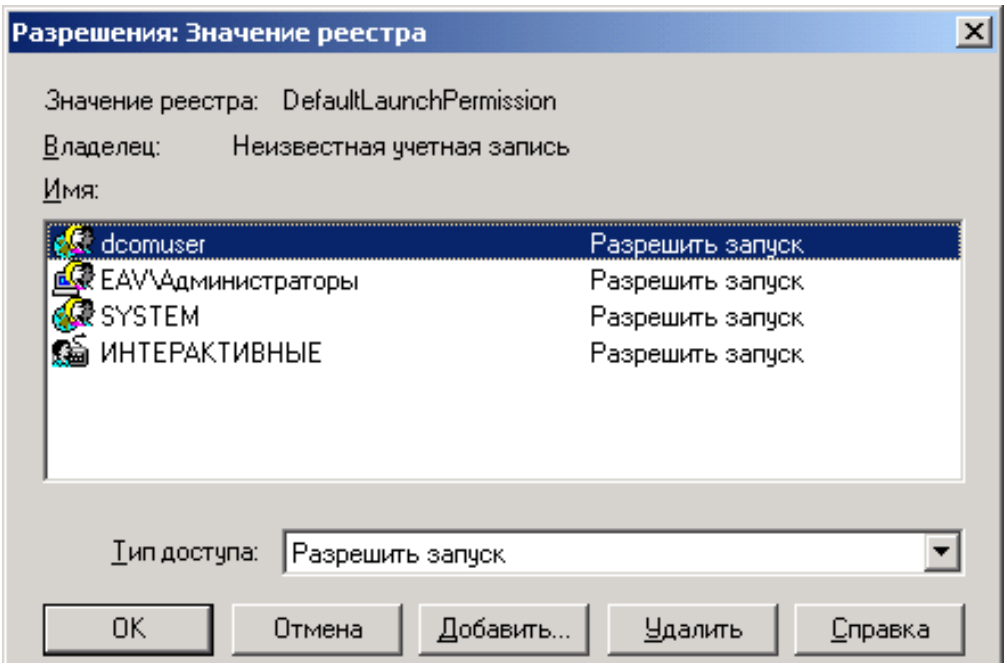
2)Для разрешения доступа в поле «Тип доступа» («Type of Access») в выпадающем списке выберите «Разрешить запуск» («Allow Access» или «Grant Access»);

3)Нажмите кнопку «ОК» для подтверждения или «Отмена» («Cancel») для отмены изменений;

4)Для удаления пользователя воспользуйтесь кнопкой «Удалить» («Remove»).

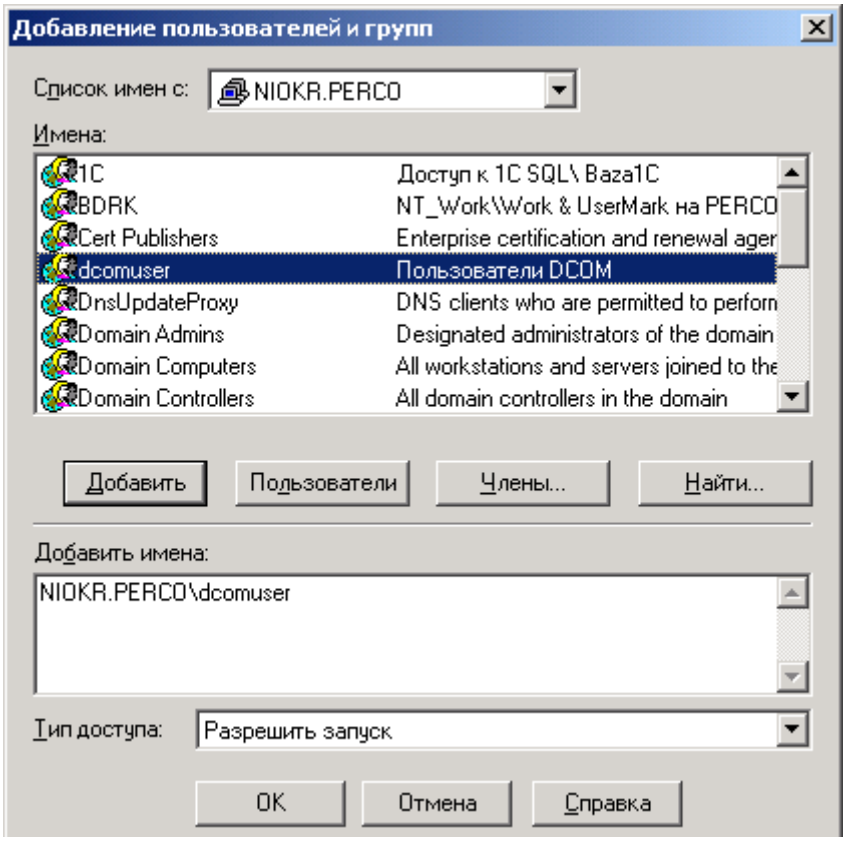
Разрешение запуска приложений по умолчанию

Для изменения стандартных разрешений запуска в поле «Разрешения запуска по умолчанию» («Default Launch Permissions») нажмите кнопку «Изменения умолчаний» («Edit Default»). При этом появится диалоговое окно редактирования списка пользователей, имеющих права запуска по умолчанию:



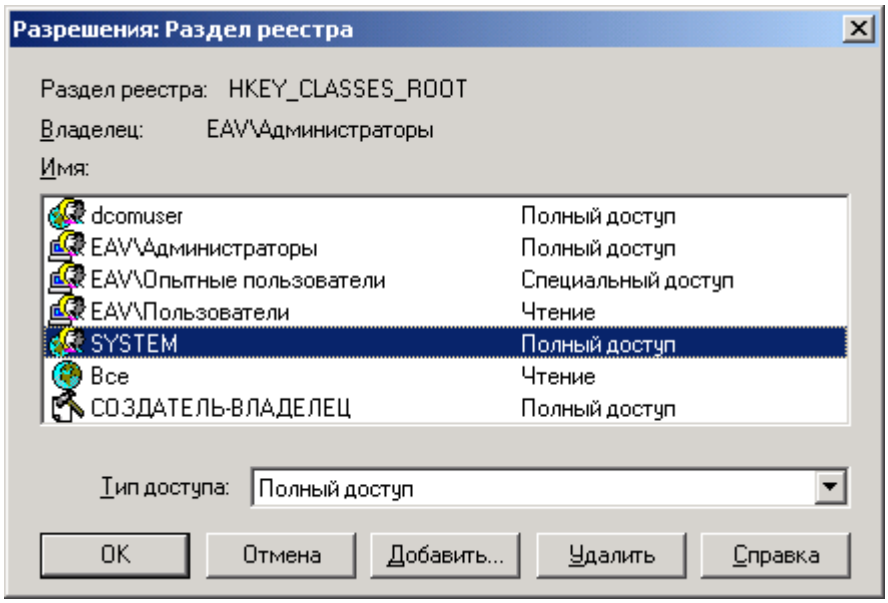
Выберите пользователей «SYSTEM», «ИНТЕРАКТИВНЫЕ» ("INTERACTIVE"), группу пользователей «DCOMUser» и установите для них в поле «Тип доступа» («Type of Access») в выпадающем списке «Разрешить запуск» («Allow Launch»), то есть разрешить этим пользователям запускать все объекты. Затем нажмите кнопку «Добавить».

На экране появится окно:

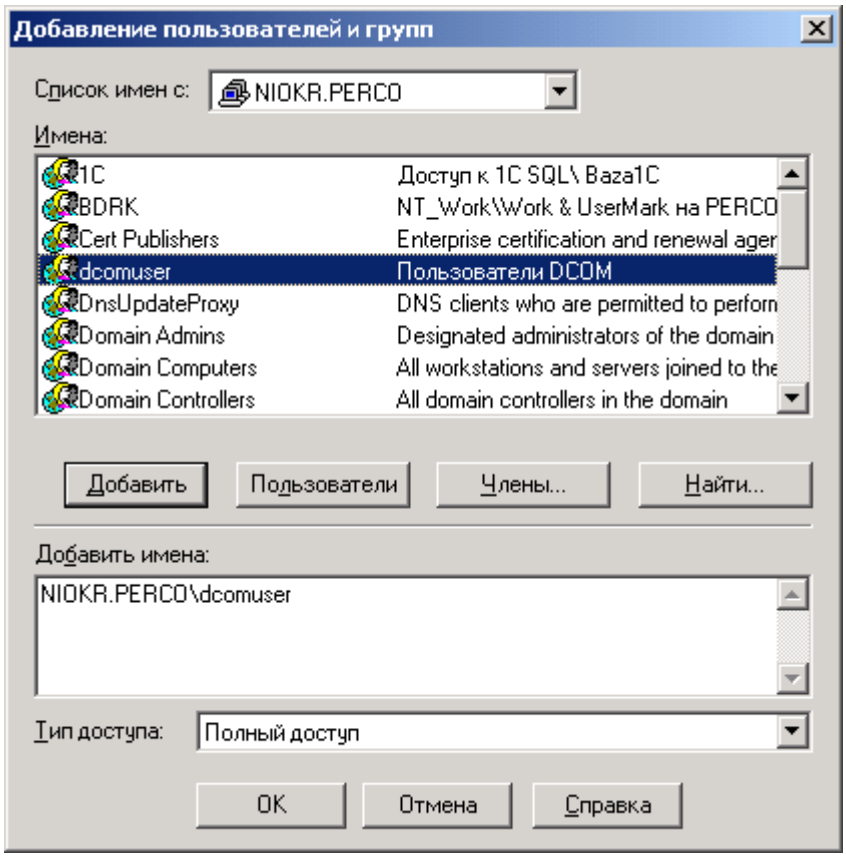


Разрешение настройки по умолчанию

Для изменения стандартных разрешений настройки в поле «Разрешения настройки по умолчанию» («Default Configurations Permissions») нажмите кнопку «Изменение умолчаний» («Edit Default»). Появится диалоговое окно редактирования списка пользователей, имеющих права настройки по умолчанию:



Выберите пользователя «SYSTEM», группу пользователей «DCOMUser» и установите для них в поле «Тип доступа» («Type of Access») в выпадающем списке — «Полный доступ» («Full Control»), то есть разрешите этим пользователям конфигурировать все объекты. Нажмите кнопку «Добавить»:

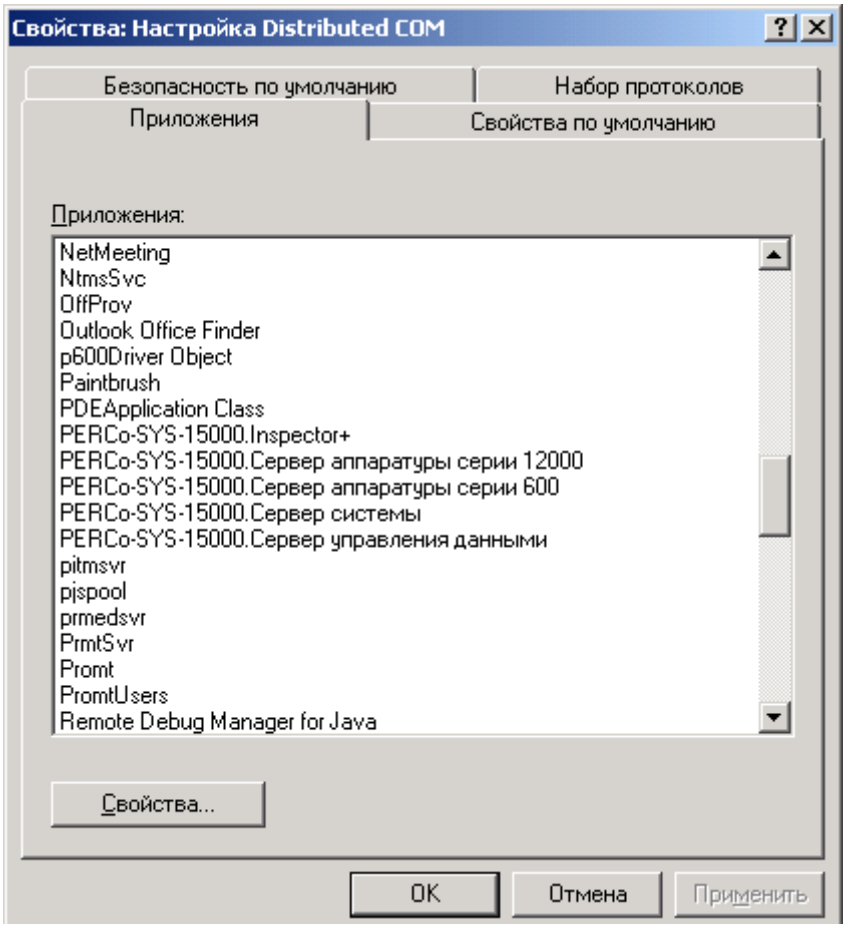


По окончании настройки параметров DCOM, используемых по умолчанию, можно приступать к настройке параметров определенного приложения.

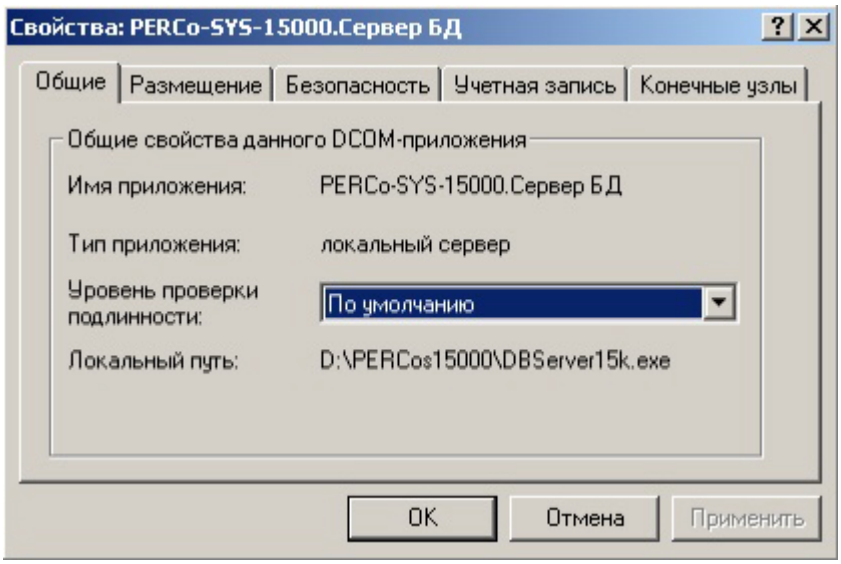
Настройка объектов DCOM

Настройки осуществляются в следующей последовательности:

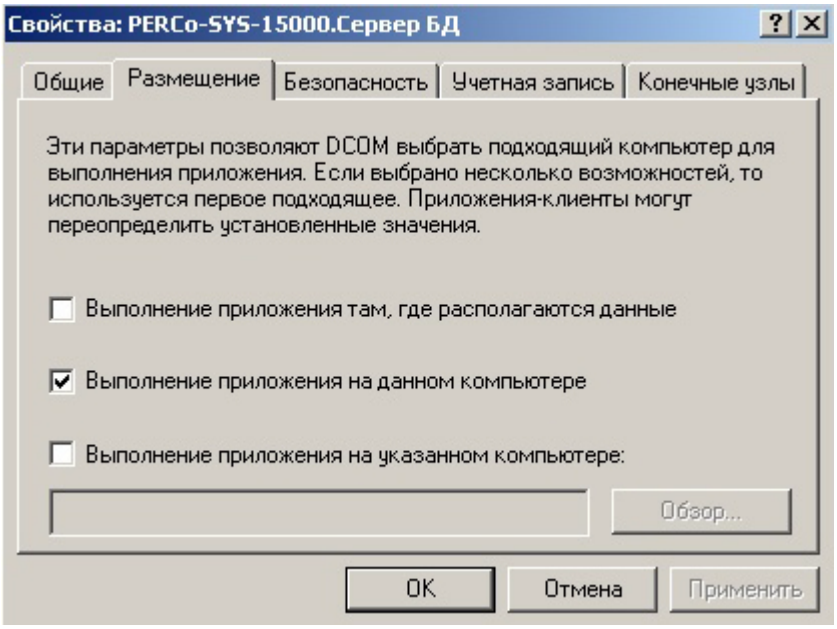
1) Выберите из списка на странице «Приложения» («Applications») одно из приложений: «PERCo-SYS-15000.Сервер аппаратуры серии 600», «PERCo-SYS-15000.Сервер аппаратуры серии 12000», «PERCo-SYS-15000. Сервер управления данными» и «PERCo-SYS-15000.Сервер системы» (для каждого сервера настройка проводится одинаково);



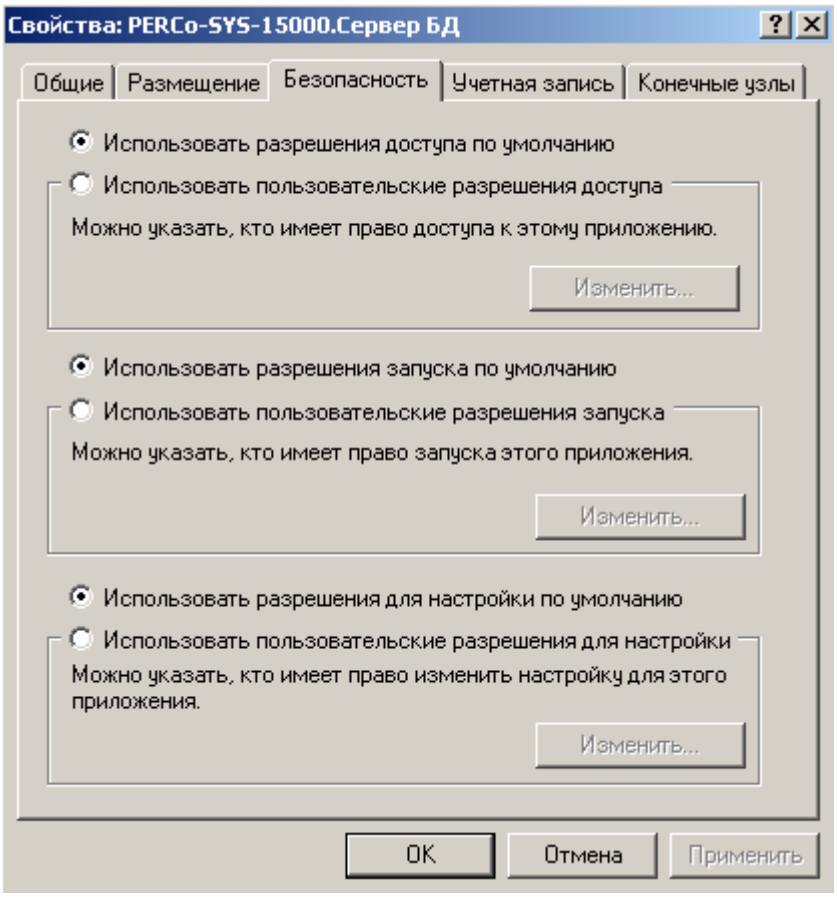
2) Нажмите кнопку «Свойства» («Properties»). В открывшемся окне на закладке «Общие» («General») показаны свойства выбранного приложения. Здесь можно установить «Уровень проверки подлинности» («Authentication Level»). Рекомендуемое значение указано на рисунке:



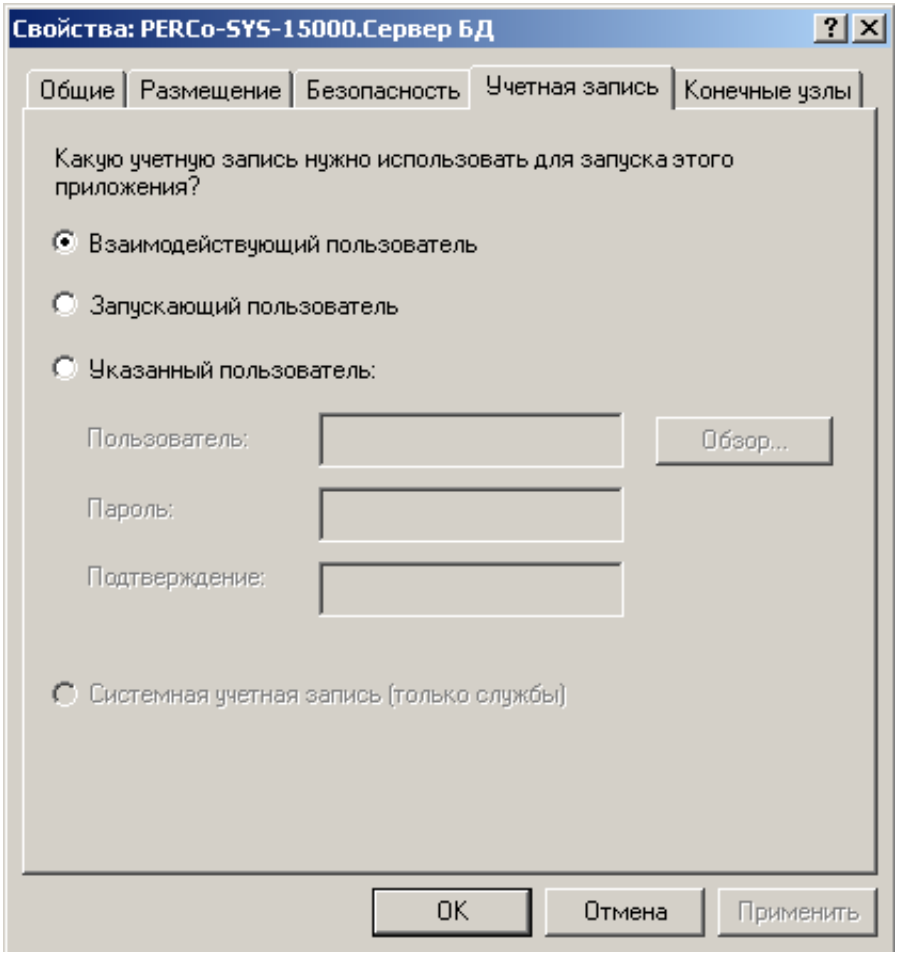
3) На закладке «Размещение» («Location») установите параметры, указанные на рисунке:



4) Для установки безопасности по умолчанию перейдите на закладку «Безопасность» («Security») и установите параметры, указанные на рисунке:



5) Для установки метода идентификации по умолчанию перейдите на закладку «Учетная запись» («Identify») и установите параметры, указанные на рисунке (см. следующую страницу):



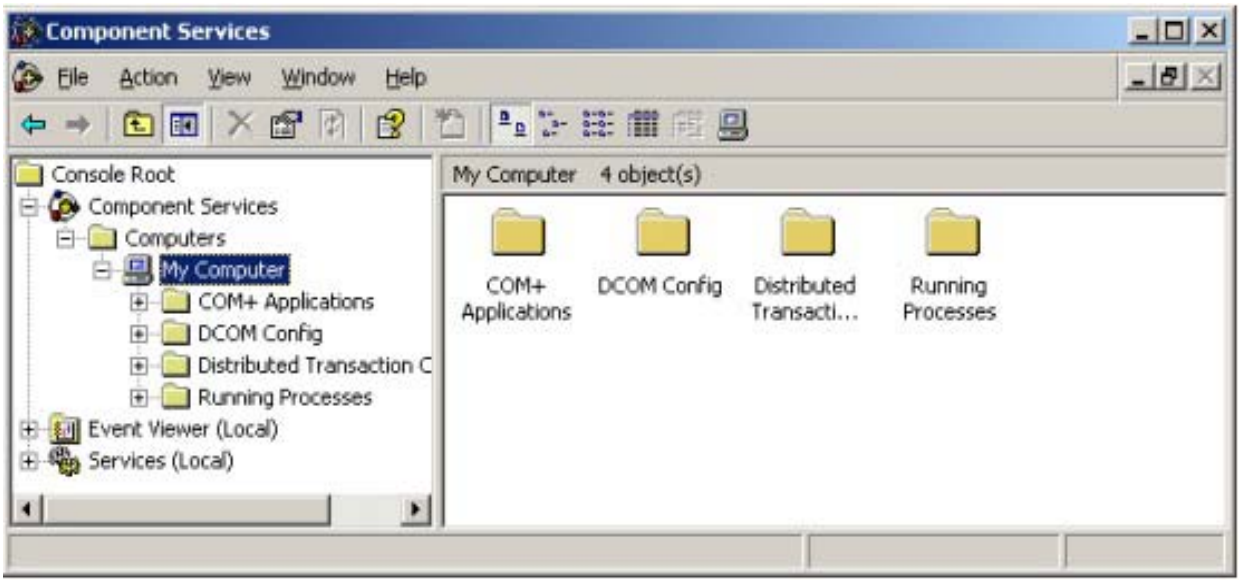
По окончании настройки конфигурации DCOM и отдельных приложений можно приступать к работе.

4.2. Настройка DCOM в операционной системе Windows XP

Запустите утилиту DCOMcnfg.exe. Для этого выполните следующие действия:

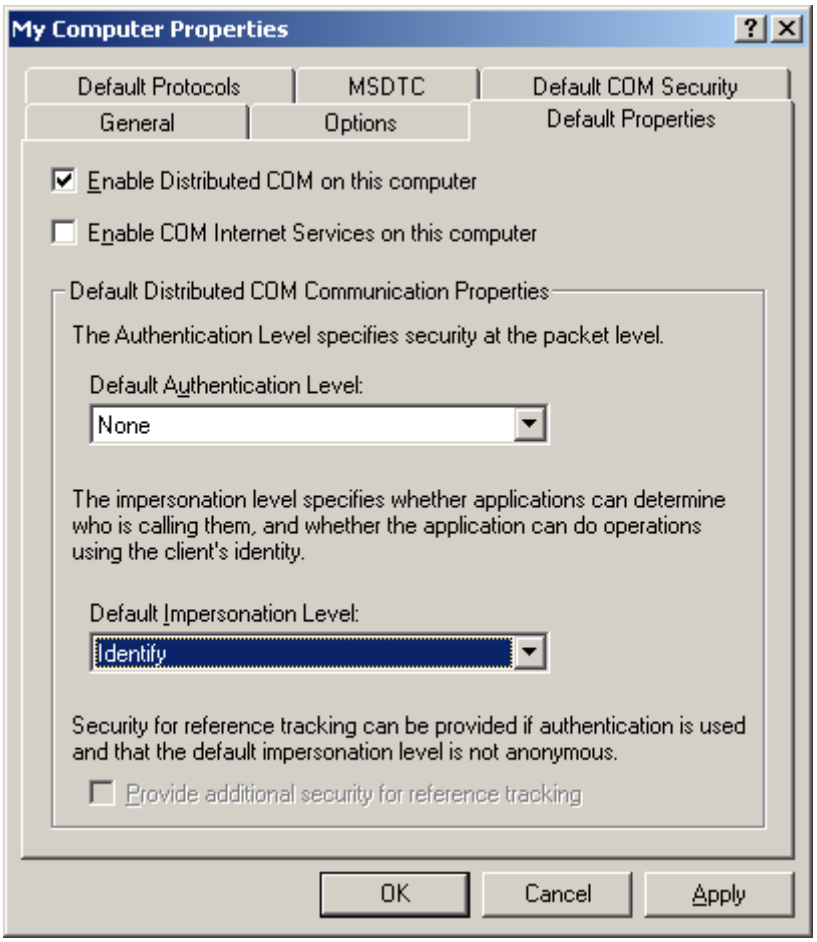
1) Выберите пункт меню «Пуск» («Start») команду «Выполнить» («Run»);
2) В появившемся окне «Запуск программы» в поле «Открыть» при помощи клавиатуры введите DCOMcnfg.exe;
3) Нажмите в окне «Запуск программы» кнопку «ОК»;

После запуска программы на экран будет выведено окно:



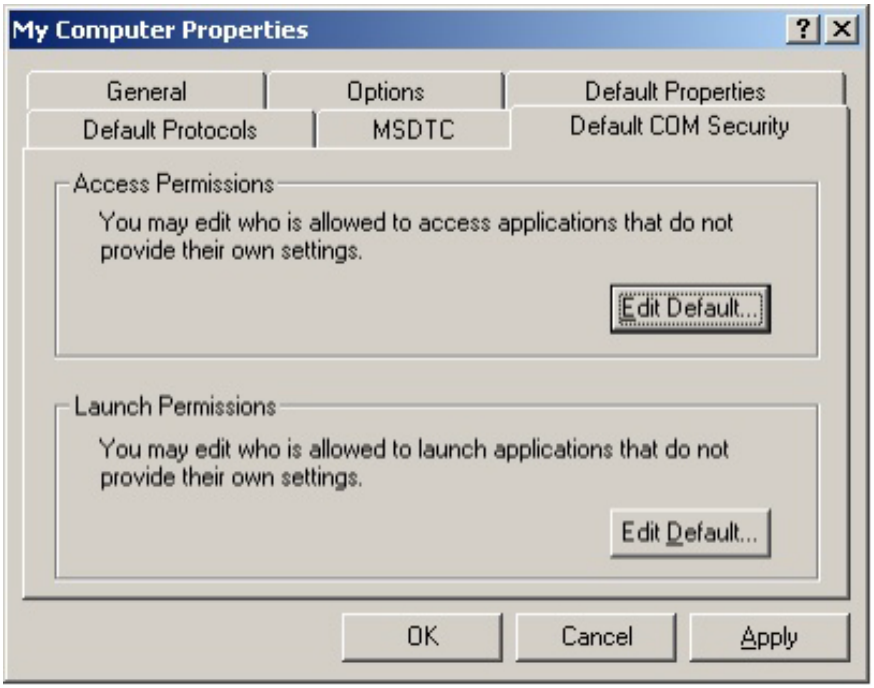
Установка свойств по умолчанию

Выберите закладку «Свойства по умолчанию» («Default Properties») и установите параметры, указанные на рисунке. Данное диалоговое окно вызывается с помощью щелчка правой кнопки мыши на значке «My computer», пункт меню «Properties».



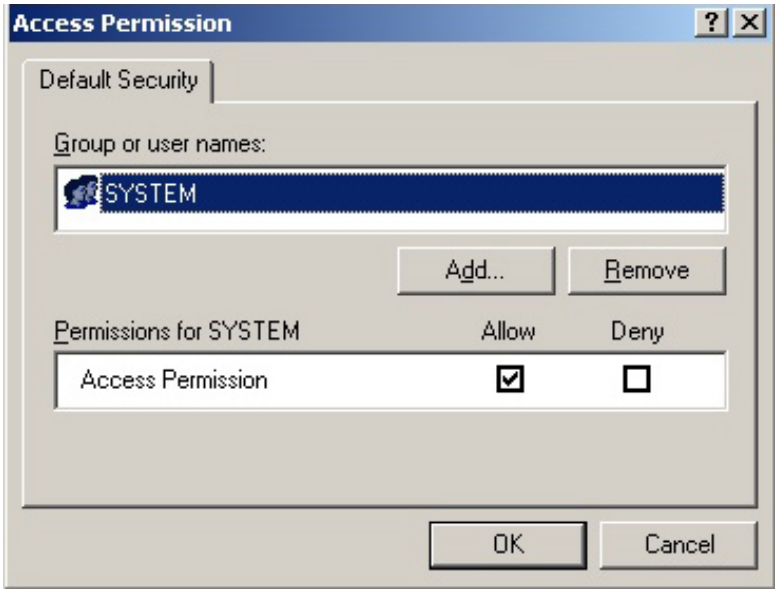
Установка безопасности по умолчанию

Выберите закладку «Безопасность по умолчанию» («Default Security»).

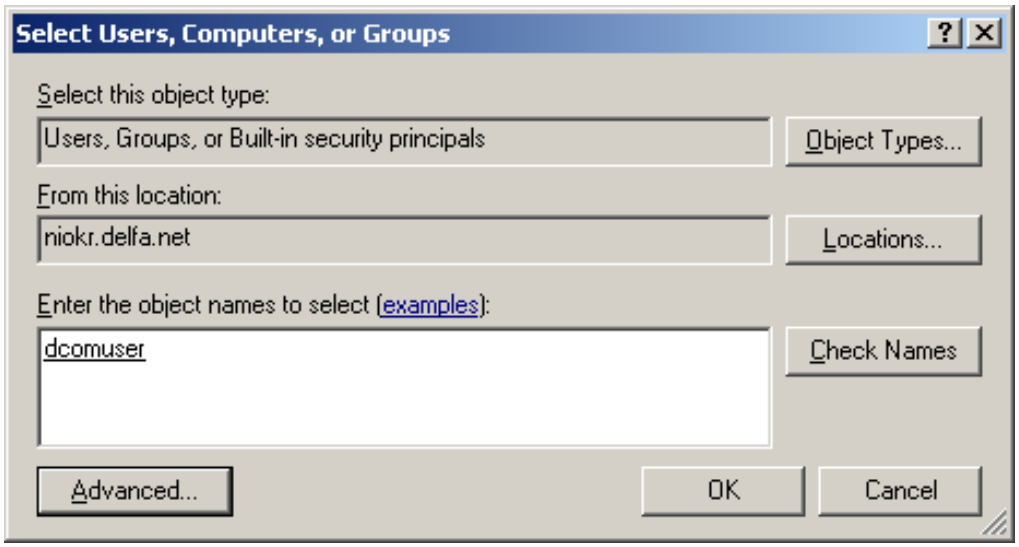


Разрешение доступа по умолчанию

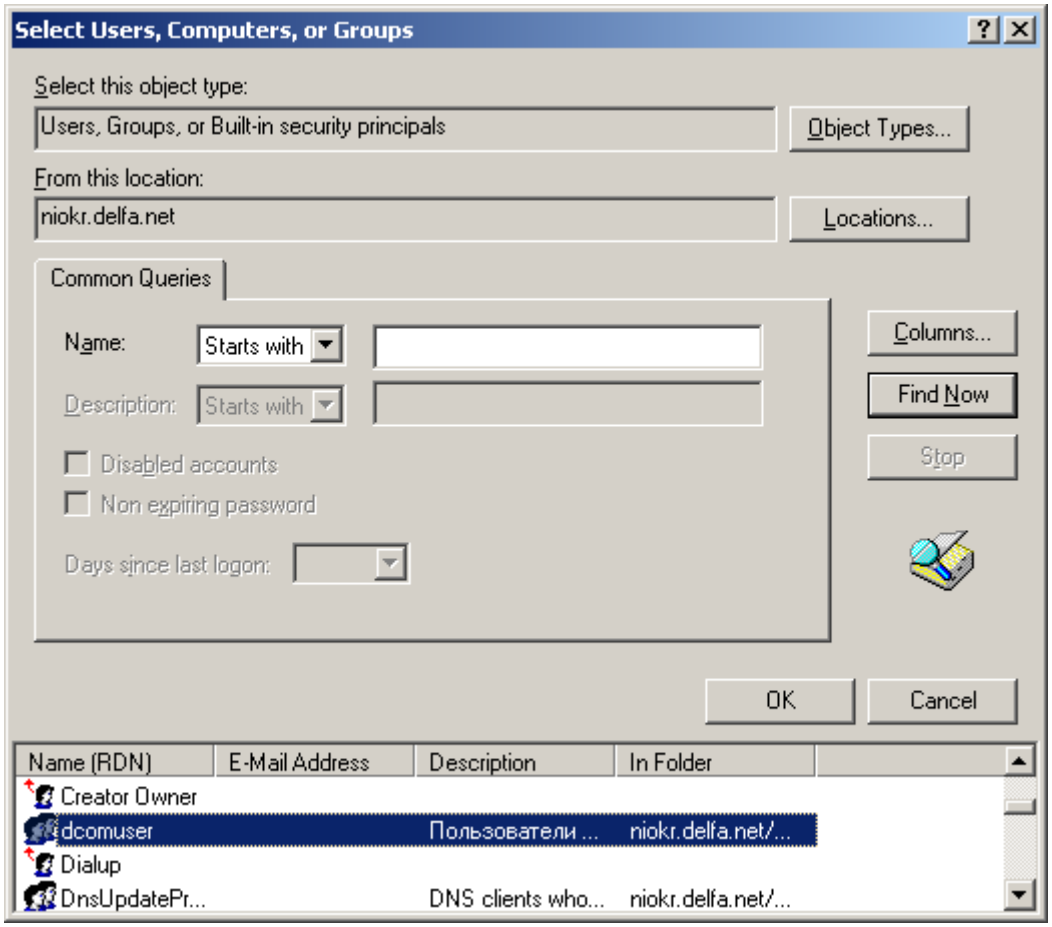
Для изменения стандартных разрешений доступа в поле «Разрешения доступа по умолчанию» («Default Access Permissions») нажмите кнопку «Изменение умолчаний» («Edit default»). При этом появится диалоговое окно редактирования списка пользователей, имеющих права доступа по умолчанию.



Для добавления пользователя или группы пользователей нажмите на кнопку "Добавить" ("Add"): при этом откроется диалоговое окно, в котором необходимо выбрать тип добавляемого объекта (пользователи, группы и др.), указать местоположение домена и ввести объект, например, группу:

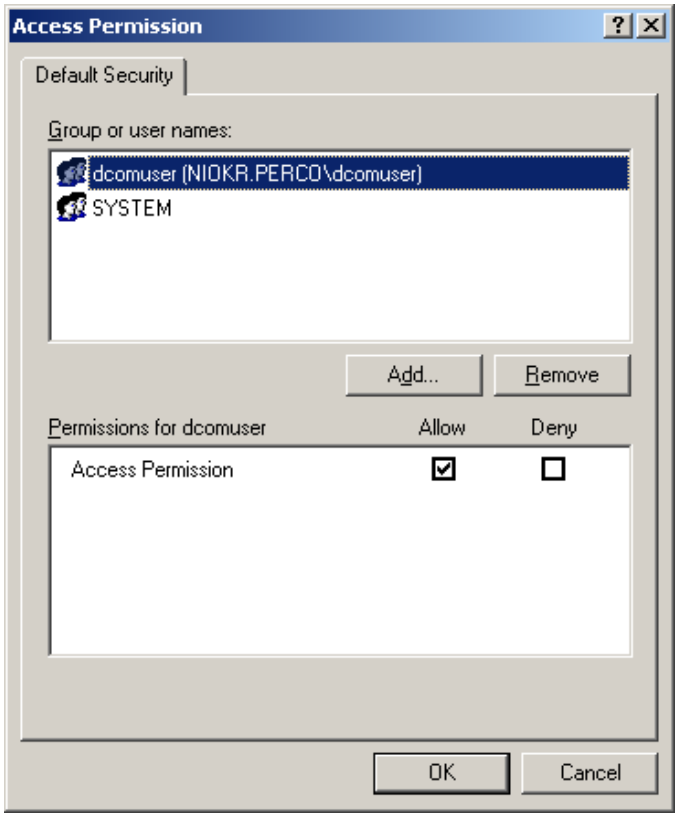


Для выбора объекта можно воспользоваться кнопкой "Advanced" и затем кнопкой "Find Now":



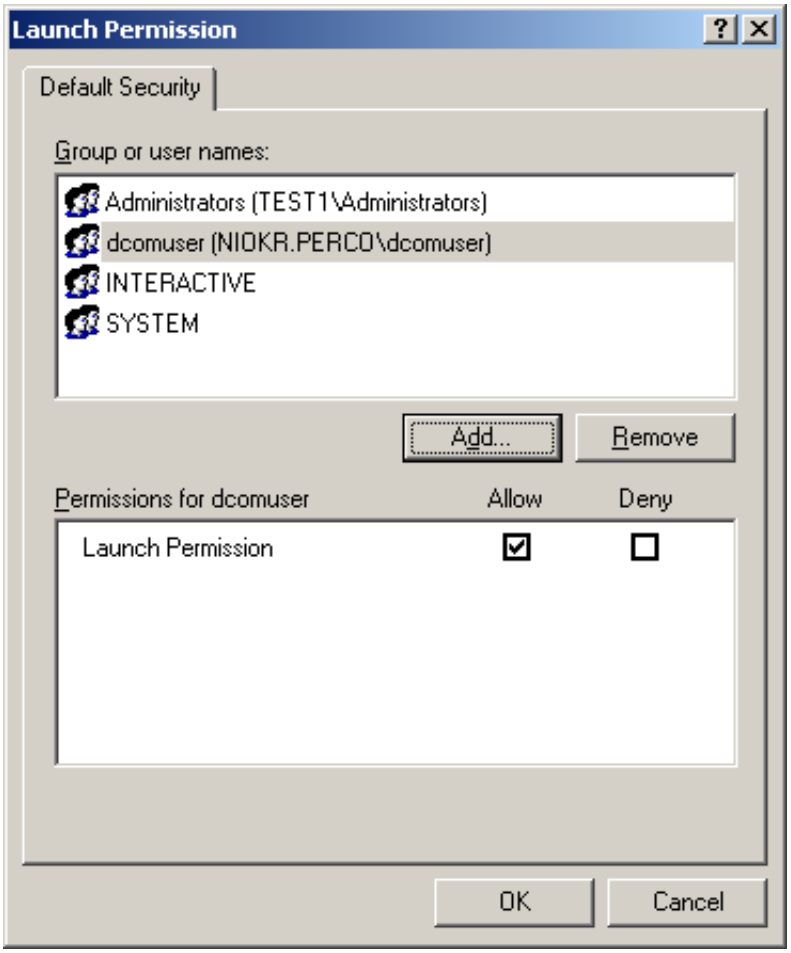
После добавления группы необходимо настроить права доступа:

1) В списке имен пользователей выберите «SYSTEM» и группу пользователей «DCOMUser»;
2) Для разрешения доступа в поле «Permissions» выберите значение «Allow»;
3) Для удаления пользователя воспользуйтесь кнопкой "Удалить" ("Remove").



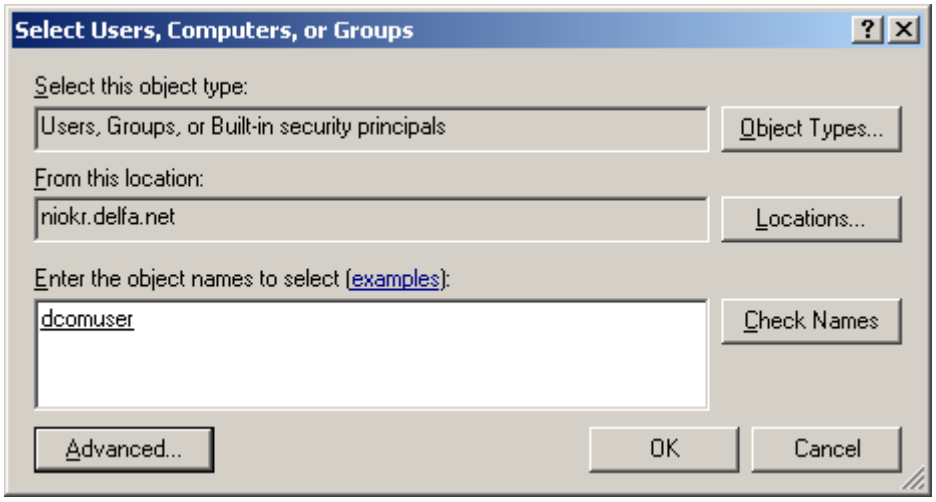
Разрешение запуска приложений по умолчанию

Для изменения стандартных разрешений запуска в поле «Разрешения запуска по умолчанию» («Default Launch Permissions») нажмите кнопку «Изменения умолчаний» («Edit Default»). При этом появится диалоговое окно редактирования списка пользователей, имеющих права запуска по умолчанию:



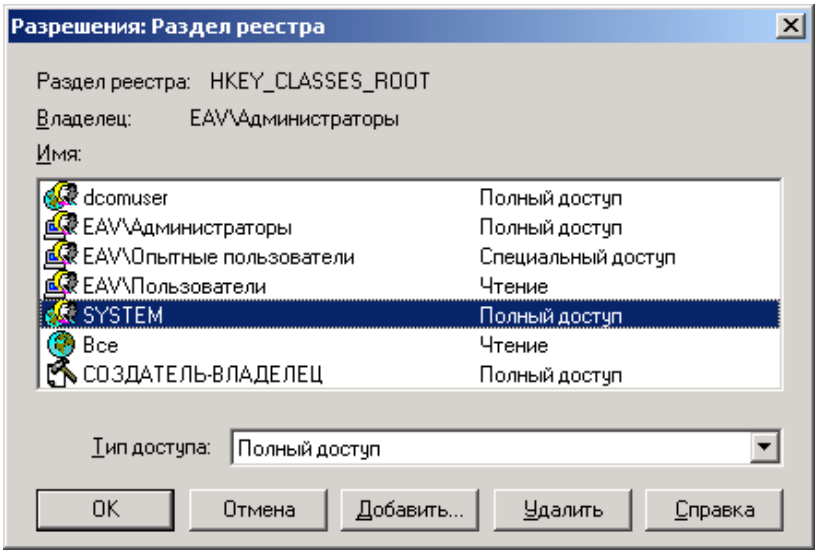
Выберите пользователей «SYSTEM», «ИНТЕРАКТИВНЫЕ» («INTER- ACTIVE»), группу пользователей «DCOMUser» и установите для них в поле «Permissions» значение «Allow», то есть разрешить этим пользователям запускать все объекты.

Для добавления пользователя или группы пользователей нажмите кнопку «Add». На экране появится окно:

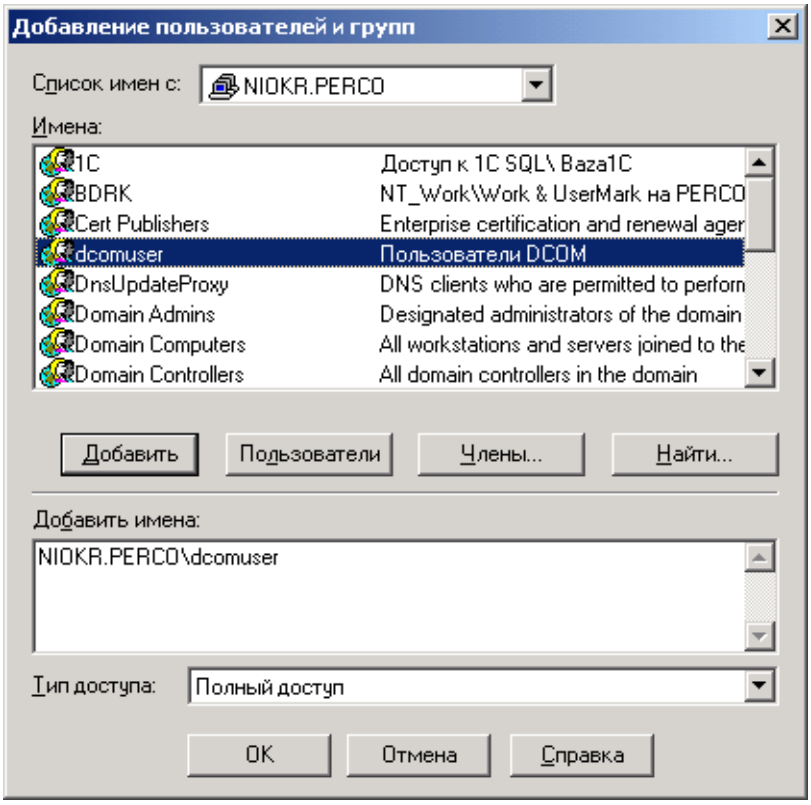


Разрешение настройки по умолчанию

Для изменения стандартных разрешений настройки в поле «Разрешения настройки по умолчанию» («Default Configurations Permissions») нажмите кнопку «Изменение умолчаний» («Edit Default»). Появится диалоговое окно редактирования списка пользователей, имеющих права настройки по умолчанию:



Выберите пользователя «SYSTEM», группу пользователей «DCOMUser» и установите для них в поле «Тип доступа» («Type of Access») в выпадающем списке — «Полный доступ» («Full Control»), то есть разрешите этим пользователям конфигурировать все объекты. Нажмите кнопку «Добавить»:

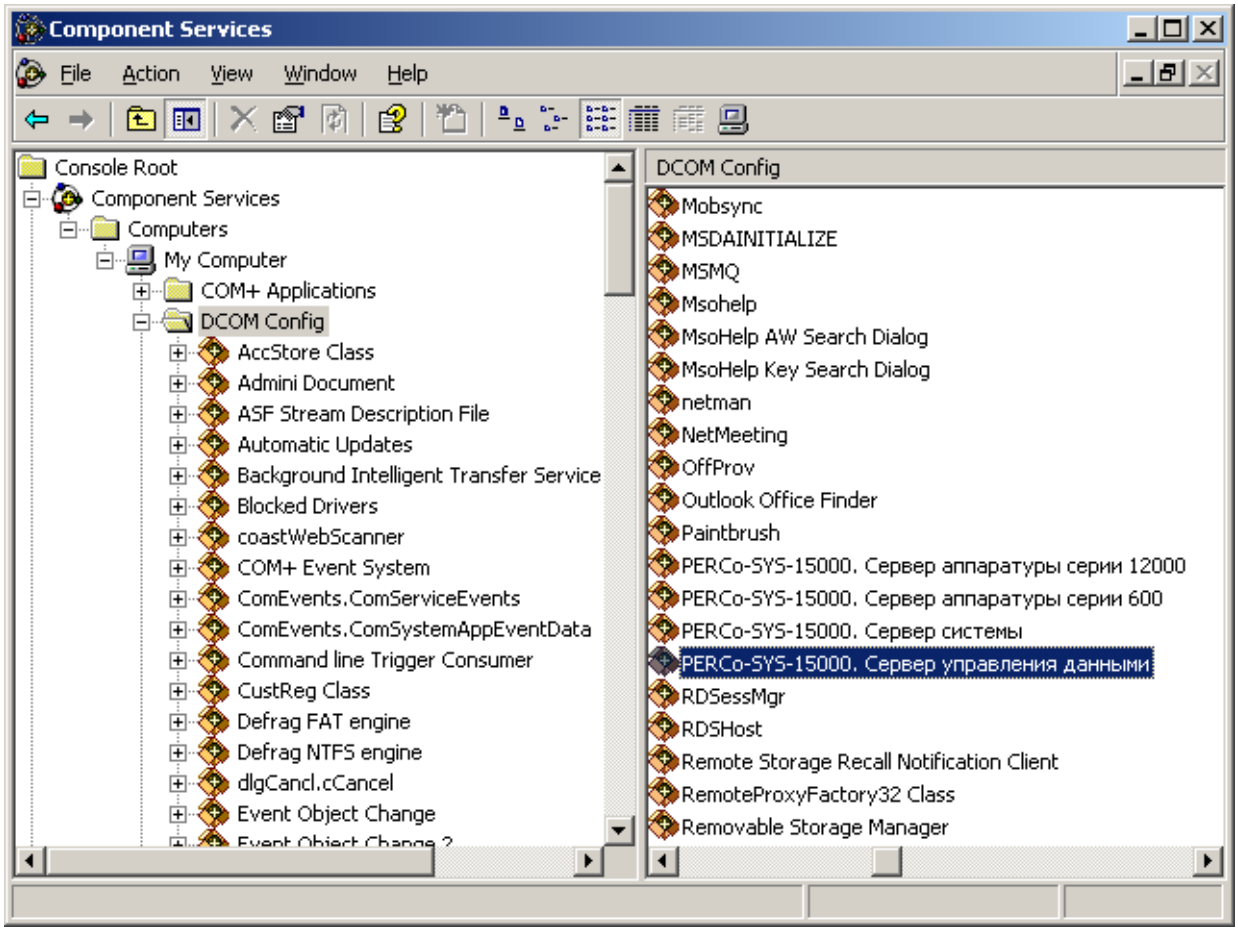


По окончании настройки параметров DCOM, используемых по умолчанию, можно приступать к настройке параметров определенного приложения.

Настройка объектов DCOM

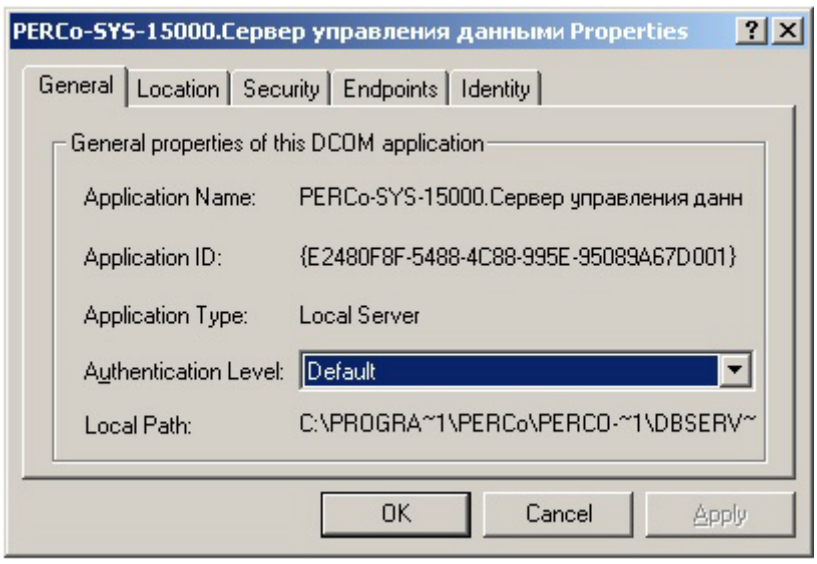
Настройки осуществляются в следующей последовательности:

1) Выберите из списка на странице «Приложения» («Applications») одно из приложений: PERCo-SYS-15000. Сервер аппаратуры серии 600», «PERCo-SYS-15000. Сервер аппаратуры серии 12000», «PERCo-SYS-15000. Сервер управления данными» и «PERCo-SYS-15000. Сервер системы» (для каждого сервера настройка проводится одинаково).

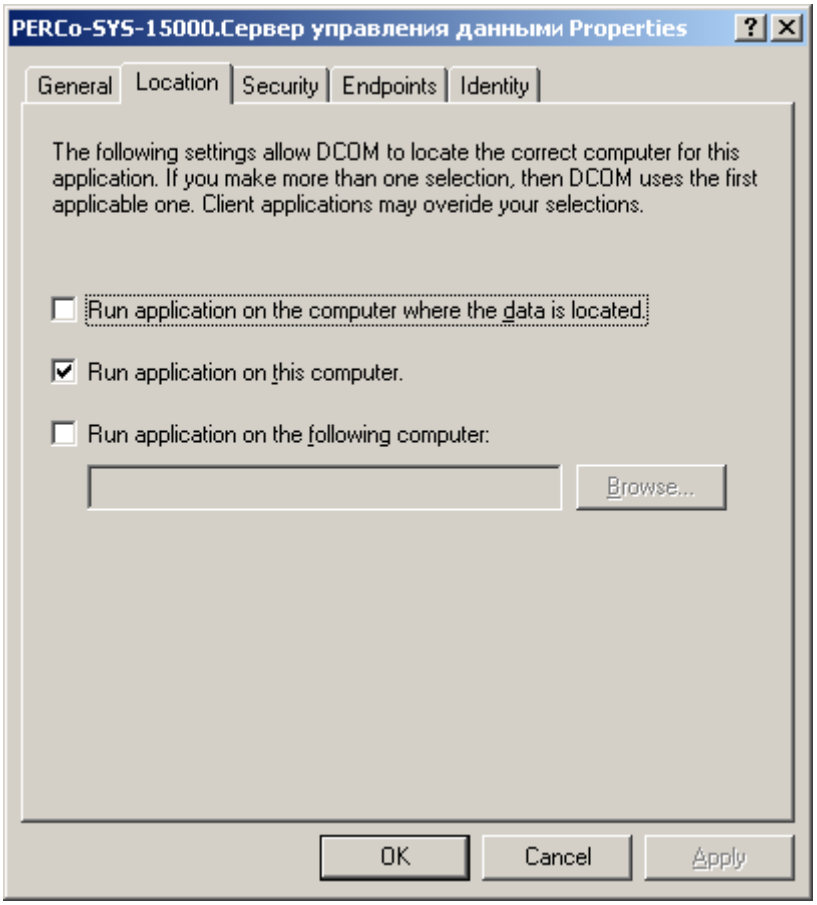


2) Выберите пункт «Properties» контекстного меню. В открывшемся окне на закладке «Общие» («General») показаны свойства выбранного приложения. Здесь можно установить «Уровень проверки подлинности» («Authentication Level»).

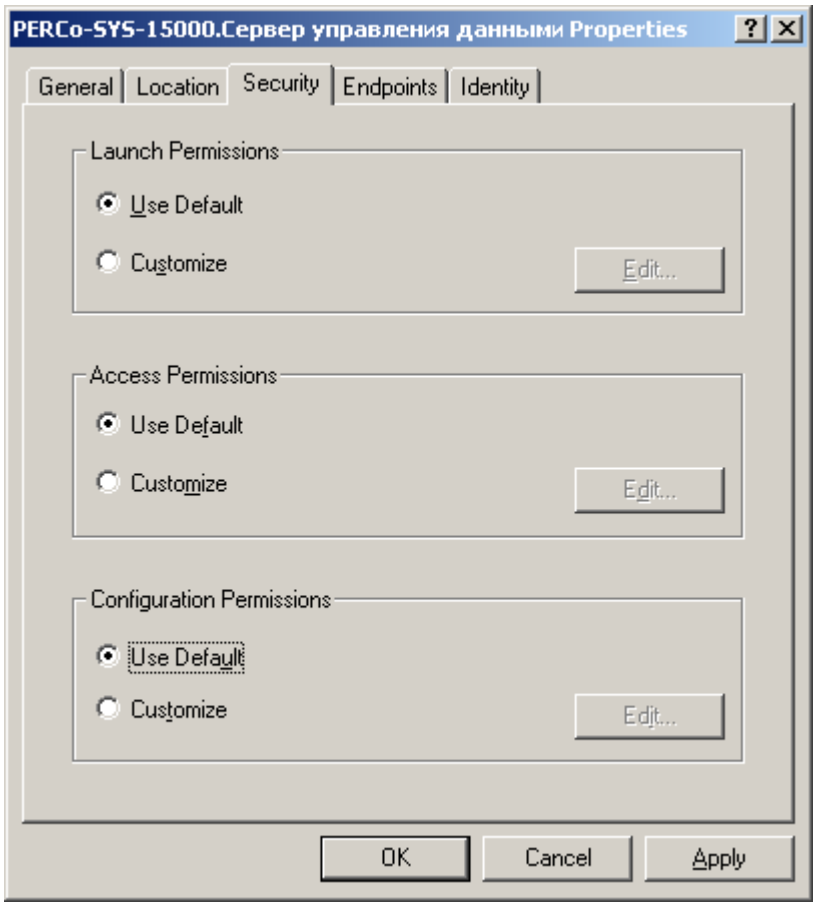
Рекомендуемое значение указано на рисунке:



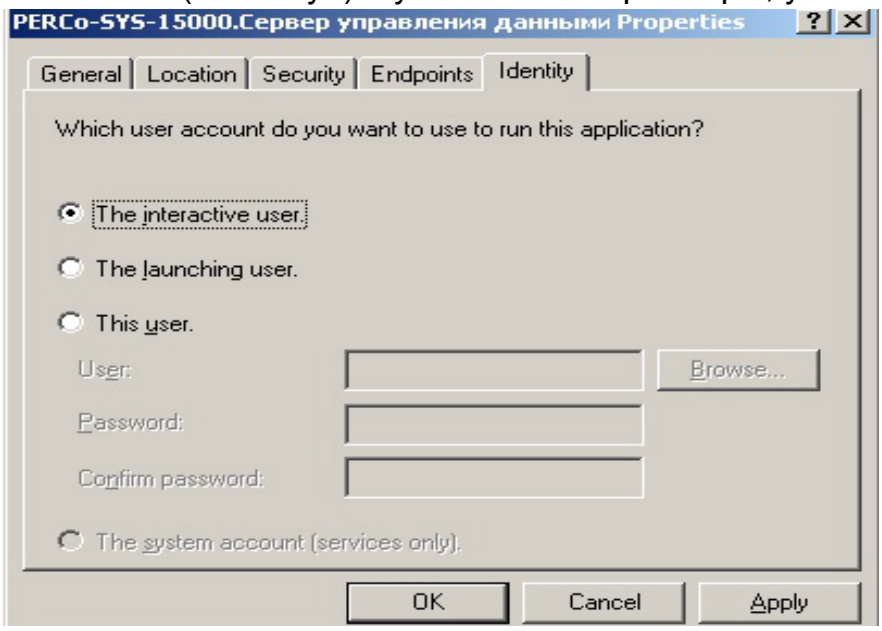
3) На закладке «Размещение» («Location») установите параметры, указанные на рисунке:



4) Для установки безопасности по умолчанию перейдите на закладку «Безопасность» («Security») и установите параметры, указанные на рисунке:



5) Для установки метода идентификации по умолчанию перейдите на закладку «Учетная запись» («Identify») и установите параметры, указанные на рисунке:



4.3. Настройка DCOM в операционной системе Windows Server 2003

Настройка DCOM в операционной системе Windows Server 2003 производится так же, как и в Windows XP.

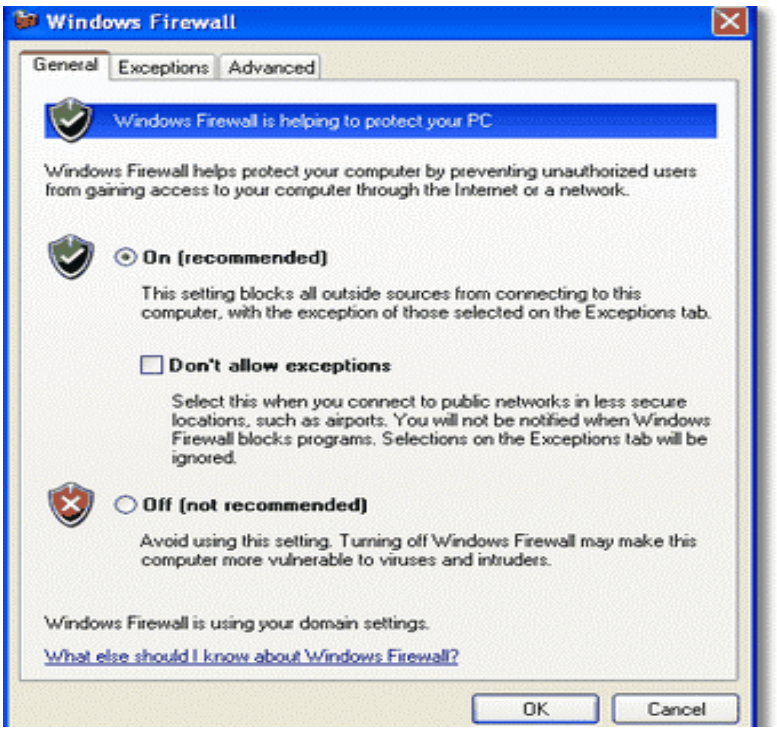
4.4.Настройка DCOM на Microsoft Windows XP SP2

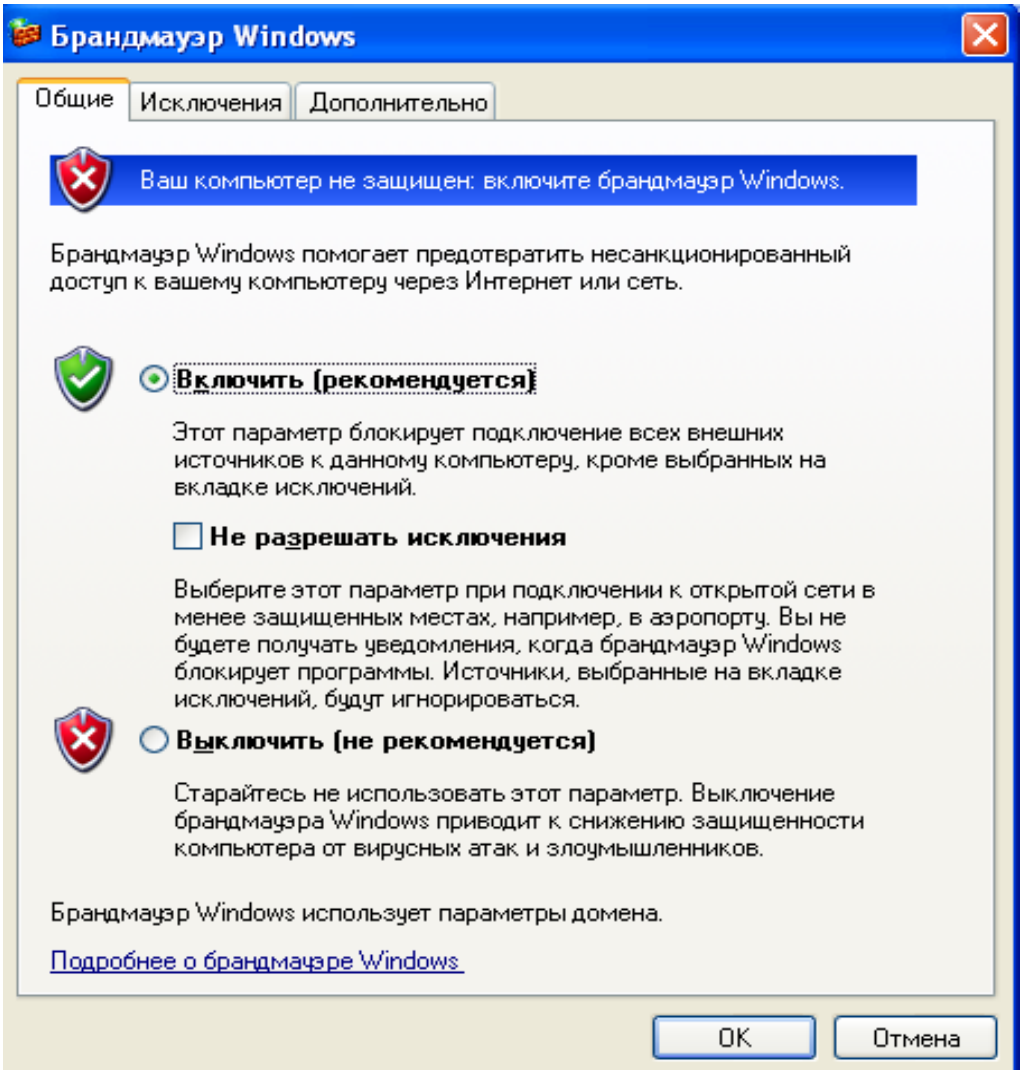
Для обеспечения работы сервера аппаратуры на компьютере под управлением Microsoft Windows XP SP2 необходимо выполнить настройку встроенного в данную систему "Security Center" и изменить некоторые настройки DCOM.

Все перечисленные ниже действия необходимо выполнить из-под учетной записи администратора данного компьютера.

4.4.1 Настройка встроенного Firewall:

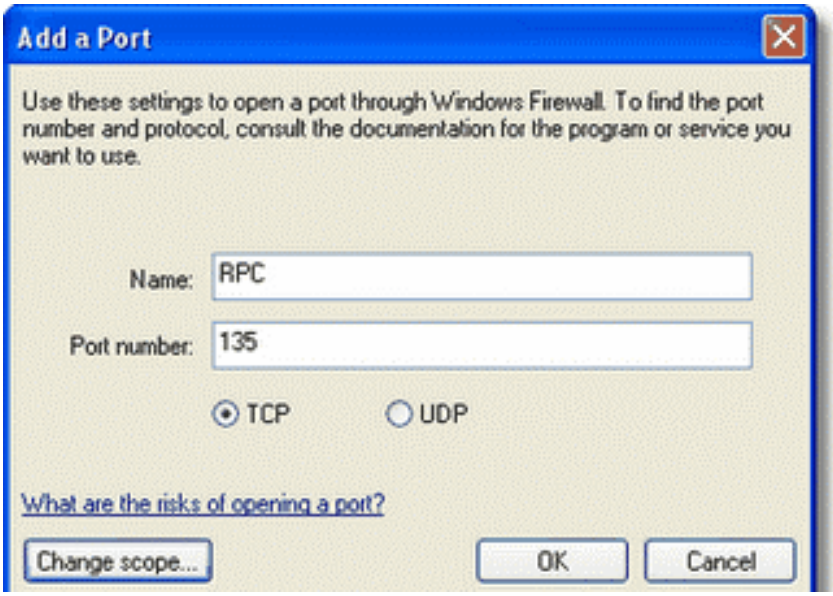
Итак, нажмите кнопку "Пуск", выберите пункт "Программы" (All Programs) ➔ "Стандартные" (Accessories) ➔ "Служебные" (System Tools) ➔ "Центр безопасности" (Security Center), после чего перед вами появится окно:

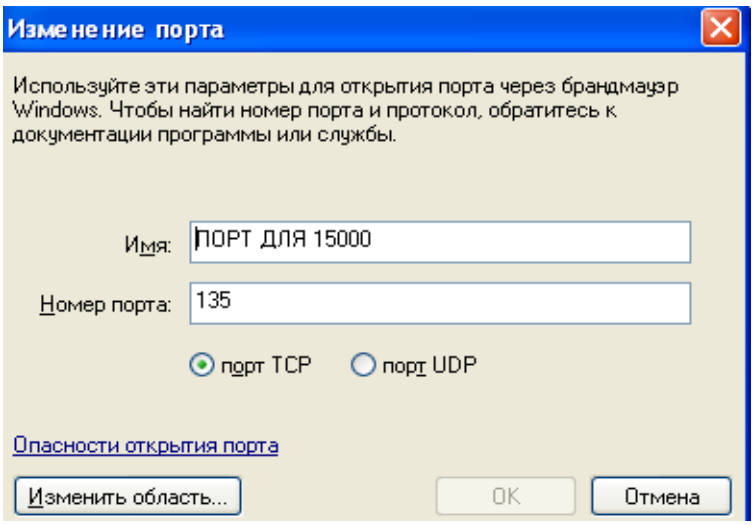




Если Firewall находится в положении "Выключен" (Off), вы можете пропустить этот абзац, и перейти сразу к настройке DCOM.

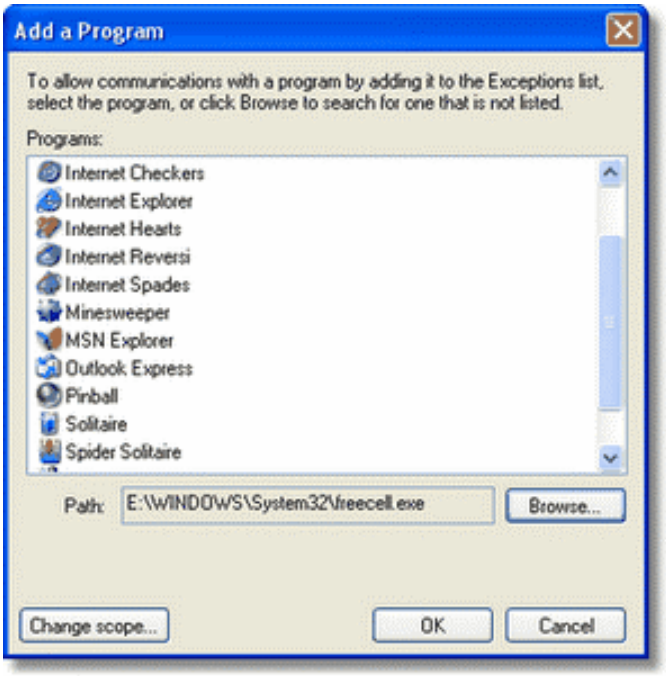
На приведенном выше рисунке Firewall включен. В этом случае убедитесь, что пункт "Don't allow exceptions""Не разрешать исключения" не отмечен (т.е. положение, как на рисунке выше). Откройте вкладку "Исключения" (Exceptions), нажмите "Добавить порт" (Add Port), и в появившемся на экране окне введите: Имя (Name): RPC (или любое понятное для вас название), Номер порта (Port Number): 135, тип: TCP.

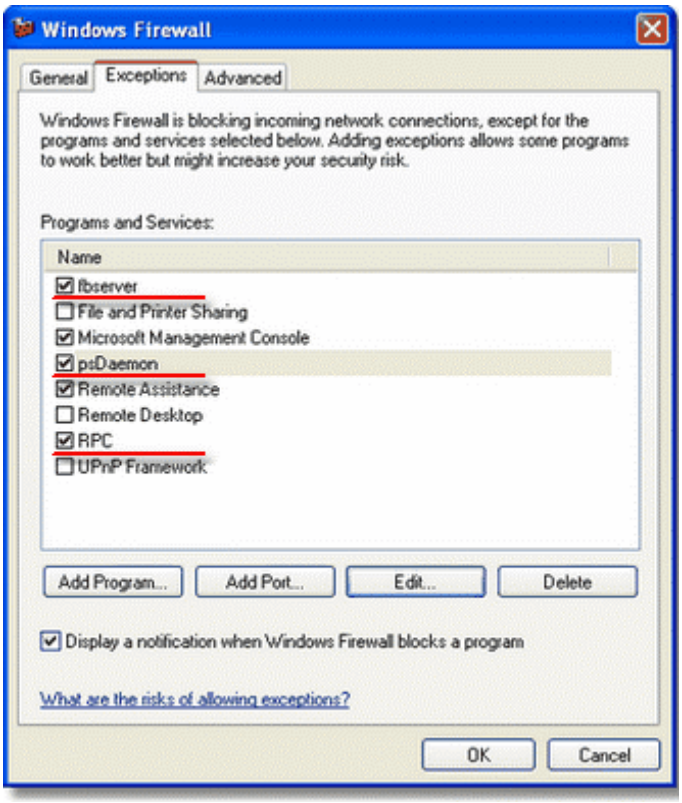


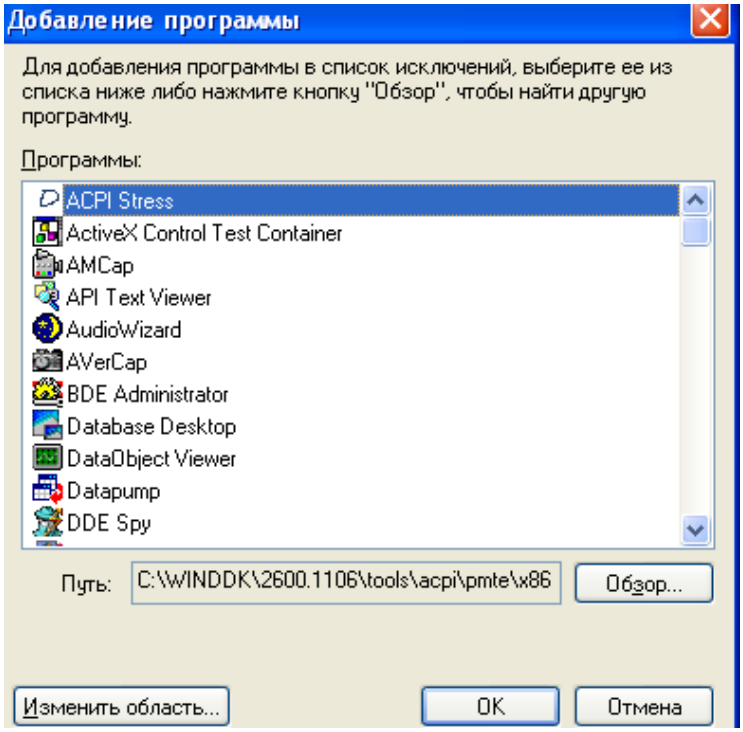


Этим действием вы разрешите компьютеру принимать DCOM-подключения с других компьютеров. Убедитесь, что введенные вами значения в точности соответствуют приведенным на рисунке выше и нажмите кнопку "ОК".

Далее на той же вкладке "Исключения" (Exceptions) и нажмите "Добавить программу" (Add Program):

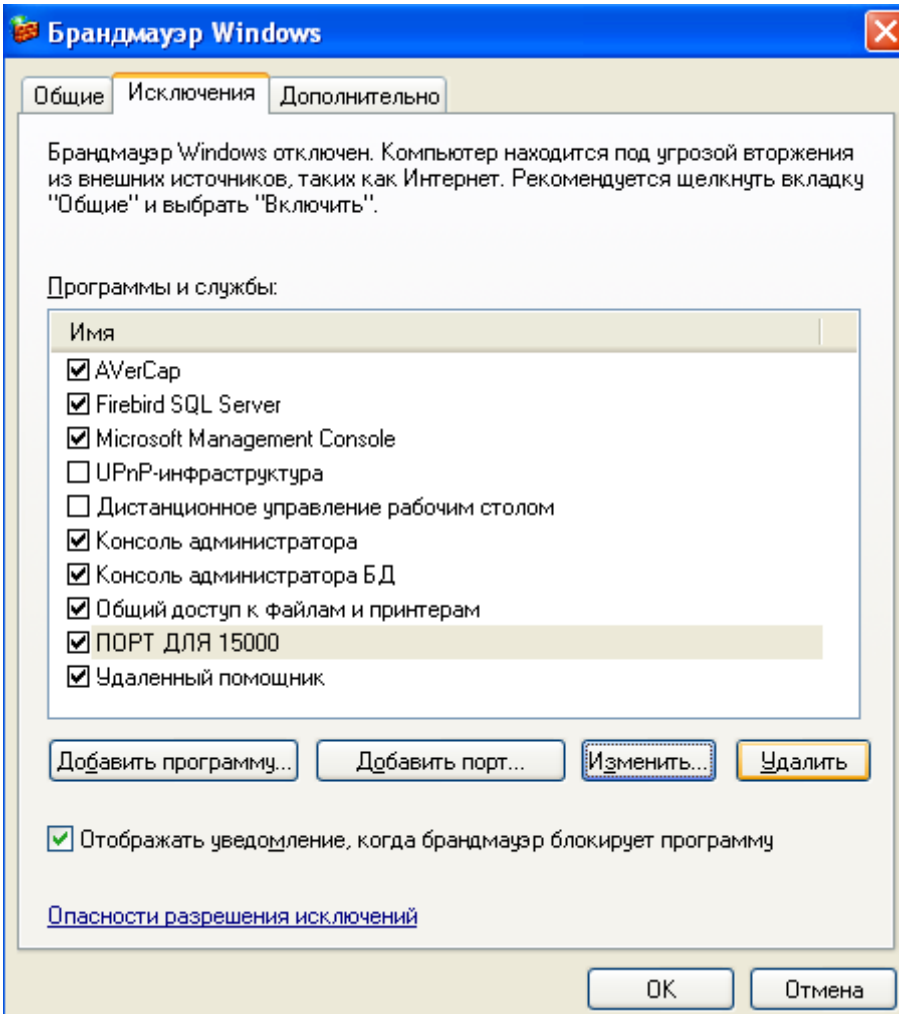






В появившемся диалоговом окне нажмите кнопку "Обзор" (Browse), и выберите программы **DBServer15k.exe, SServer15K.exe, HWServer12K.exe, HWServer600.exe** из папки, куда был установлен сервер управления базой данных (По умолчанию — эта папка "C:\Program Files\PERCo-SYS-15000"), затем точно таким же образом программу **fbserver.exe** из папки "C:\Program Files\Firebird\bin".

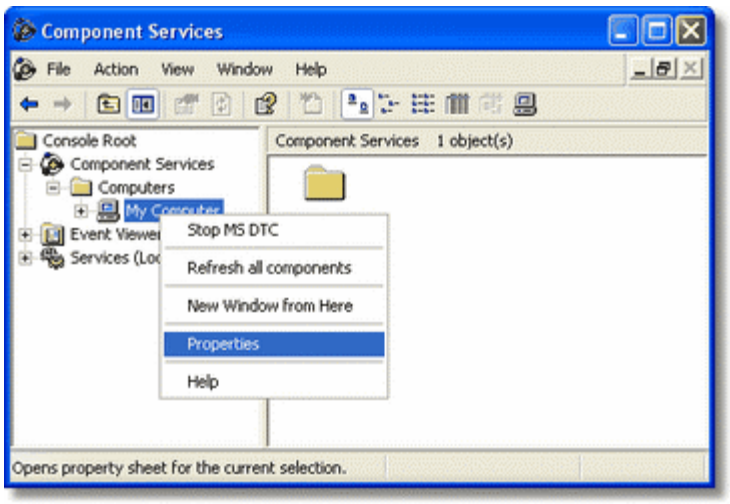
Естественно, вы можете расположить каждый сервер на отдельном компьютере, в этом случае вышеописанные действия,для каждого из серверов, необходимо осуществить на каждом из них, где установлена ОС Windows XP SP2.
После выполнения этих действий закладка "Исключения" (Exception) должна выглядеть примерно так ➔:

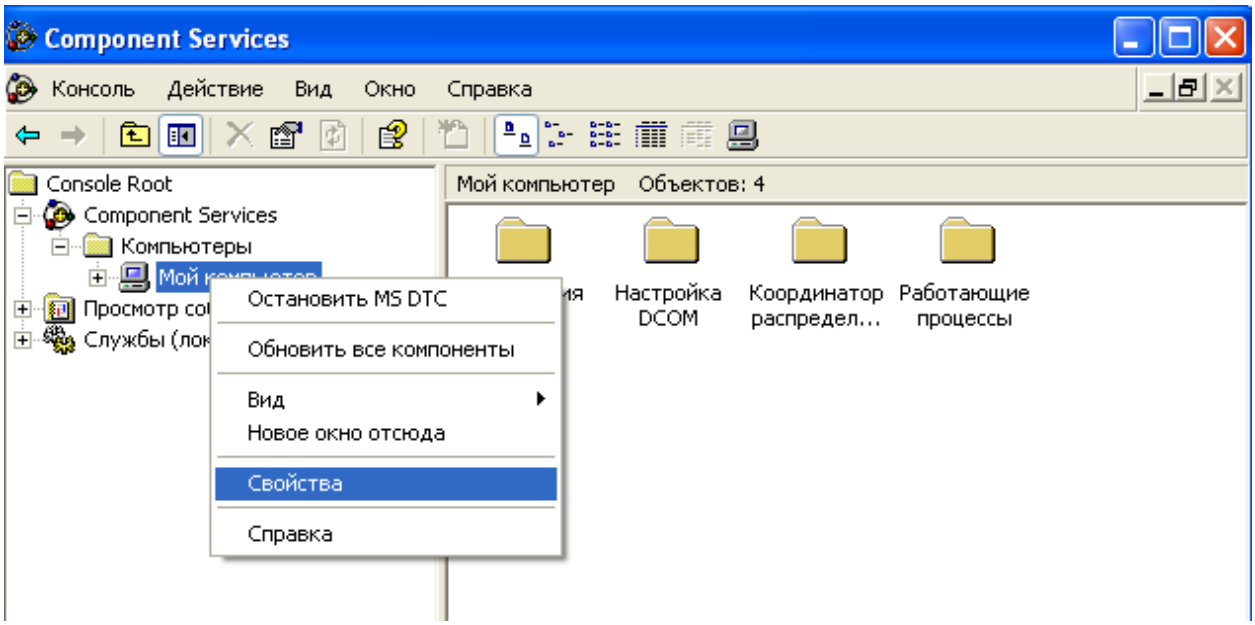


Убедитесь, что все пункты: fbserver, **DBServer15k.exe, SServer15K.exe, HWServer12K.exe, HWServer600.exe** и RPC, подчеркнутые красным на рисунке, присутствуют у вас на экране и отмечены "галочкой".
На этом настройка Firewall закончена и можно переходить к настройке DCOM.
Нажмите кнопку "Ок".

4.4.2. Настройка DCOM:

Нажмите кнопку "Пуск", выберите пункт "Выполнить" (Run), и в появившемся окне выполните команду "**dcomcnfg**" (Без кавычек), после чего на экране появится следующее окно:

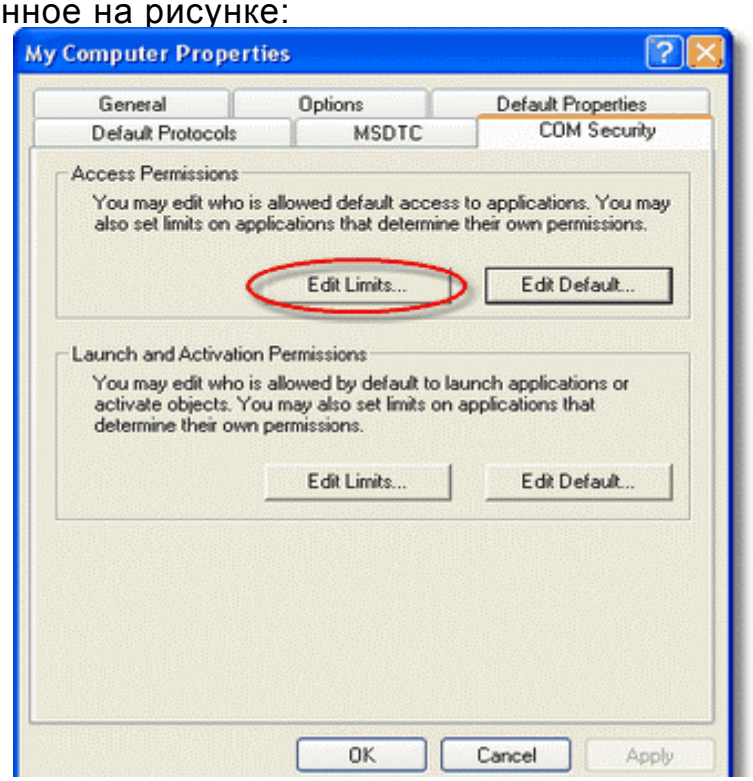


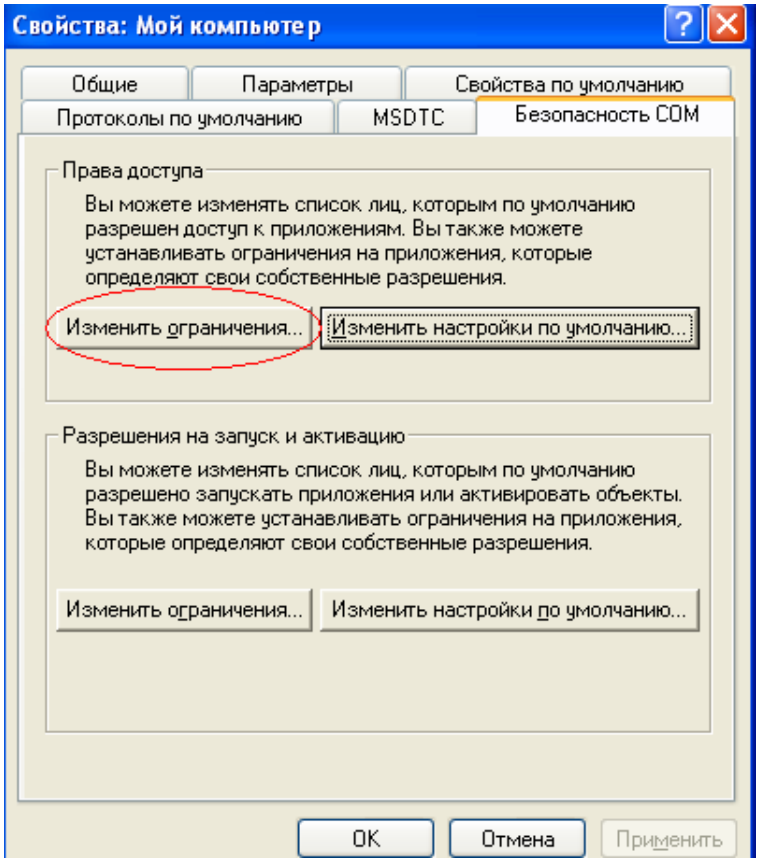


Примечание: при первом запуске этой программы на экране может появиться окно предупреждения следующего содержания:

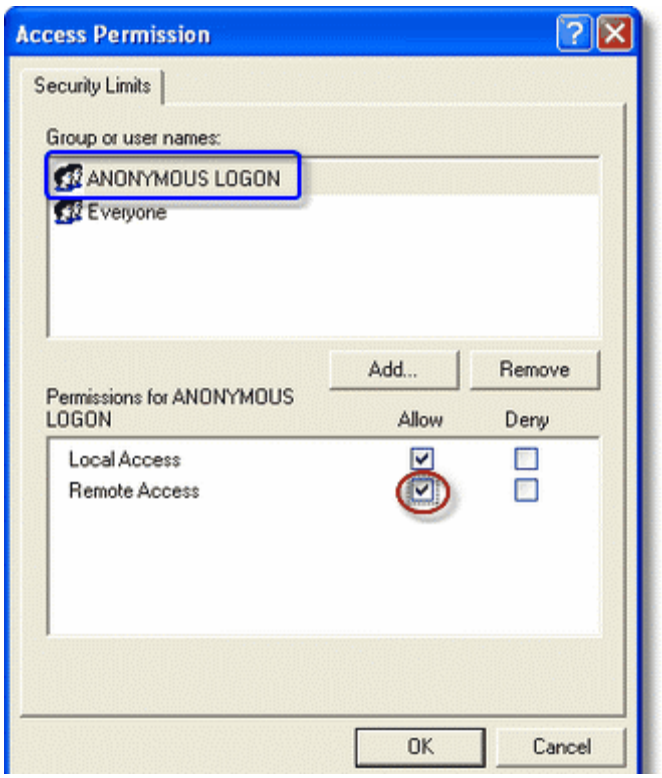
Не обращайте внимание на это сообщение, нажмите "Разблокировать" (Unblock) или "Напомнить позднее" (Ask me Later).

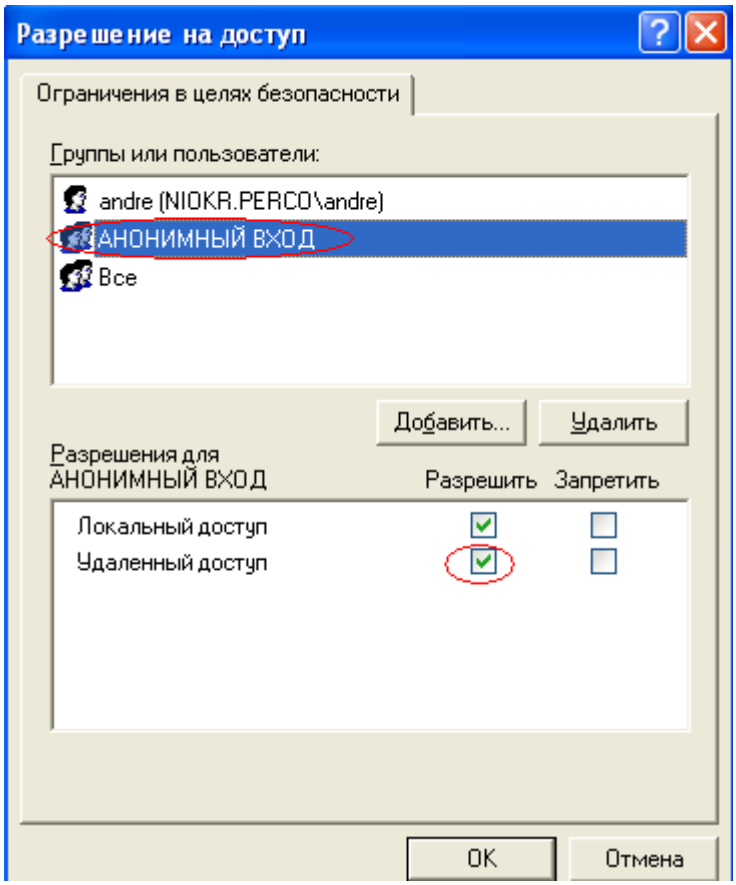
Далее, выберите в древовидном списке в левой части окна пункт "Component Services" ➔ "Computers" ➔ "My Computer" и с помощью правой кнопки мыши вызовите контекстное меню этого элемента. В раскрывшемся меню выберите пункт "Свойства" (Properties), после чего на экране появится окно "My Computer Properties", показанное на рисунке:





Откройте вкладку "Com Security""Безопасность COM", и нажмите "Edit Limits" ("Изменить ограничения") в разделе "Access Permissions" ("Права доступа") (Кнопка выделена на рисунке выше), после чего на экране появится следующее диалоговое окно "Access Permissions(Разрешение на доступ)":





В списке "Group or User Names(Группы или пользователи)" выделите пункт "ANONYMOUS LOGIN(Анонимный вход)" (***Отмечен на рисунке***), и в списке ниже поставьте "галочку" в столбце "Allow" строки (Локальный доступ) "Remote Access(Удаленный доступ)" (***Отмечена на рисунке***). После чего закройте все открытые окна нажатием кнопки "Ок" и перезагрузите компьютер, на этом настройка DCOM закончена.

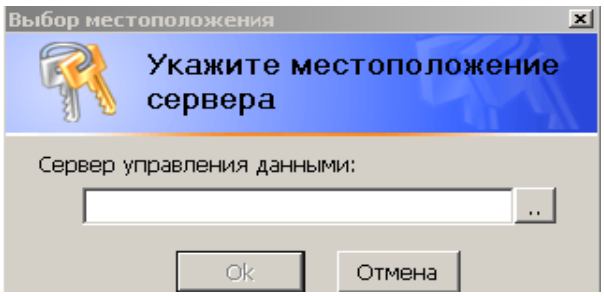
Следует учесть, что Анонимный вход следует настраивать и на компьютерах, где не установлены сервера, а только Консоль Управления 15000 системы.

5. НАСТРОЙКА БАЗЫ ДАННЫХ

5.1. Создание файла базы данных

Для создания файла базы данных нажмите кнопку «Пуск» на панели задач Windows, выберите меню «Программы». В выпадающем окне найдите строку «PERCo» и наведите на нее курсор мыши. После этого выберите «СКУД PERCo-SYS-15000», затем «Консоль администратора БД».

При первом запуске появится окно «Выбор местоположения»:



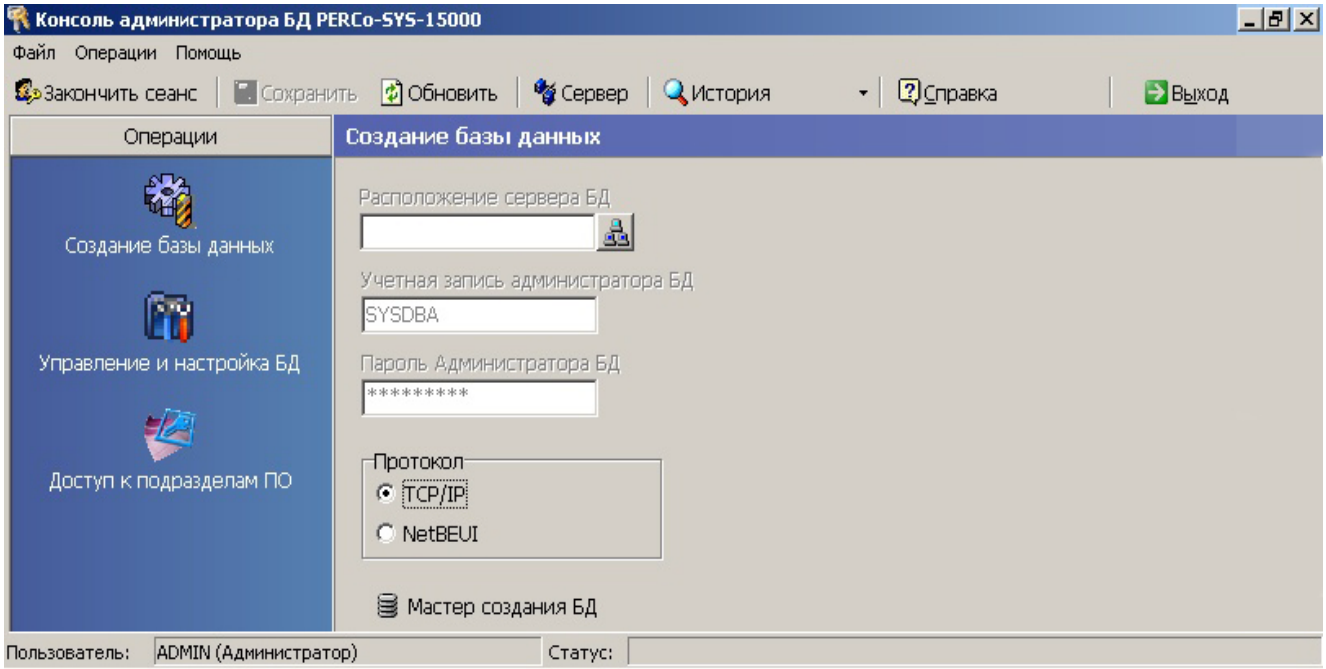
Расположение сервера управления данными — это имя компьютера, на котором установлен сервер приложений по работе с БД.

Имя компьютера можно задать, либо с помощью списка компьютеров, выпадающих при нажатии кнопки справа, либо ручным способом, введя его при помощи клавиатуры.

При нажатии кнопки на экране высвечивается окно «Обзор компьютеров». Выберите компьютер, к которому подключена аппаратура системы, и подтвердите выбор.

После проведения данных операций, вы получаете доступ к созданию базы данных.

Далее появится следующее окно:



Программное обеспечение имеет удобный русскоязычный интерфейс, аналогичный большинству современных приложений Windows.

Окна программ состоят из неизменной части (строка основного меню программы и панель вызова разделов программы) и изменяющейся части (окно вызванного раздела). В зависимости от выполняемых операций, содержимое окон меняется.

Управление системой осуществляется из окон программ с помощью функциональных кнопок.

В верхней части окна располагается строка основного меню программы. В левой части окна располагается панель вызова разделов программы. Центральную часть окна занимает окно вызванного раздела.

Строка меню программы «Консоль администратора БД» включает в себя следующие кнопки:

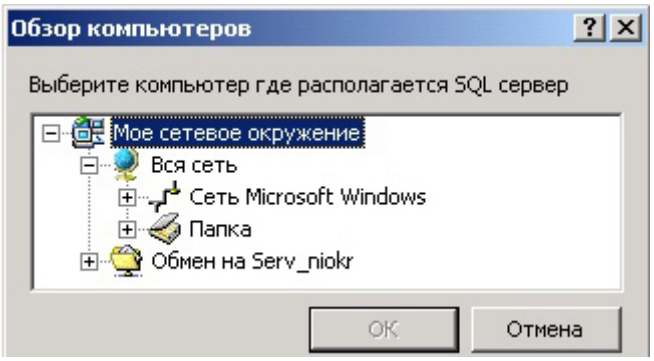
- «Файл» — позволяет выйти из программы)
- «Операции» — кнопка, вызывающая разделы программы)
- «Справка» — позволяет получить справку по ПО, попасть на Интернет сайт компании PERCo, отправить письмо или получить справочную информацию о компании)

Ниже располагаются кнопки:

- «Закончить сеанс» — управление сеансом работы пользователя с программой
- «Сохранить» — сохранение всех изменений
- «Обновить» — обновление данных
- «Сервера» — установление местоположения серверов
- «История» — показ истории переключения подразделов программы

Для создания базы данных необходимо осуществить следующие действия:

1) Выбрать сервер БД. Это — компьютер, на котором установлен и уже запущен SQL- сервер Firebird 1.5. Он может совпадать с расположением сервера управления данными, а может и не совпадать. Для этого следует нажать на кнопку , вызвав диалоговое окно:

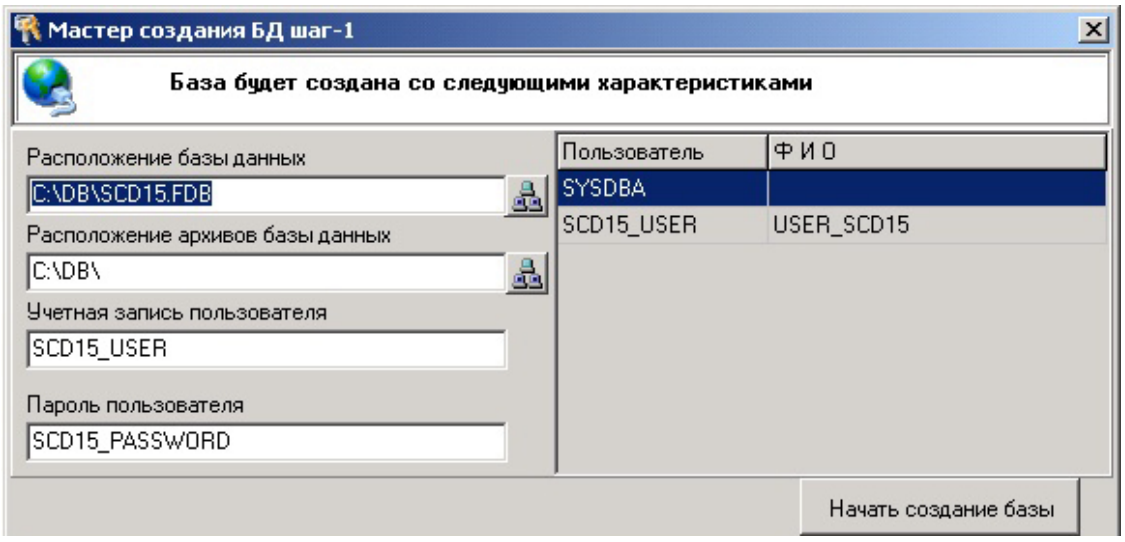


2) Ввести имя администратора базы: «SYSDBA»;
3) Ввести пароль администратора БД (системный пароль по умолчанию — «masterkey»). Если у вас уже был ранее установлен SQL-сервер Firebird 1.5, то введите существующий пароль;
4) Указать протокол соединения с SQL-сервер Firebird 1.5;
5) нажмите кнопку «Сохранить».

После ввода пароля станет доступна кнопка «Мастер создания БД».

Операция по созданию БД включает 2 шага:

Шаг-1



1) Укажите путь к тому месту, где будет создан файл базы данных. Это путь к компьютеру, где был ранее установлен SQL-сервер Firebird 1.5. Папку, в которой вы создаете файл базы данных, для повышения безопасности не рекомендуется предоставлять в общее пользование. Если база находится на том же компьютере, что и сервер управления, вы можете выбрать путь с помощью кнопки , если нет, то кнопка будет не активна, и вы должны ввести путь вручную;

2) Укажите путь к архиву базы данных. Это — путь к директории, где будут создаваться архивные копии файла базы данных. Имя самого файла базы данных и архива лучше не изменять. Имя директории может вводиться вручную (тогда это директория на компьютере, где находится SQL-сервер) или выбираться нажатием на кнопку . В этом случае можно выбирать директорию, к которой предоставлен общий доступ с любого компьютера сети. Если SQL-сервер запущен как сервис, то данному сервису должен быть предоставлен полный доступ к директории, если SQL-сервер запущен как приложение, то учетной записи, под которой он запущен, должны быть предоставлены права на директорию;

3) Введите имя пользователя, который будет создателем и владельцем файла базы данных (оставьте предопределенное);

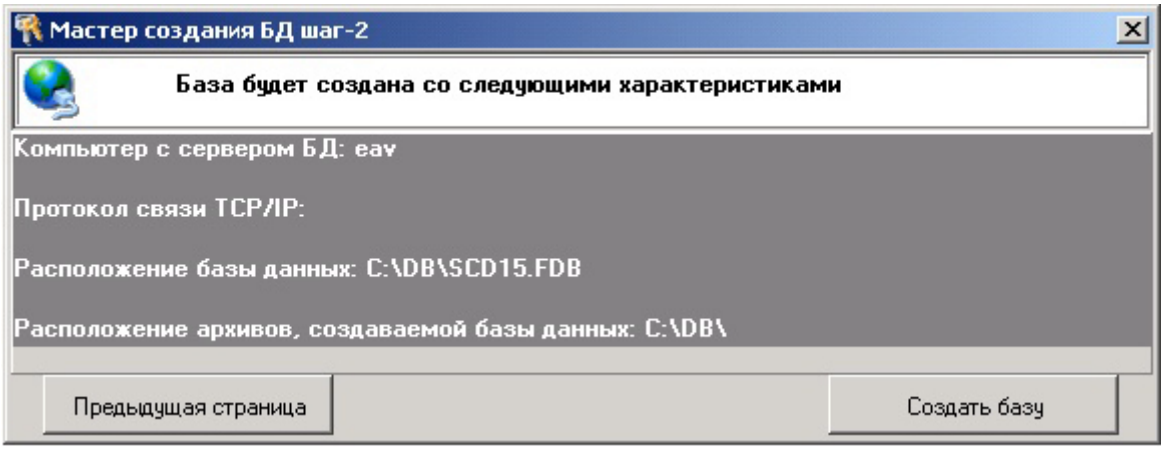
4) Введите пароль пользователя для доступа к БД (оставьте предопределенный).

Примечание: пользовательские имя и пароль указываются один раз при создании базы данных. Они не имеют отношения к реальным пользователям, которые получат доступ к БД из клиентских приложений.

В правой части окна виден список пользователей, зарегистрированных на сервере БД.

После ввода всех характеристик нового файла баз данных, нажмите кнопку «Начать создание базы».

Шаг-2



Второй шаг создания базы введен для страховки, чтобы пользователь проверил введенные параметры.

После осуществления данных операций, нажмите кнопку «Создать базу», и если все параметры введены корректно, то файл базы будет создан.

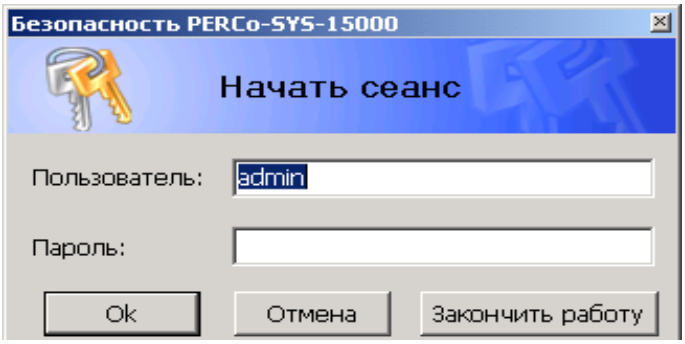
После создания базы можно работать с любым разделом программного обеспечения системы PERCo-SYS-15000.

Для проведения дальнейших настроек требуется закрыть приложение и снова запустить «Консоль администратора БД».

Примечание: после создания базы данных, для загрузки приложения «Консоль администратора БД» по умолчанию используется имя «admin» без пароля (до момента формирования списка администраторов и пользователей системы со своими паролями).

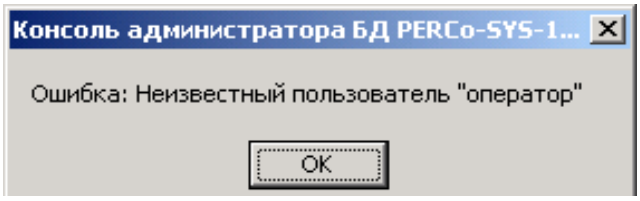
5.2. Работа с консолью администратора БД

При последующих запусках программы на экране появляется диалоговое окно «Начать сеанс», в котором по умолчанию в поле «Пользователь» будет находиться имя «Admin», а поле «Пароль» будет пустым.



Введите имя и пароль и нажмите кнопку «ОК». Система произведет загрузку программы.

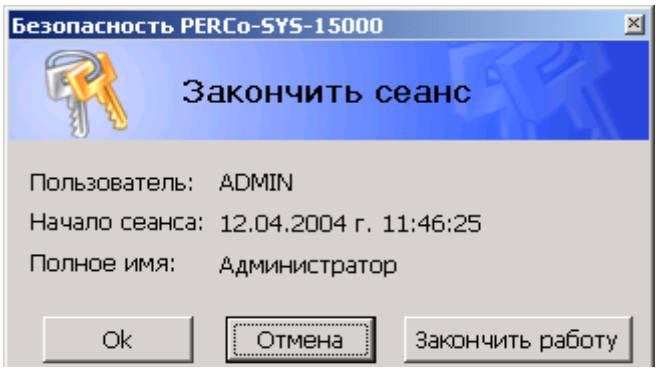
Если имя и/или пароль пользователя были указаны неверно, то программа выдаст информацию об ошибке при вводе имени и пароля:



Нажмите кнопку «ОК». На экране вновь появится окно «Начать сеанс». Введите имя и пароль еще раз.

Сеанс подразумевает работу с конкретным пользователем, имеющим определенные права доступа. Если необходимо приступить к работе другому пользователю с другими правами доступа, то необходимо в меню программы нажать кнопку «Закончить сеанс».

На экране появится диалоговое окно «Закончить сеанс», в котором следует нажать кнопку «ОК».



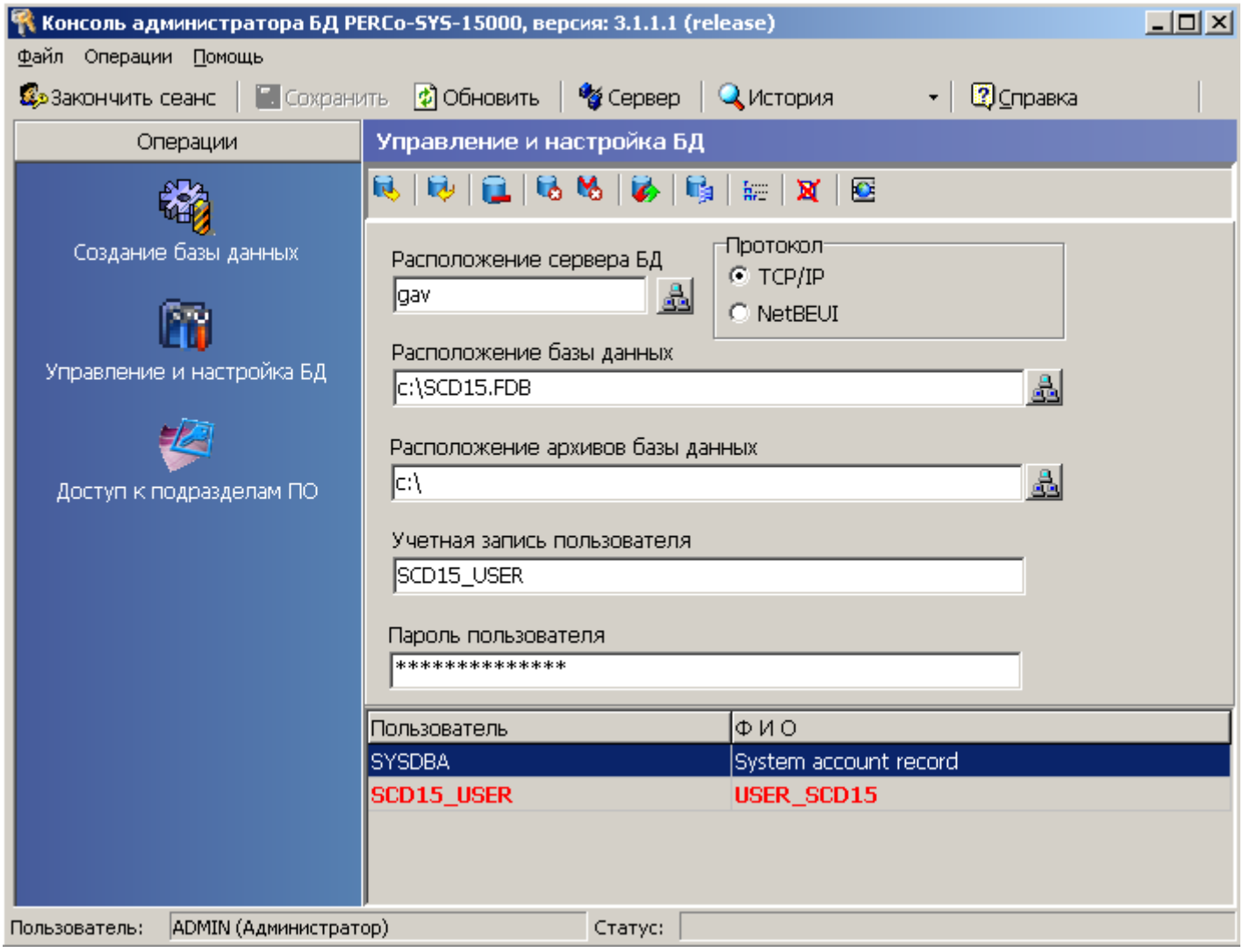
Предыдущий сеанс работы будет завершен, и на экране вновь появится окно «Начать сеанс» с предложением ввести имя нового пользователя и его пароль.

Для выхода из программы в диалоговом окне «Закончить сеанс» следует нажать кнопку «Закончить работу».

5.3. Выбор места расположения резервных копий базы данных

Выбор места расположения резервной копии БД определяется на этапе создания в разделе «Создание базы данных». Создание резервной копии осуществляется в разделе «Управление и настройка БД». В этом же разделе изменяется путь к архиву и местоположение БД. Для внесения изменений необходимо произвести следующие действия:

1) Выбирается имя компьютера, на котором установлен Сервер БД, т.е. указывается имя компьютера, где расположен SQL-сервер Firebird 1.5;
2) Вводится путь к файлу базы данных. Необходимость менять путь к базе может возникнуть при переносе базы. Если база находится на том же компьютере, что и сервер управления, то Вы можете выбрать путь с помощью кнопки , если нет, то кнопка будет не активна, и Вы должны ввести путь вручную;
3) Указывается директория, в которой сохраняются архивные файлы. Имя директории может вводиться вручную (тогда это — директория на компьютере, где находится SQL-сервер) или выбираться нажатием на кнопку . В этом случае можно выбрать директорию, к которой предоставлен общий доступ с любого компьютера сети(не рекомендуется замедляет создание архивов и восстановление) рекомендуется иметь второй HDD на компьютере с сервером FireBird и сохранять ахивы на диск отличный от диска, где находится база;
4) Указывается пользователь, от имени которого создается база данных и его пароль;
5) После консультации с системным администратором выбирается сетевой протокол, принятый в вашей сети;
6) После внесения изменений в поля необходимо нажать кнопку «Сохранить», иначе все настройки при переходе к другой форме будут потеряны.



Красным цветом выделен пользователь, являющийся создателем и владельцем базы данных.

Функциональные кнопки имеют следующее назначение:

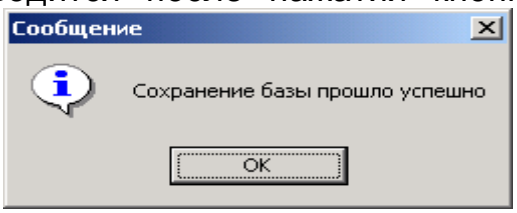
1 2 3 4 5 6 7 8 9 10

1 – «Сохранение базы данных»
2 – «Восстановление базы данных»
3 – «Удаление данных по мониторингу»
4 – «Удаление данных о проходах»
5 – «Удаление событий и кадров видеоидентификации»
6 – «Работа с сохраненными данными о проходах и данных мониторинга»
7 – «Дополнительные настройки»
8 – «Оптимизация индексов базы данных»
9 – «Очистка кэша конфигурации базе данных»
10 - «Обновление версии базы данных»

5.4. Резервное копирование базы данных

Действия по резервному копированию необходимо производить ежедневно, так как, помимо автоматической оптимизации рабочей базы, это позволит иметь архив данных на случай ее повреждения. Это полезно еще тем, что при этом происходит очистка файла БД от устаревших записей.

Выполнение копирования производится после нажатия кнопки (1) — .

По завершению появится сообщение: 

По умолчанию создается одна резервная копия БД, однако количество копий может варьироваться от 1 до 7. Изменение количества резервных копий и просмотр параметров БД осуществляется в дополнительных настройках (см. п. 5.12).

5.5. Восстановление базы данных из резервной копии

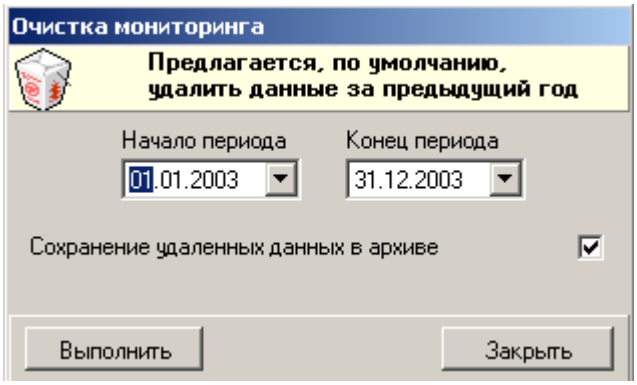
Восстановление данных из архива выполняется при помощи нажатия кнопки (2) - .

Сохраненная копия базы данных после восстановления имеет то же название что и рабочая база, но с добавлением символа «#». После успешного выполнения команды восстановленная база становится рабочей.

При следующем восстановлении копия будет иметь то же название, но уже без символа «#» на конце. После выполнения команды она также сразу станет рабочей. В результате, при нормальной работе существуют 2 файла базы данных (рабочая и предыдущая копия), а также набор архивных копий. Данная особенность создания резервных копий позволяет повысить надежность действий при восстановлении базы данных из архива и обеспечить безусловную работоспособность базы даже при наличии повреждений на диске.

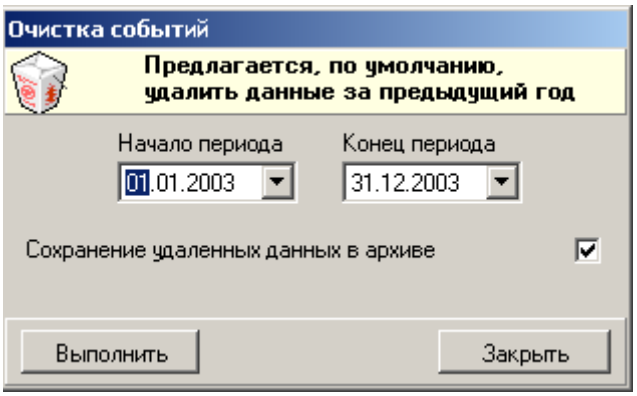
5.6. Удаление из БД данных по мониторингу

Удаление данных по мониторингу можно выполнить после нажатия кнопки (3) - .



5.7. Удаление из БД данных о проходах

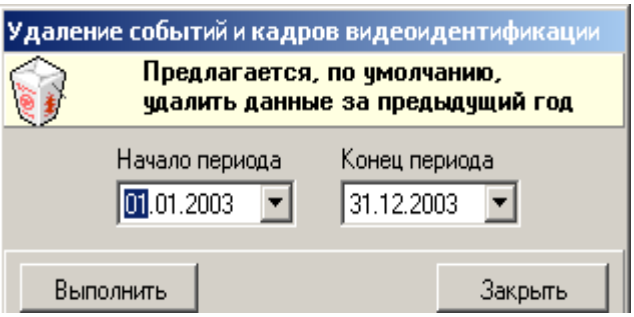
Удаление данных о проходах становится возможным после нажатия кнопки (4) - .



5.8. Удаление событий и кадров видеоидентификации

Удаление событий видеоидентификации из БД и одновременное удаление соответствующих им кадров с диска производится с помощью кнопки (5) - .

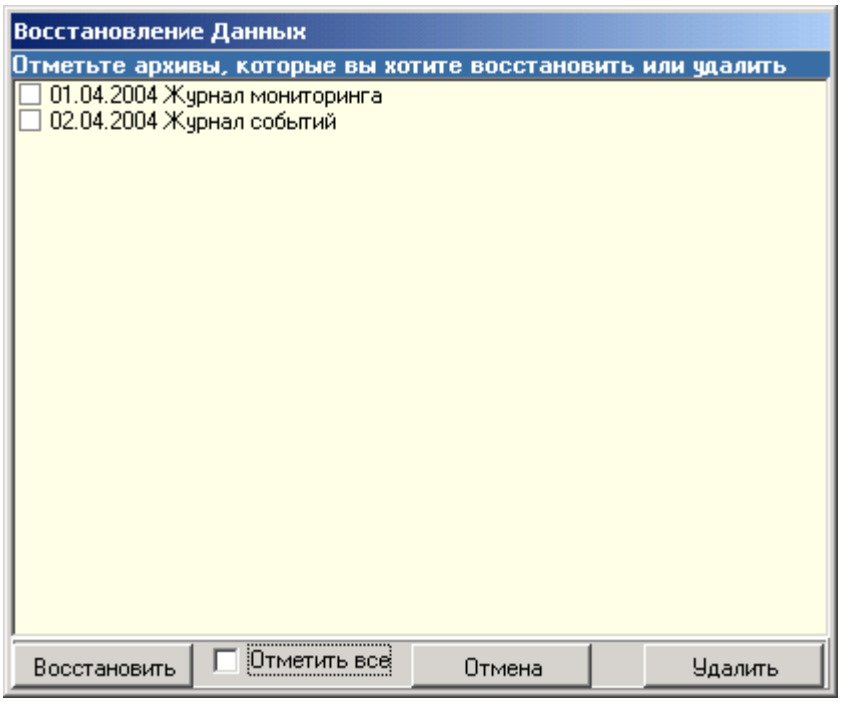
Файлы кадров видеоидентификации хранятся в подкаталоге SnapShots каталога, где размещен “Сервер управления данными” и сгруппированы по годам/месяцам/дням в виде соответствующих вложенных папок (например, папка \SnapShots\2005\01\25 содержит кадры за 25 января 2005 года). Окно, с помощью которого происходит удаление, аналогично окнам для удаления данных мониторинга и данных о проходах:



Если требуется оперативный доступ к событиям за определённый период времени, но для хранения кадров за этот период места на диске с ПО PERCo-SYSTEM-15000 уже недостаточно, то следует переместить папки с кадрами на другой диск данного ПК, или на другой ПК (например, всю папку \SnapShots\2004 с кадрами за 2004-й год). При этом нельзя удалять сами события видеоидентификации, как это было описано выше в данном разделе. Если в дальнейшем возникнет необходимость просмотреть кадры из перемещенной папки, достаточно восстановить её в том же самом виде в папке SnapShots.

5.9. Работа с сохраненными в архиве данными о проходах и данными мониторинга

Можно полностью или частично восстановить удаленные данные о проходах и данные мониторинга путём нажатия на кнопку (6) - и выбором необходимого архива.



5.10. Оптимизация индексов базы данных

Оптимизация индексов осуществляется нажатием на кнопку (8) — (рекомендуется проводить раз в неделю).

5.11. Очистка кэша конфигурации базы данных

Очистка кэша конфигурации осуществляется нажатием на кнопку (9) - и используется при аварийных отключениях питания и других ситуациях, когда ПО начинает работать нестабильно. В этом случае, с большой долей вероятности, «Очистка кэша конфигурации» поможет восстановить работоспособность ПО.

5.12. Дополнительные настройки базы данных

Окно «Дополнительные настройки БД» вызывается нажатием кнопки (7)_- :

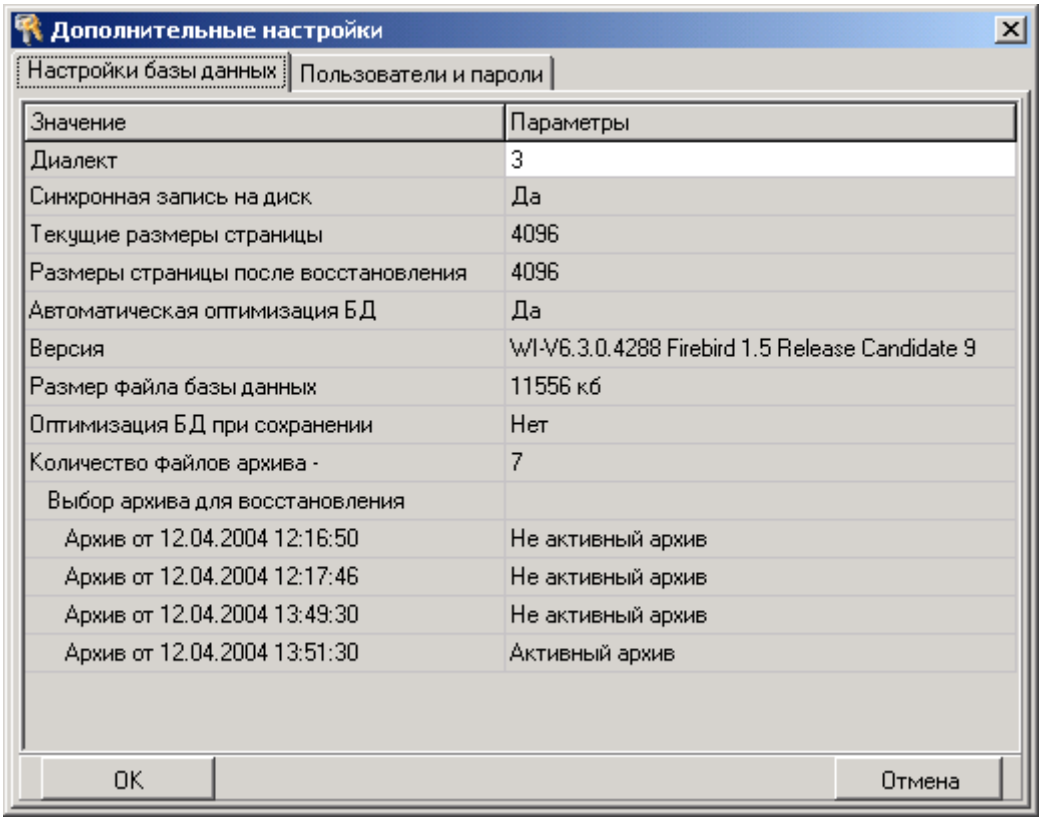
Доступ к дополнительным настройкам возможен только при знании системного пароля SQL-сервера (по умолчанию «masterkey»).

Окно «Дополнительные настройки» включает две закладки «Настройки базы данных» и «Пользователи и пароли».

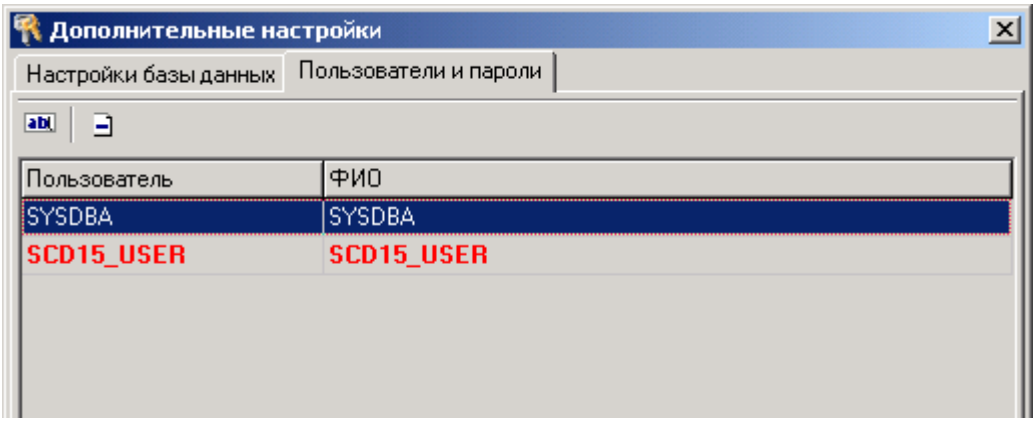
Закладка «Настройки базы данных» включает следующие позиции:

- «Диалект» - сугубо внутреннее представление файла БД для сведения;
- «Синхронная запись на диск» — если SQL-сервер установлен на компьютер с источником бесперебойного питания, то лучше поставить «Нет» (для ускорения записи), в другом случае — «Да»;
- «Текущие размеры страницы» — по умолчанию файл БД создается с размерами страницы 4096 байт;
- «Размеры страницы после восстановления» — указав другой размер после восстановления базы из архива, получим указанный размер страницы. Размер страницы желательно устанавливать равным размеру кластера диска, на котором расположен файл БД;

- «Автоматическая оптимизация БД» — при работе SQL-сервера создаются разные версии записей. При режиме «Да» они чистятся самим сервером, однако это замедляет его основную деятельность. Следует учесть, что сборка «мусора» происходит при сохранении базы данных, которое рекомендуется делать ежедневно. Поэтому рекомендуется выбирать режим «Нет»;
- «Версия» — версия SQL-сервера;
- «Размер файла базы данных» (Кб);
- «Количество Файлов архива» — от 1 до 7. Восстановить можно из любого;
- «Выбор архива для восстановления» — перечень созданных архивов. По умолчанию архив, созданный последним, предназначен для восстановления, однако, при желании, можно сделать активным любой архив.



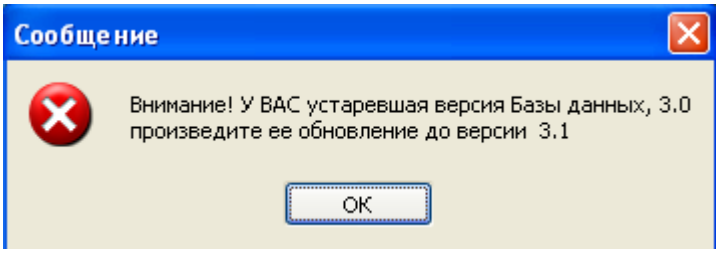
В закладке «Пользователи и пароли» красным цветом выделен пользователь, являющийся создателем и владельцем файла базы данных:



Рекомендуется заменить пароль «masterkey», являющийся общеизвестным, на пароль, известный только администратору системы (пароли регистрозависимы).

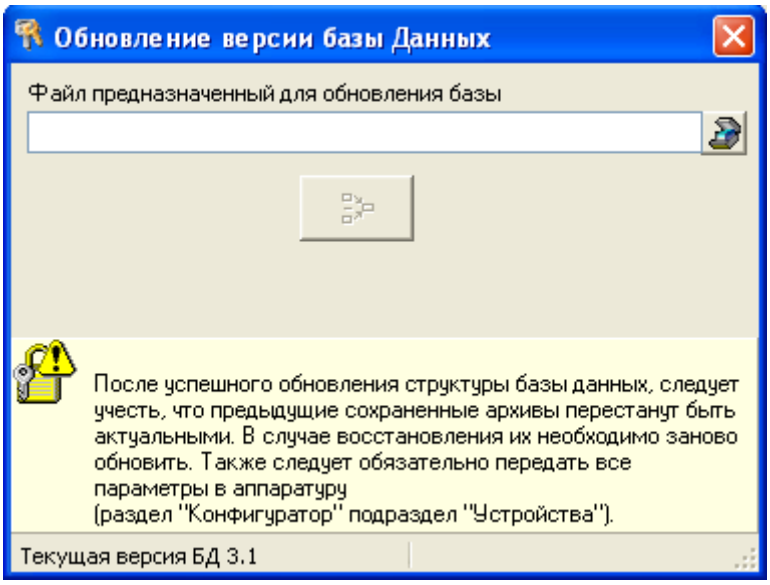
5.13. Обновление базы данных.

При запуске Администратора Баз данных возможно появление следующего предупреждения:

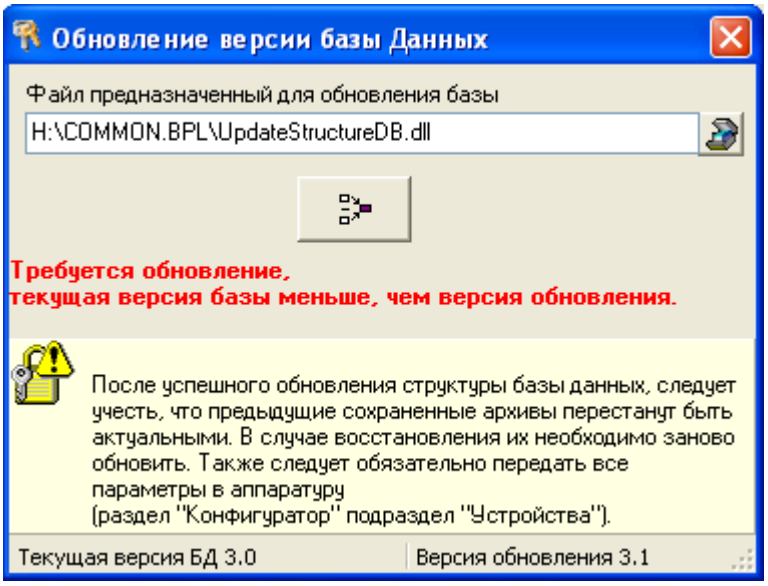


Это означает, что необходимо обновить структуру базы данных

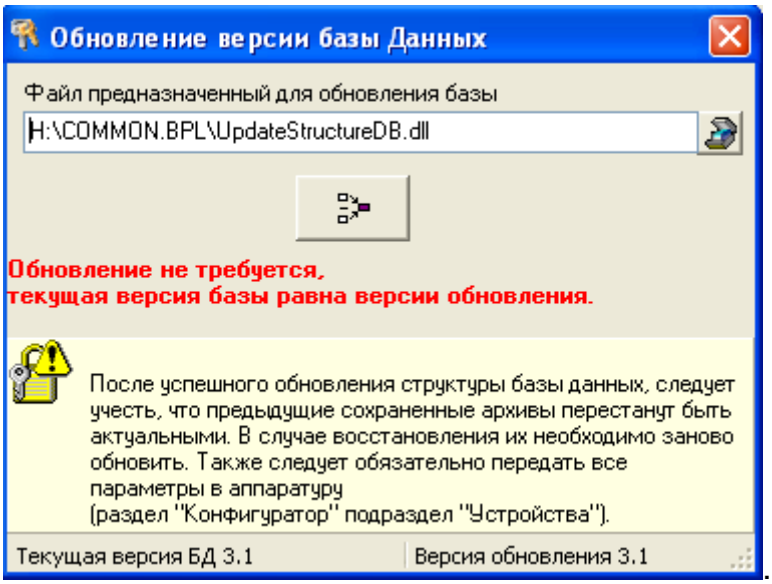
Периодически, по мере обновления программного обеспечения будет рассылаться файл с обновлением базы данных UpdateStructureDB.dll. Для проведения операции обновления версии ПО следует нажать кнопку (10) - . В результате откроется окно, вида:



После активизации файла обновления (с помощью кнопки) система проанализирует, нужно ли обновление (путем сравнения текущей и требующейся версии), и, в зависимости от принятого решения, будет доступна или недоступна кнопка запуска операции обновления в окне:



или:

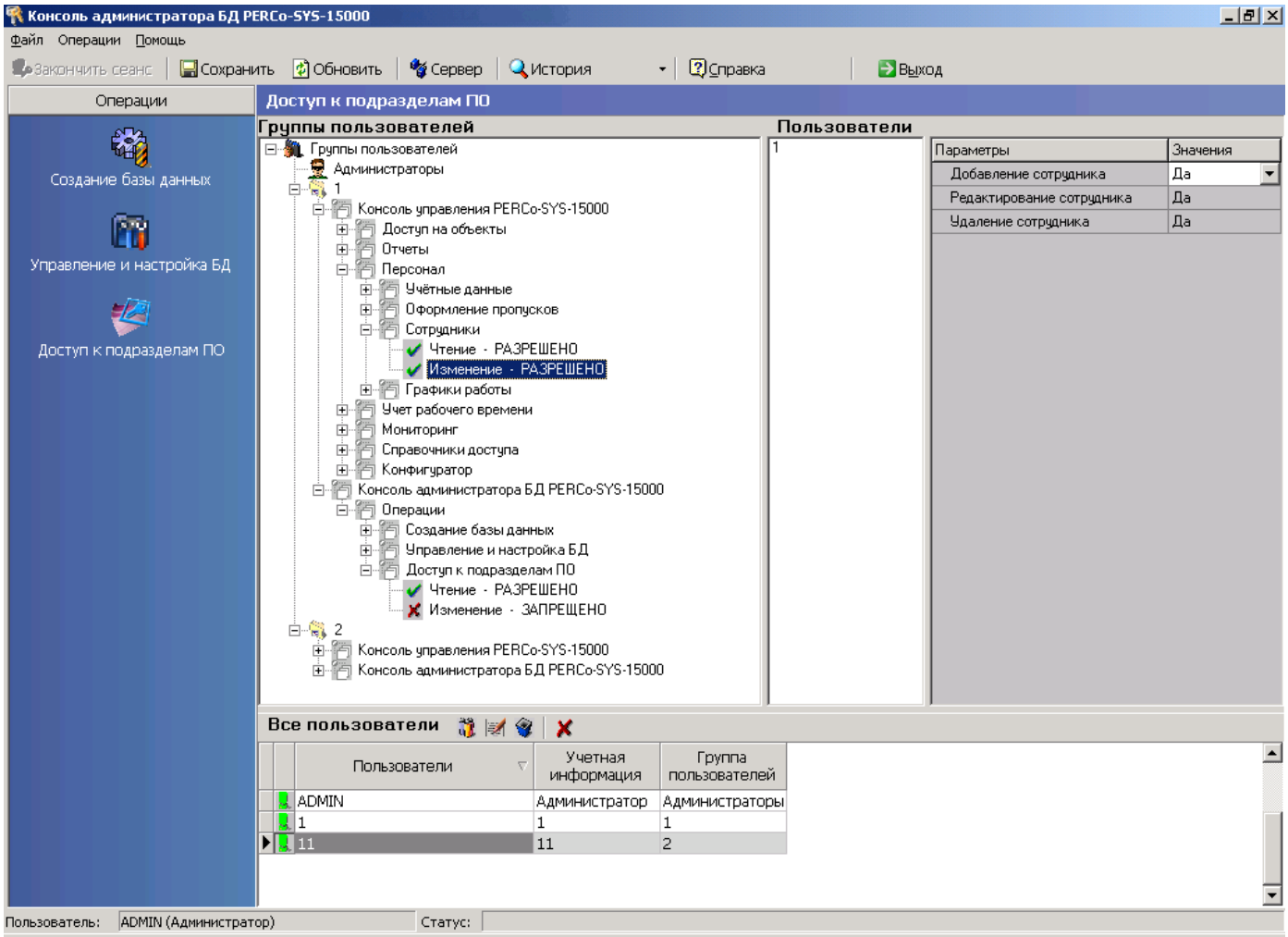


Особое внимание следует обратить на примечание в нижней части окна.

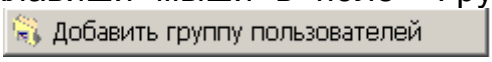
6. Задание прав доступа пользователей к подразделам программного обеспечения системы

6.1. Формирование групп доступа к подразделам программного обеспечения

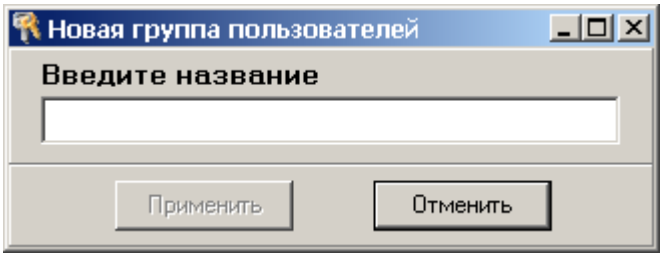
Данная операция осуществляется в окне «Доступ к подразделам ПО» программы «Консоль Администратора БД»:



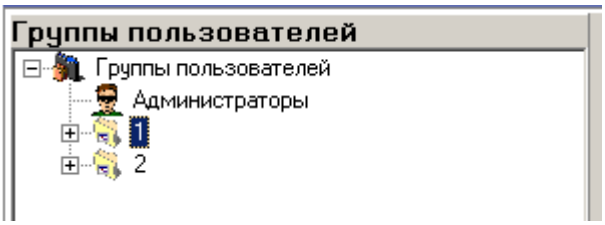
Перед заданием прав конкретным пользователям необходимо сформировать группы доступа. Это осуществляется из контекстного меню вызовом команды «Добавить группу доступа» (нажатием правой клавиши мыши в поле «Группы пользователей» в окне «Доступ к разделам ПО»):



Появляется окно:

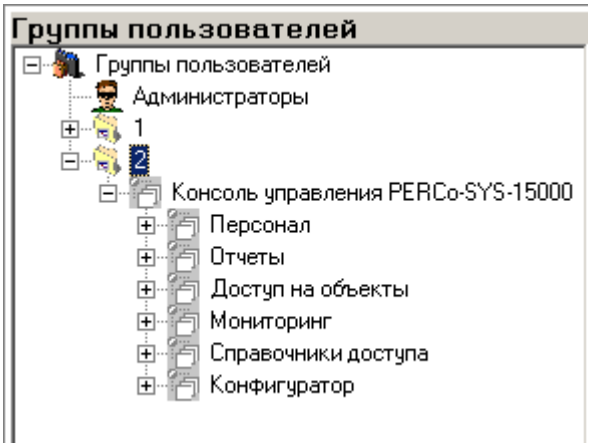


Введите название группы (например «2») и нажмите кнопку «Применить». Новая группа появится в окне «Группы доступа»:



После этого, вызовом из этого же контекстного меню команды «Добавить приложение», группе доступа «2», выделенной мышью, ставятся в соответствие необходимые разделы программы (для регистрации разделов программы необходимо первоначально произвести их запуск — см. п.6.3):

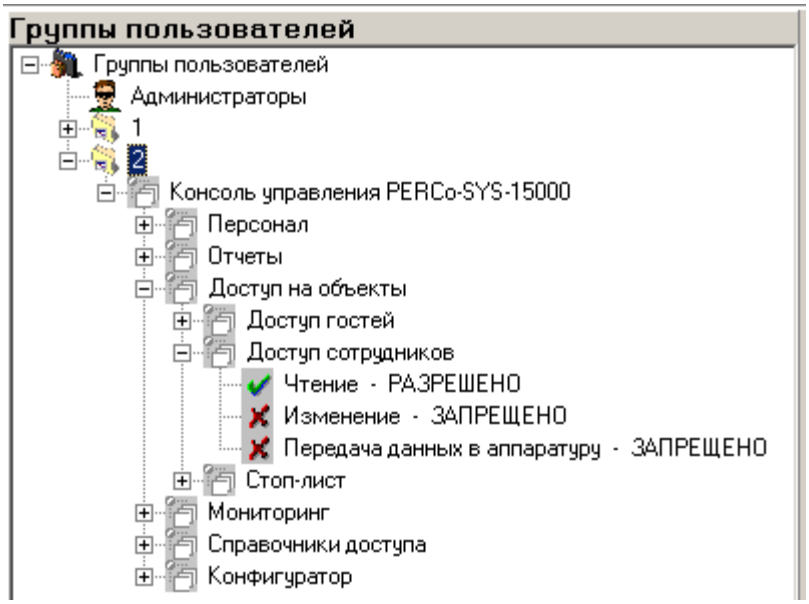
После выбора, например, консоли управления, все ее подразделы добавляются в окно «Группы доступа» в виде дерева под строкой «2» (см. п.6.4):



Каждому из подразделов ПО соответствуют следующие режимы доступа:

- «Чтение»
- «Изменение»
- «Передача данных в аппаратуру» (для некоторых подразделов)

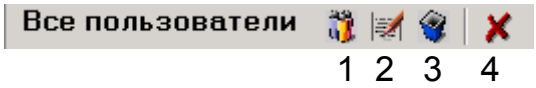
Каждому режиму соответствует две возможности – «Разрешить» и «Запретить», которые также вызываются из контекстного меню:



В этом окне конкретным группам задаются права доступа к подразделам ПО. Для этого следует выделить необходимую команду в дереве подразделов.

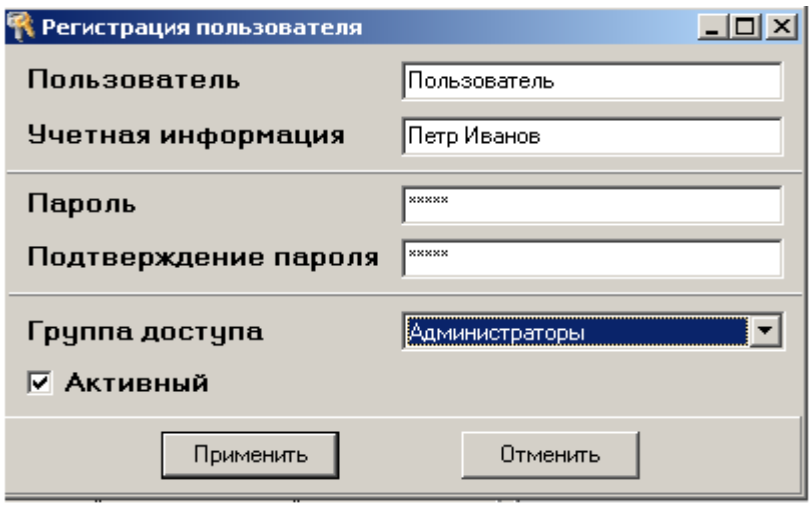
6.2. Ввод, редактирование и удаление данных о пользователях

Панель быстрых кнопок в окне, содержащем информацию о пользователях, имеет следующее назначение:



1 — «Добавить нового пользователя»
2 — «Изменить характеристики»
3 — «Удалить»
4 — «Запретить»

Для добавления нового пользователя следует в поле «Все пользователи» окна «Доступ к подразделам ПО» нажать на кнопку (1) - . Появится диалоговое окно «Регистрация пользователя»:



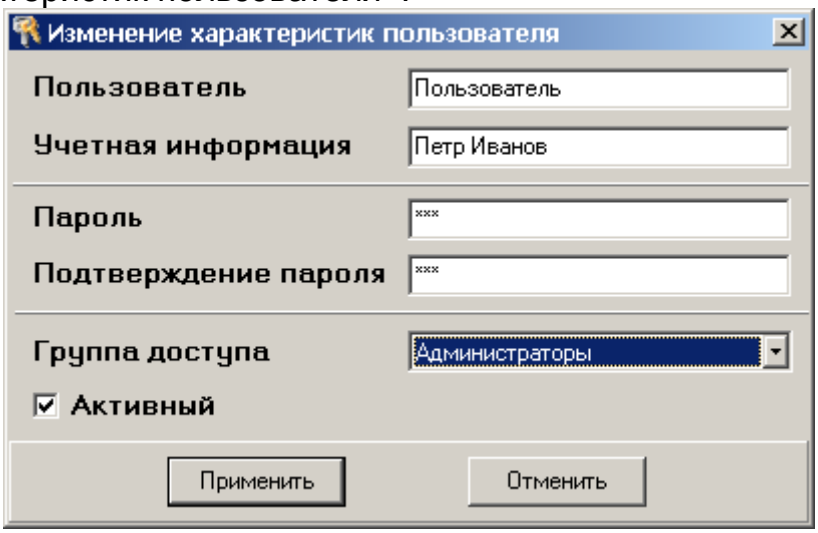
В появившемся диалоговом окне делаются следующие записи:

- «Пользователь» — имя, под которым пользователь входит в систему
- «Учетная информация» — дополнительная информация о сотруднике (ФИО)
- «Пароль» — уникальный пароль для данного пользователя
- «Подтверждение пароля» — повторение пароля пользователя
- «Группа доступа» — группа доступа, в которую входит данный пользователь. Здесь в разворачивающемся списке представлены те группы доступа, которые были заданы ранее в поле «Группы доступа»

Внизу окна находится опция «Активный», разрешающая (с отметкой) или запрещающая (без отметки) учетную запись пользователя.

После внесения всех записей следует нажать клавишу «Применить». Имя пользователя, при выделении соответствующей ему группы доступа, будет представлено в правом поле «Пользователи» окна «Доступ к разделам ПО».

Для изменения пароля доступа необходимо в поле «Все пользователи» окна «Доступ к подразделам ПО» нажать кнопку (2) - . Появится диалоговое окно «Изменение характеристик пользователя»:



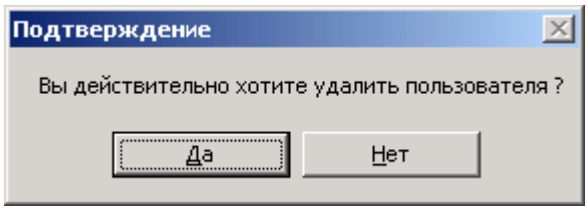
В появившемся диалоговом окне делаются следующие записи:

- «Пользователь» — имя, под которым пользователь входит в систему
- «Учетная информация» — дополнительная информация о сотруднике (ФИО)
- «Пароль» — новый пароль для данного пользователя
- «Подтверждение пароля» — повторение нового пароля пользователя
- «Группа доступа» — группа доступа, в которую входит данный пользователь.

Внизу окна находится опция «Активный», разрешающая (с отметкой) или запрещающая (без отметки) учетную запись пользователя.

После внесения изменений следует нажать кнопку «Применить». В окне появятся измененные данные.

Для удаления данных о пользователе необходимо выделить строку с его данными в поле «Все пользователи» окна «Доступ к разделам ПО» и нажать кнопку (3) — . Появится диалоговое окно с просьбой подтвердить удаление:



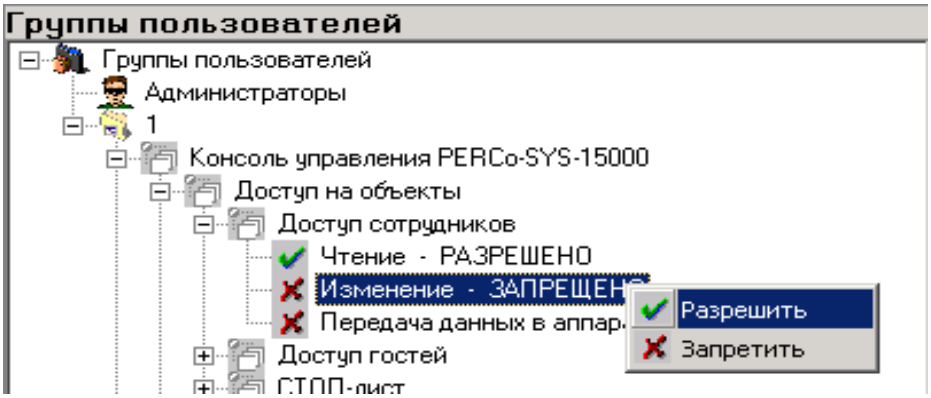
После подтверждения строка с данными о пользователе будет удалена.

Можно временно запретить пользователю доступ к ПО, а затем снова разрешить, не вводя всю информацию заново. Для этого нужно выделить строку с его данными в поле «Все пользователи» окна «Доступ к подразделам ПО» и нажать кнопку «Запретить» (4) — . Для разрешения доступа следует вновь нажать кнопку «Запретить», отменив данную команду.

6.3. Задание прав доступа к разделам программного обеспечения

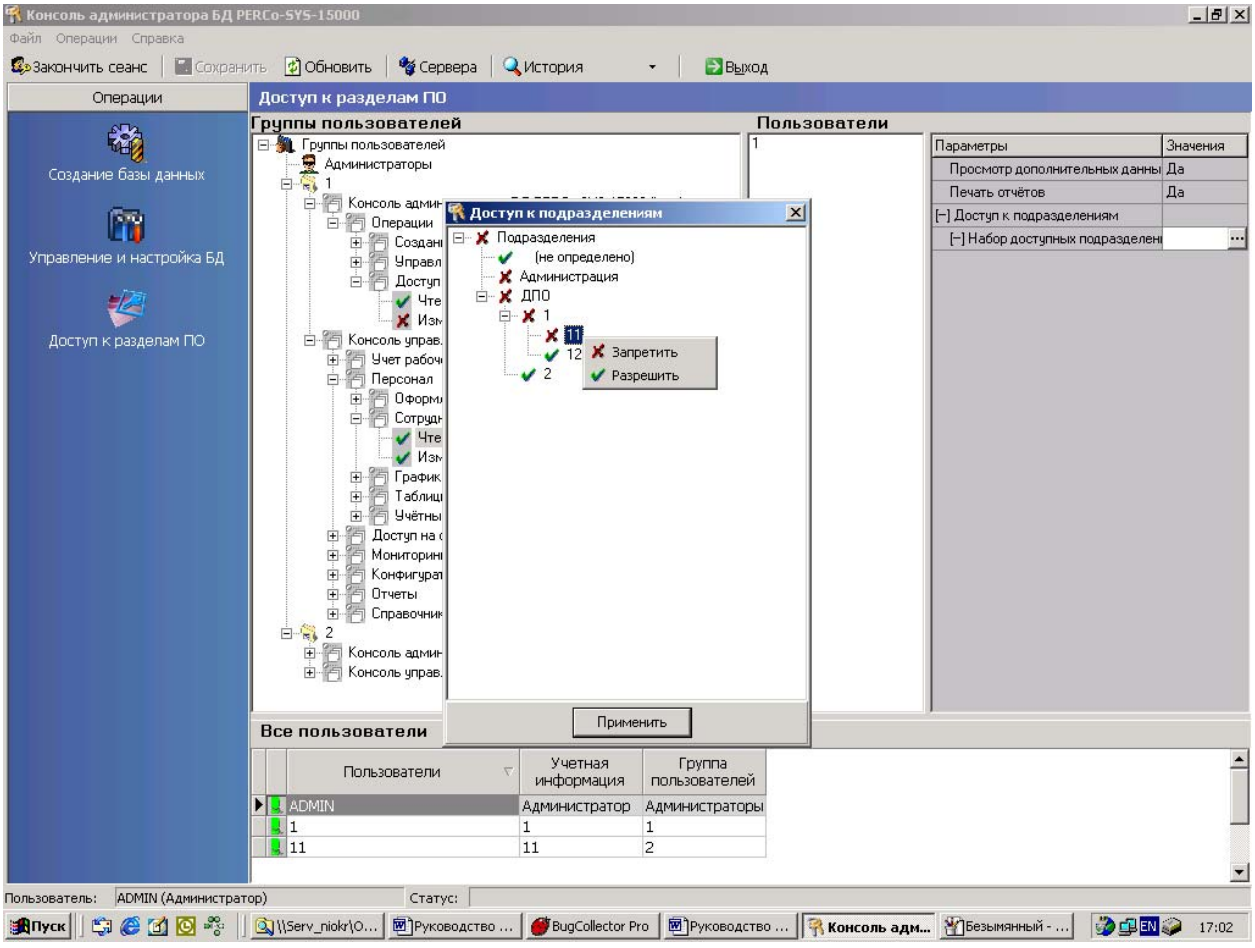
Каждое приложение, раз запустившись, регистрирует себя в БД (первый запуск приложений «Консоль администратора БД» и «Консоль управления БД» производит Администратор системы, уже создав базу и введя имя Admin и пароль, который задал для себя). После этого необходимо запустить «Консоль Администратора БД» и создать группы, если они еще не созданы, создать пользователей и поместить их в группы. Затем в каждую группу добавить приложения, которые должны обслуживаться пользователями данной группы, и задать права как на работу с самим приложением, так и на функции, которые данное приложение осуществляет.

Создание групп, добавление приложений в группы и задание прав производится из контекстного меню (щелчок правой кнопкой мыши).



6.4. Задание прав доступа к подразделениям

Все пользователи, не входящие в группу «Администраторы», изначально не имеют доступа к подразделениям (кроме как к подразделению «не определено»). Все новые подразделения недоступны, пока на них не даны права.



Воспользовавшись контекстным меню, вы можете разрешить или запретить доступ к любому подразделению, за исключением «Подразделения» и «не определено». После этого пользователь получит доступ к выбору разрешенных подразделений.

7. НАСТРОЙКА СЕРВЕРА СИСТЕМЫ

Для того чтобы пользователь мог получать информацию от оборудования системы, необходимо настроить связь между компьютером пользователя и аппаратурой системы. Для этого существует модуль «Сервер системы», входящий в состав базового ПО.

Модуль устанавливает расположение в сети Сервера управления данными и позволяет задать список серверов аппаратуры — узлов аутентификации системы. Полученные данные от сконфигурированных узлов передаются Серверу управления данными. При успешном запуске Сервера управления данными или добавлении сервера аппаратуры, «Сервер системы» устанавливает с ними связь посредством технологии Microsoft DCOM, использующейся для взаимодействия в локальной сети Microsoft всех программ, входящих в состав системы «PERCo-SYSTEM-15000».

Основной задачей Сервера системы является взаимодействие с серверами аппаратуры. Данное взаимодействие можно разделить на две группы: прямое и косвенное.

Прямое (непосредственное) взаимодействие включает в себя:

- Установку расположения в сети на персональном компьютере сервера аппаратуры (при этом тип поддерживаемой им аппаратуры может быть 600 или 12000 серии) или одновременно двух серверов, каждый из которых поддерживает аппаратуру определённого типа (в этом случае требуется наличие на выбранном компьютере двух рабочих COM-портов)
- Изменение настроек сервера аппаратуры (номера COM-порта, признака подключения, пользовательского описания)

Прямое взаимодействие выполняется через пользовательский интерфейс данного модуля.

Косвенное взаимодействие включает в себя:

- Мониторинг сконфигурированных серверов аппаратуры — сбор данных от различных ветвей системы в один информационный поток с последующей передачей его Серверу управления данными;
- Получение команды от клиентского приложения и передача серверам аппаратуры с последующим контролем её состояния;
- Постоянный контроль наличия связи с подключенными серверами аппаратуры

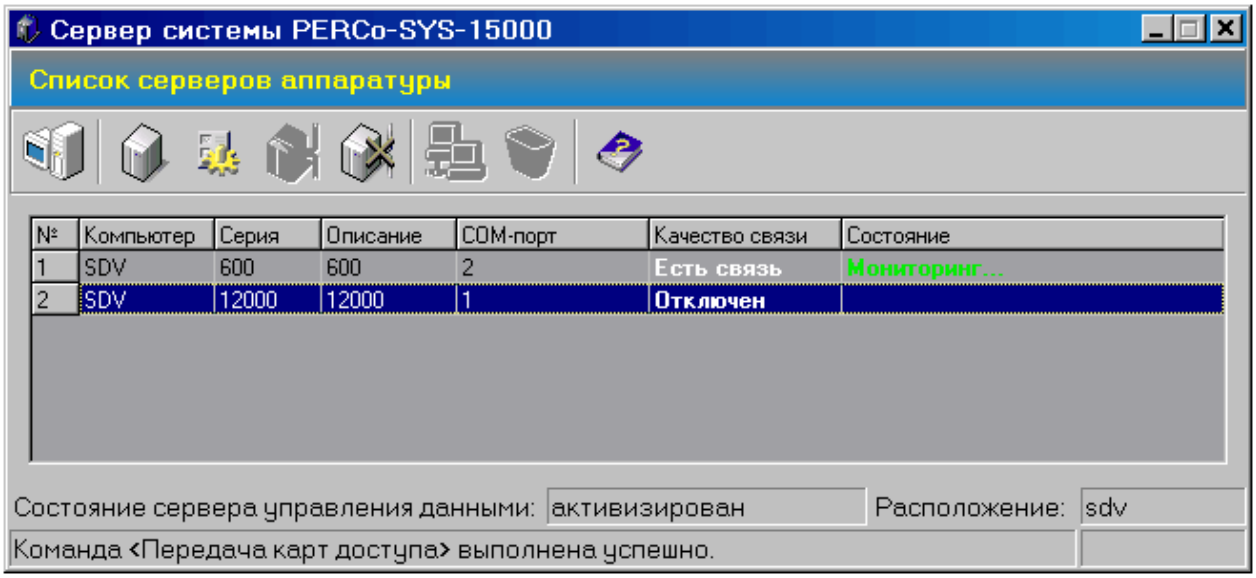
Косвенное взаимодействие Сервера системы с серверами аппаратуры осуществляется автоматически.

Главное окно приложения «Сервер системы» содержит панель с кнопками, список для отображения серверов аппаратуры, устанавливаемых в системе, и две информационных строки.

В строках отображается вспомогательная информация. В верхней — состояние и расположение «Сервера управления данными» баз данных, в нижней — служебная информация о системе в целом. Текст сообщения зависит от конкретных действий пользователя или работы Сервера системы.

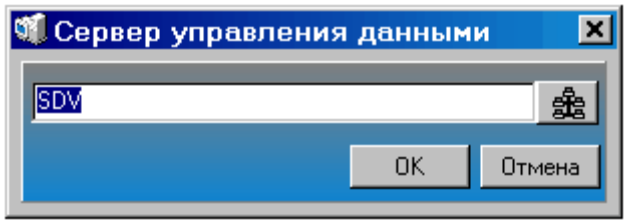
7.1. Задание компьютера, на котором установлен сервер управления данными

Главное окно модуля содержит панель с кнопками, список для отображения серверов аппаратуры, устанавливаемых в системе, и две информационные строки.

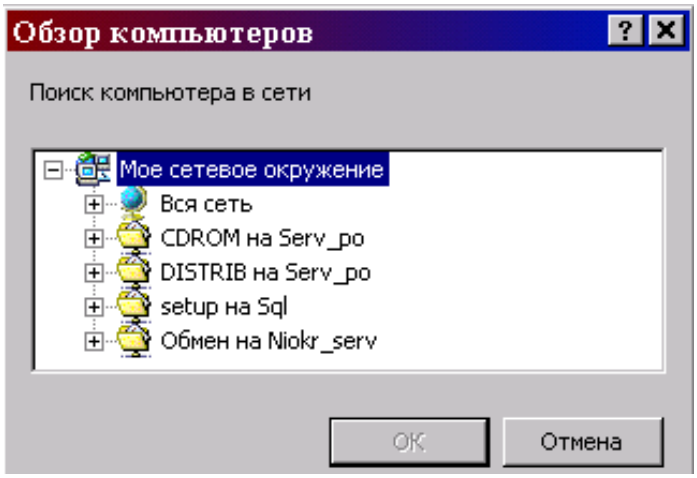


1 — «Выбрать расположение Сервера управления данными»
2 — «Добавить Сервер аппаратуры»
3 — «Настроить Сервер аппаратуры»
4 — «Включить Сервер аппаратуры»
5 — «Отключить Сервер аппаратуры»
6 — «Изменить местоположение Сервера аппаратуры»
7 — «Удалить Сервер аппаратуры»
8 — «Справка»

Кнопка (1) «Выбрать расположение Сервера управления данными» на панели окна приложения вызывает диалоговое окно для подключения к Серверу управления данными:



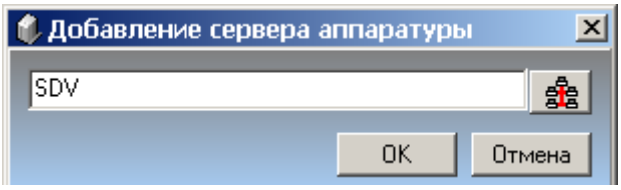
Это диалоговое окно позволяет задать имя компьютера, на котором установлен «Сервер управления данными». Это происходит, либо набором вручную при помощи клавиатуры прямо в поле редактирования, либо поиском нужного имени в сети при нажатии на кнопку :



Эта операция будет возможна только тогда, когда Сервер системы запущен вручную и нет ни одной загруженной Консоли управления.

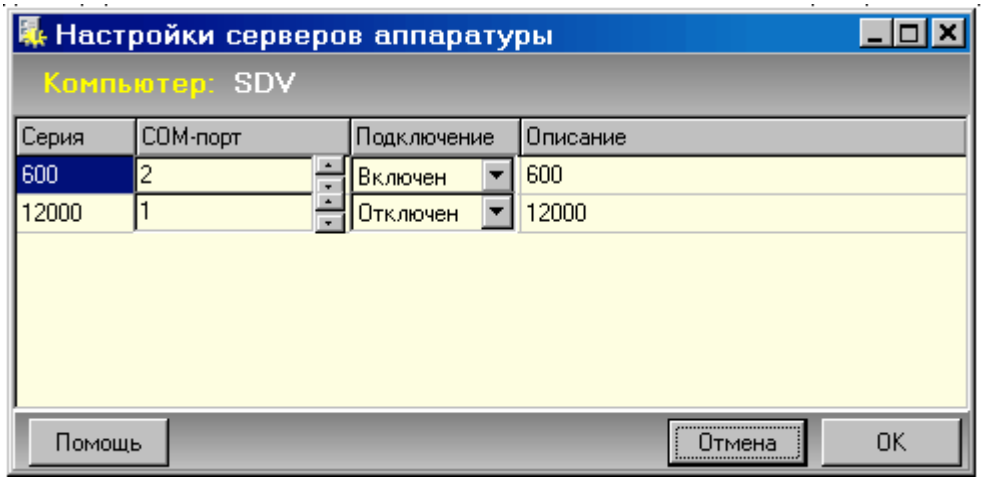
7.2.Задание компьютеров, на которых установлены серверы аппаратуры

Кнопка (2) — «Добавить Сервер аппаратуры» - на панели окна вызывает диалоговое окно для добавления Сервера аппаратуры:



Это диалоговое окно позволяет задать имя компьютера, на котором установлен сервер аппаратуры. Имя задается так же, как и в предыдущем случае. Так как система «PERCo-SYSTEM-15000» способна работать с аппаратурой 600 и 12000 серии, то после нажатия кнопки «OK» будет произведен поиск серверов аппаратуры обоих типов.

Найденные серверы аппаратуры будут представлены в следующей форме:

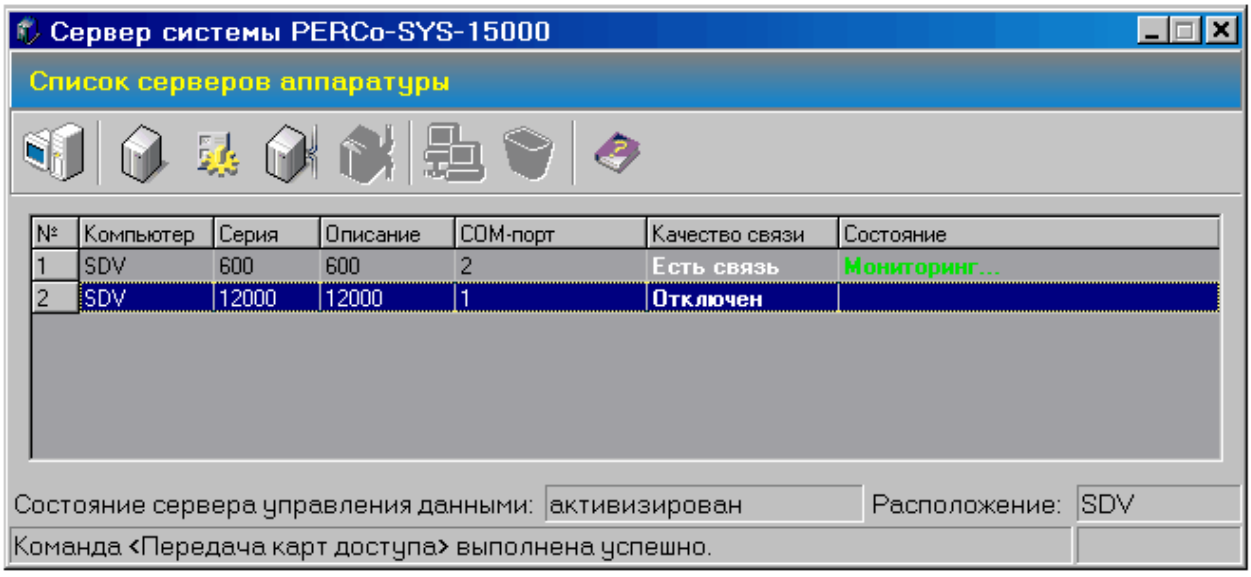


В данном окне необходимо указать, какой именно сервер аппаратуры вы хотите выбрать, задав значение в графе «Подключение» и указав номер COM-порта, к которому подключено оборудование. Кроме этого, вы можете ввести описание канала, который будет в дальнейшем использоваться.

Доступ к окну настройки серверов аппаратуры возможен также при нажатии на кнопку (3) — «Настроить сервер аппаратуры».

7.3. Включение и отключение серверов аппаратуры

На панели главного окна находятся кнопки (4) — «Включить Сервер аппаратуры» и (5) — «Отключить Сервер аппаратуры», которые доступны в зависимости от состояния сервера аппаратуры, выделенного в этот момент в списке.



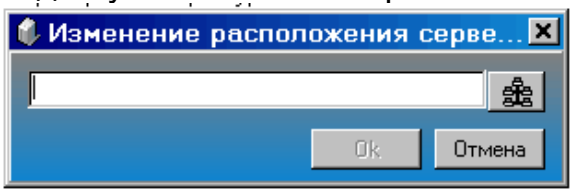
Как видно из приведенного выше рисунка, кнопка (4) — «Включить Сервер аппаратуры» — доступна, так как выбранный в списке сервер аппаратуры «SDV, 12000» в данный момент отключен.

При выборе сервера аппаратуры «SDV, 600», который в данный момент включен, кнопка (5) - «Отключить Сервер аппаратуры» - активизируется.

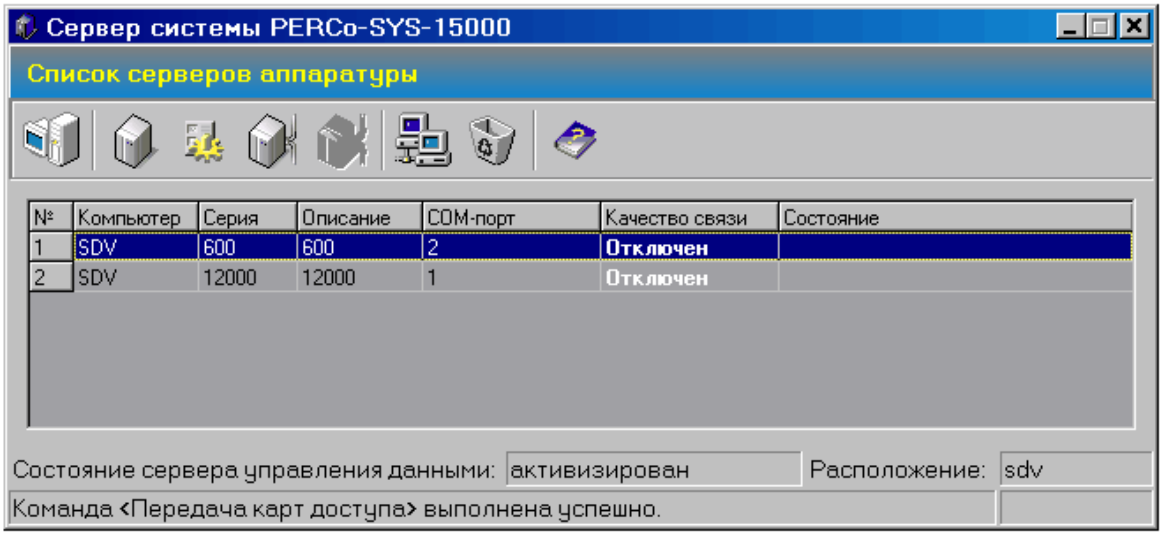
Отключение сервера аппаратуры приводит к тому, что он перестает получать данные о состоянии оборудования и передавать данные контроллерам, которые подключены к данному компьютеру. Отключать сервер аппаратуры следует только при проведении ремонтных работ.

7.4. Изменение места расположения аппаратуры

Кнопка (6) — «Изменить местоположение сервера аппаратуры» — на панели вызывает диалоговое окно для указания нового расположения сервера аппаратуры.



Эта кнопка доступна только тогда, когда Сервер системы запущен вручную, все серверы аппаратуры отключены, и нет ни одной загруженной Консоли управления.



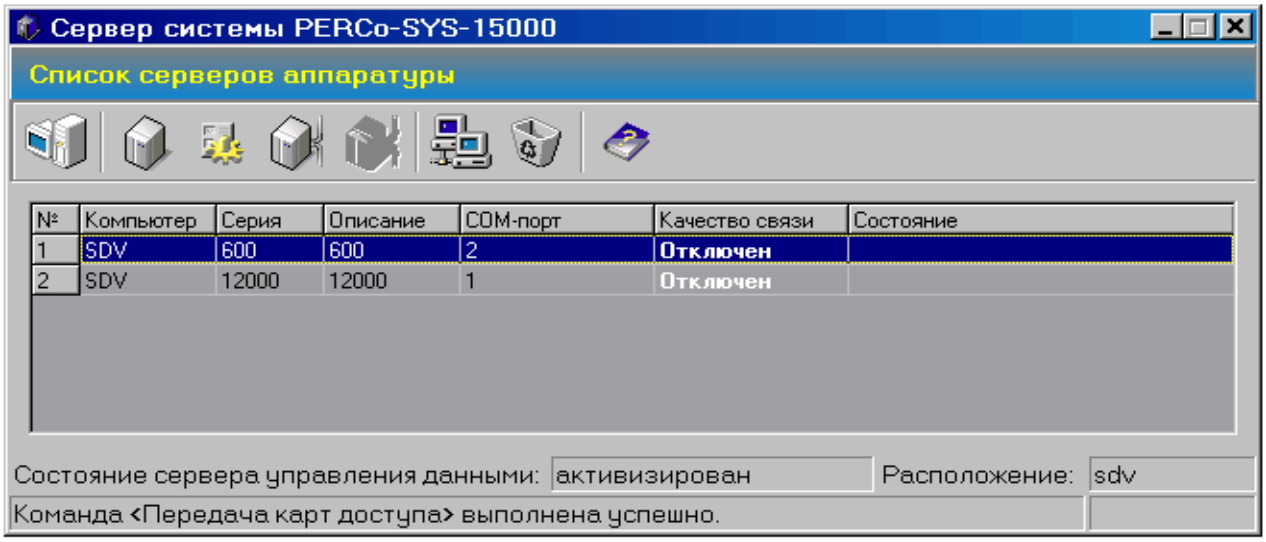
Изменение местоположения сервера аппаратуры может понадобиться, если вышел из строя компьютер, на котором изначально была проведена конфигурация сервера аппаратуры. В этом случае аппаратуру переключают на другой компьютер и указывают новое расположение сервера аппаратуры.

7.5. Удаление сервера аппаратуры

Кнопка (7) - «Удалить Сервер аппаратуры» - удаляет сервер аппаратуры из списка серверов. После этого вся информация о конфигурации данного сервера будет потеряна.

Эта кнопка доступна только тогда, когда Сервер системы запущен вручную, все серверы аппаратуры отключены и нет ни одной загруженной Консоли управления.

Вызов справки осуществляется нажатием на кнопку «Справка».



8. КОНФИГУРИРОВАНИЕ СИСТЕМЫ

Для нормального функционирования системы необходимо определить ее аппаратный состав и произвести соответствующие настройки аппаратуры.

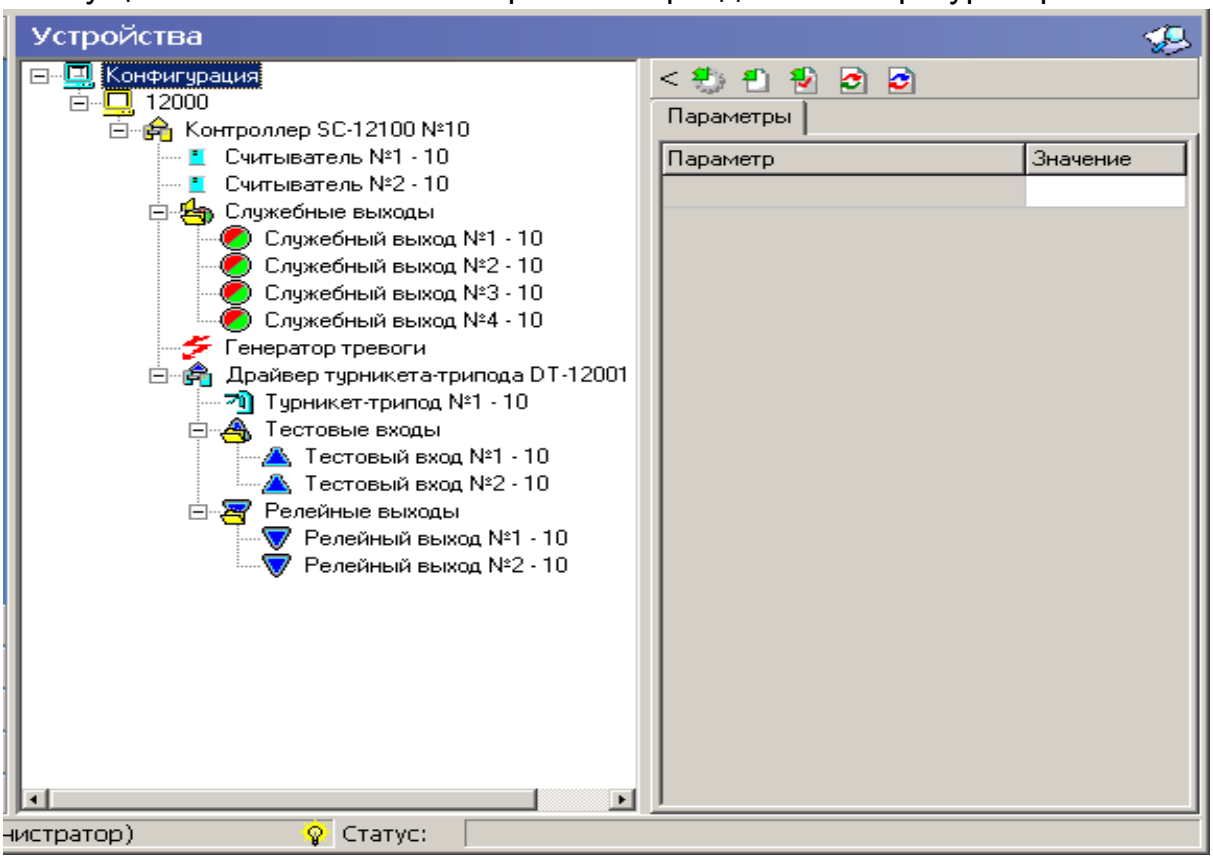
Автоконфигурация системы проводится в окне «Устройства» раздела «Конфигуратор» программы «Консоль управления». В этом же окне задаются параметры работы подключенных устройств.

Вызов подраздела осуществляется путем выбора соответствующих раздела и подраздела на левой панели рабочего окна или пункта основного меню программы «Консоль управления».

8.1. Автоматизированное определение аппаратного состава системы

Для автоматического определения аппаратного состава системы и передачи начальных параметров работы в устройства необходимо проведение автоконфигурации.

Она осуществляется в окне «Устройства» раздела «Конфигуратор»:



В левой части данного окна представлена древовидная структура сконфигурированных устройств, а в правой – инспектор устройств, состоящий из двух закладок: «Параметры» и «События». Здесь задаются параметры работы подключенных устройств, либо отражается список действий по определённым событиям, связанным с этими устройствами. Над закладками расположена строка с пятью кнопками:

1 2 3 4 5

1 — «Конфигурация системы»,

2 — «Передать все параметры»,

3 — «Передать измененные параметры»,

4 — «Восстановить параметры по умолчанию»,

5 — «Удалить действия всех событий.

Все кнопки видны только при выделении первого уровня в дереве устройств — строки «Конфигурация». При выделении узлов остаются только кнопки «Передать все параметры», «Передать измененные параметры».

(1) - — «Конфигурация системы» - при нажатии на данную кнопку осуществляется автоконфигурация системы. Программа сама опрашивает все устройства системы и составляет их список, который затем отражается в окне «Устройства». Время выполнения данных команд достаточно продолжительное.

После проведения автоконфигурации пользователь должен установить параметры функционирования оборудования, а затем передать все параметры в аппаратуру (кнопка (2) - — «Передать все параметры»). В дальнейшем, при нормальной работе системы, достаточно передавать только измененные параметры (кнопка (3) - — «Передать изменённые параметры» — становится активной только после внесения каких-либо изменений).

Можно проводить автоконфигурацию как всего оборудования, так и отдельных серверов аппаратуры. Для этого необходимо выделить соответствующий узел в древовидной структуре устройств и нажать кнопку «Конфигурация системы».

Процесс автоконфигурации необходимо проводить при каждом подключении к системе нового оборудования или замене старого.

При работе с закладкой «События» можно произвести восстановление параметров по умолчанию нажатием на кнопку (4) - — «Восстановить параметры по умолчанию», а также можно произвести очистку списка действий по всем событиям — при нажатии на кнопку (5) - - «Удалить действия всех событий».

Если объект выделен серым цветом, то он отключен, т.е. не представлен физически в аппаратуре.

8.2. Задание параметров работы подключенных устройств

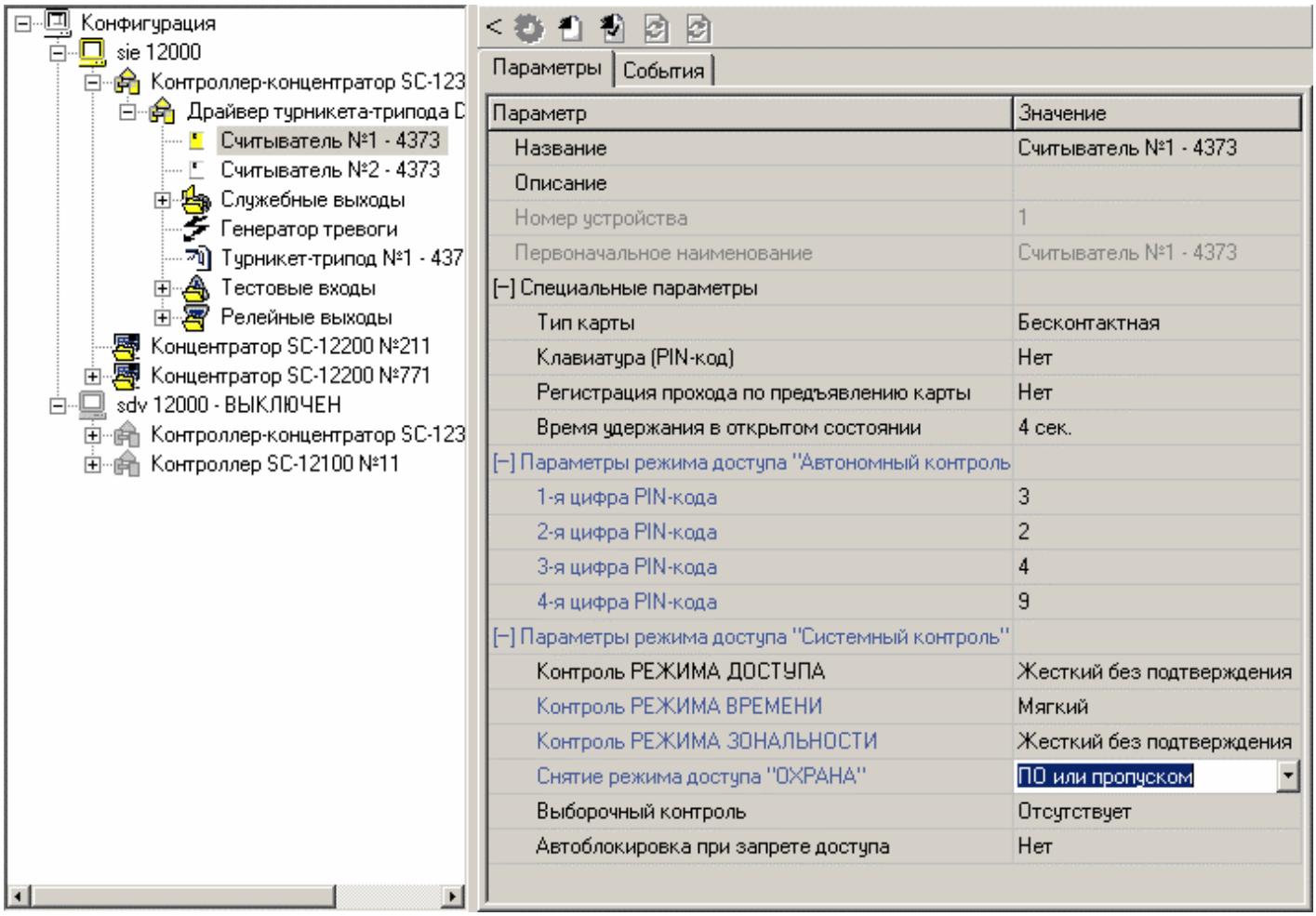
Параметры работы подключенных устройств задаются в окне «Устройства» раздела «Конфигуратор». Данное окно имеет следующий вид (см. след. стр.).

В левой части окна представлен список устройств системы, а в правой находится инспектор устройств, позволяющий задавать их параметры, изменять свойства и осуществлять другие подобные операции.

Выбор устройства из дерева системы осуществляется при помощи мыши или клавиш управления курсором. В правой части панели отображаются, либо параметры устройства (закладка «Параметры»), либо события, связанные с этим устройством (закладка «События»).

Параметр	Значение
Название	Турникет №1
Номер устройства	1
Описание	
Первоначальное наименование	Турникет №1
Входной считыватель	Вход проходной
Выходной считыватель	Выход проходной
Время удержания в открытом состоянии	00 мин. 04 сек.
Предельное время разблокировки	00 мин. 08 сек.
Время предтревоги	4
Режим управления	Статический
[—] Специальные параметры	
[—] Состояние "Закрыто"	
Запитан	Нет
[—] Нормальное (т.е заблокированное) сост	
Нормально замкнут	Да
Восстанавливать состояния "Закрыто"	После закрытия
[—] Релейные выходы, активизируемые при	
Релейный выход №1	Нет
Релейный выход №2	Нет

На первой закладке редактируются параметры выбранного устройства:



Это осуществляется путём выбора нужной ячейки со свойством объекта и вводом нового значения:

- Если параметр строковый – необходимо при помощи клавиатуры ввести новое значение

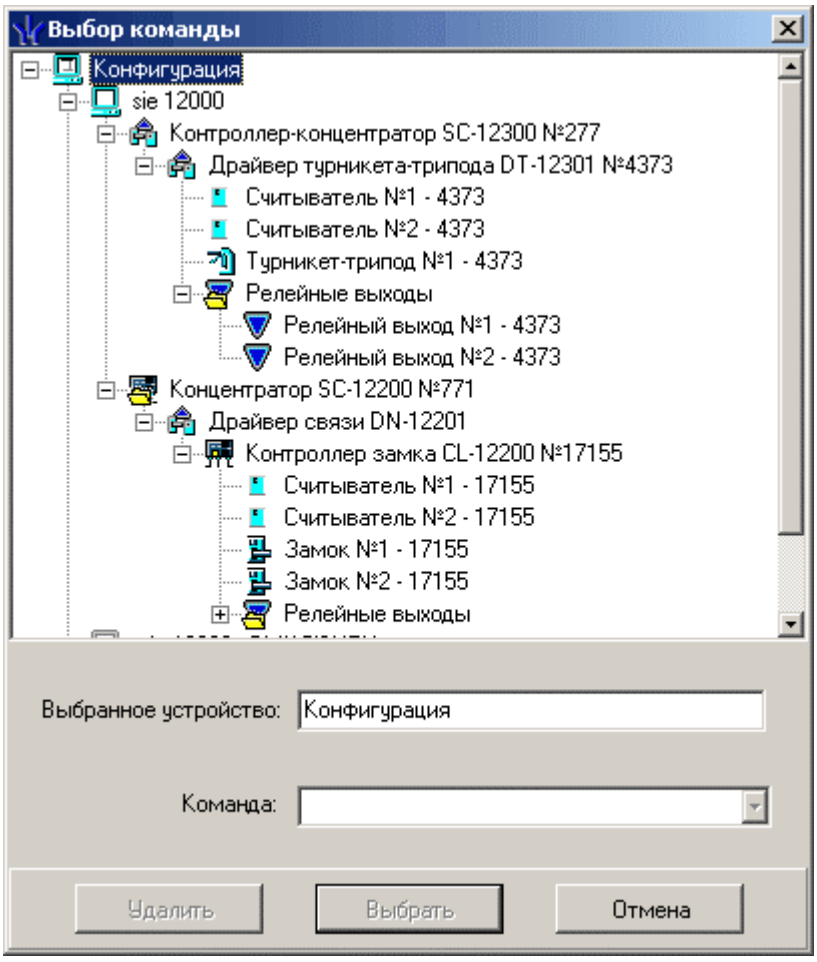
- Если возможен выбор из ограниченного числа вариантов – выбрать нужный вариант
- Если параметр числовой – ввести необходимое значение вручную, либо нажать на кнопку ... и ввести значение при помощи клавиатуры или мыши в появившемся окне для ввода

На закладке «События» представлен список событий для выбранного объекта:

Параметр	Значение
[+] Очистка журнала регистрации	
[—] Переполнение журнала регистрации	
Описание	
[—] Действия	
Действие №1	Отсутствует объект;Отсутствует команда
Действие №2	Отсутствует объект;Отсутствует команда
Действие №3	Отсутствует объект;Отсутствует команда
Действие №4	Отсутствует объект;Отсутствует команда
Действие №5	Отсутствует объект;Отсутствует команда
Действие №6	Отсутствует объект;Отсутствует команда
Действие №7	Отсутствует объект;Отсутствует команда
Действие №8	Отсутствует объект;Отсутствует команда
[+] Авария питания от электросети	

Для каждого из событий вы можете задать до 8 действий, выполняемых сервером системы при возникновении данного события на выбранном устройстве.

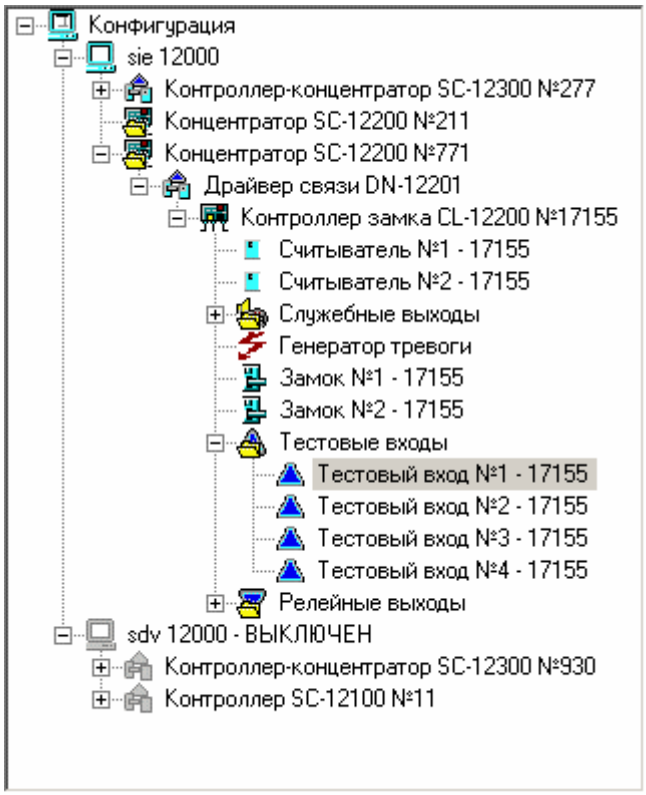
Реакции на события выбранного устройства редактируются путём выбора нужной ячейки и ввода нового значения. В качестве реакций на события происходит выполнение определённой команды указанного устройства. Для этого необходимо в правом поле окна в закладке «События» выбрать интересующие вас действия, а затем нажать на кнопку ... напротив них. Появится окно «Выбор команды»:



В этом окне надо выбрать требуемое устройство и команду (разрешено добавлять только устройства с заданными командами) и затем нажать на кнопку «Выбрать». Для удаления этого устройства с командой из выбранного события следует нажать на кнопку «Удалить».

Например, если требуется при срабатывании подключенного к одному из тестовых входов охранного датчика поднять тревогу в рамках контроллера SC-12300 №277, то необходимо выполнить следующие действия:

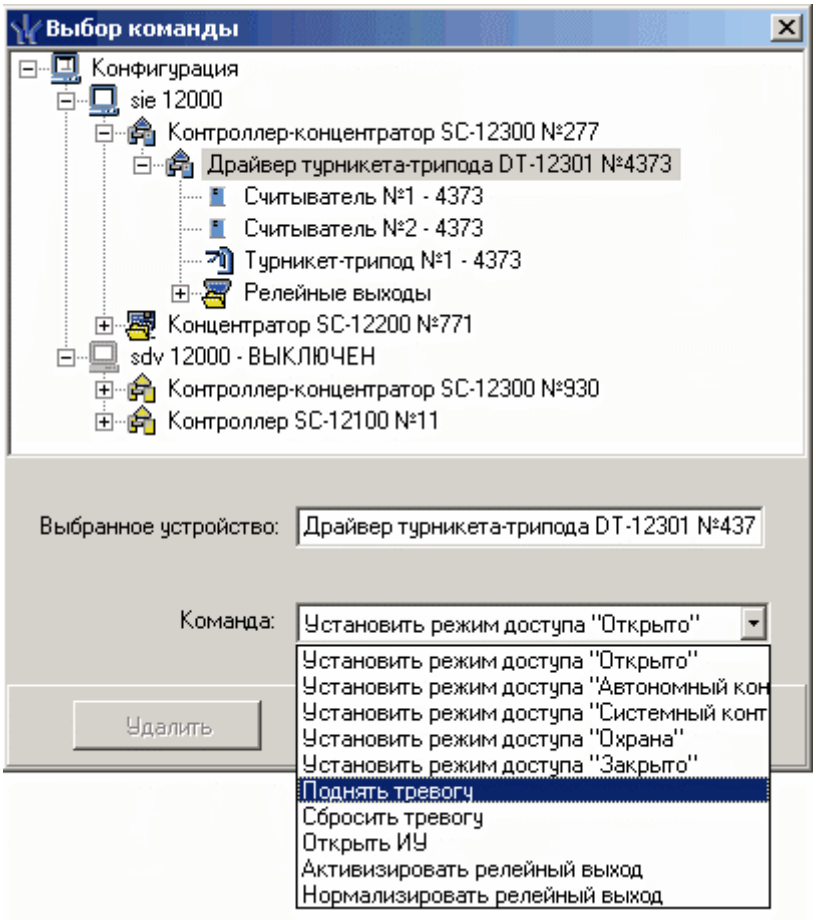
1) В дереве устройств выделить тестовый вход:



2) В правой части экрана на закладке «События» раскрыть строку «Активизация»: появится список из 8 действий:

[—] Активизация	
Описание	
[—] Действия	
Действие №1	Отсутствует объект;Отсутствует команда
Действие №2	Отсутствует объект;Отсутствует команда
Действие №3	Отсутствует объект;Отсутствует команда
Действие №4	Отсутствует объект;Отсутствует команда
Действие №5	Отсутствует объект;Отсутствует команда
Действие №6	Отсутствует объект;Отсутствует команда
Действие №7	Отсутствует объект;Отсутствует команда
Действие №8	Отсутствует объект;Отсутствует команда
[+] Сброс	
[+] Тревога по АКТИВИЗАЦИИ входа	
[+] Неизвестное событие	

3) Вызвав в одной из строк окно «Выбор объектов и команд», выбрать в дереве объектов драйвер 12300 (в случае установки действия в списке «Тревога по активизации входа» необходимо указать какой именно тестовый вход используется в параметрах генератора тревоги);
4) В нижней части данного окна в поле «Команда» задать для тестового входа в качестве ответной реакции команду «Поднять тревогу» устройства «Драйвер турникета-трипода 4373»;



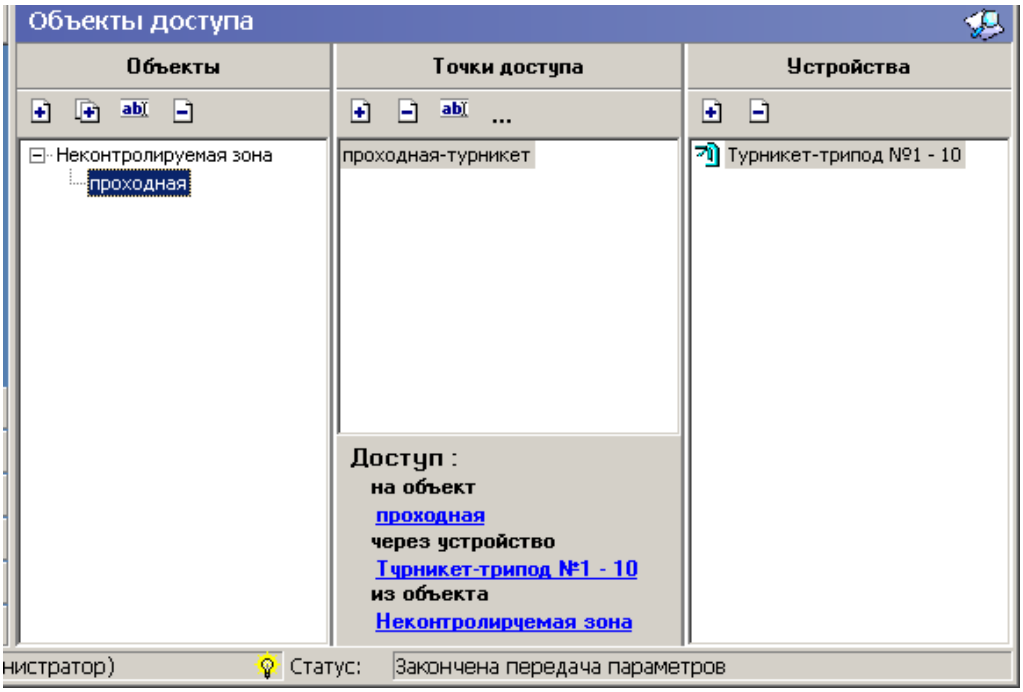
5) нажать кнопку «Выбрать» в нижней части окна.

Таким образом, вы сможете настроить систему, задав логику ее работы и алгоритм ее действий, которые будут выполняться автоматически, без участия оператора.

Более подробную информацию о значении параметров устройств, описание режимов контроля доступа смотри в разделе 4 «Технического описания СКУД PERCo-SYS-15000».

8.3. Формирование дерева объектов доступа

Данная функция осуществляется в окне «Объекты доступа» раздела «Конфигуратор»:



Окно разделено на три части: в первой представлено дерево помещений (объекты доступа), во второй — места расположения исполнительных механизмов (точки доступа), в третьей — общий список устройств, которые привязываются к выбранному помещению.

Для работы с объектами доступа служат следующие кнопки, расположенные в верхней части левого поля данного окна:

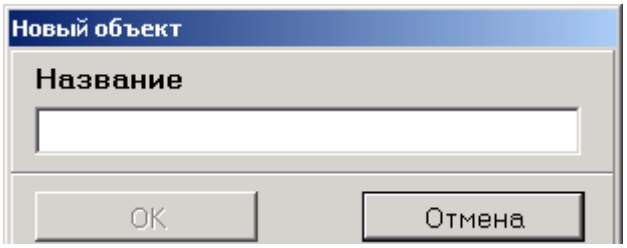
— «Добавить объект»

— «Добавить внутренний объект в выделенный объект»

— «Изменить название объекта»

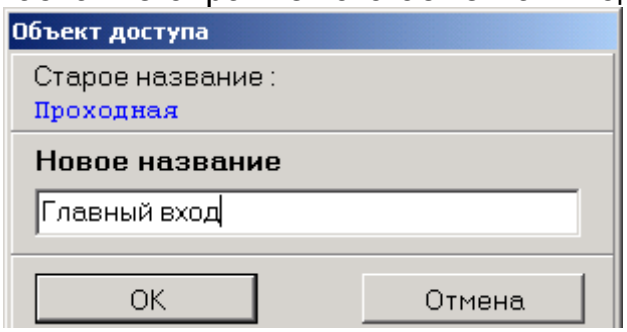
— «Удалить объект»

При создании нового объекта доступа появляется диалоговое окно, в которое нужно ввести наименование данного объекта и подтвердить изменение. После этого помещение появится в дереве объектов.



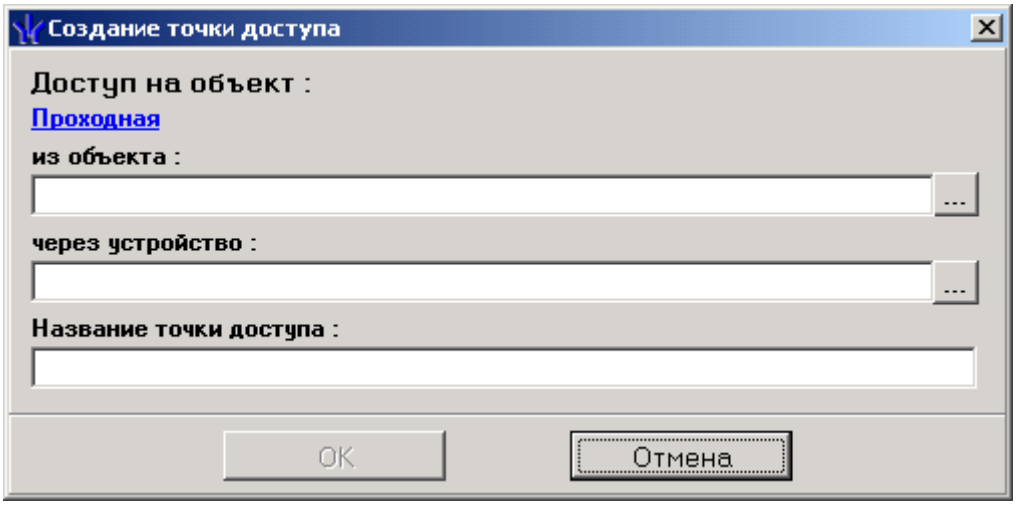
Аналогичные действия осуществляются и при добавлении внутреннего помещения в выделенное помещение.

При редактировании выбранного объекта на экран выводится окно, в которое следует ввести новое название охраняемого объекта и подтвердить изменение.

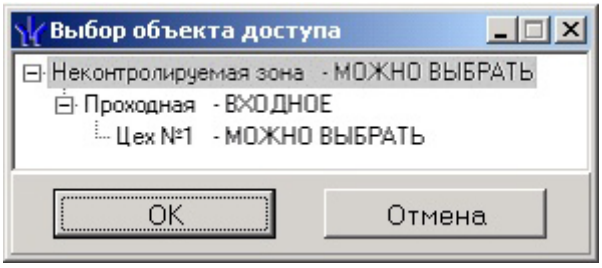


8.4. Формирование точек доступа

Для создания точки доступа следует нажать кнопку «Добавить точку доступа в объект» в поле «Точки доступа» рабочего окна программы. При этом появится диалоговое окно:

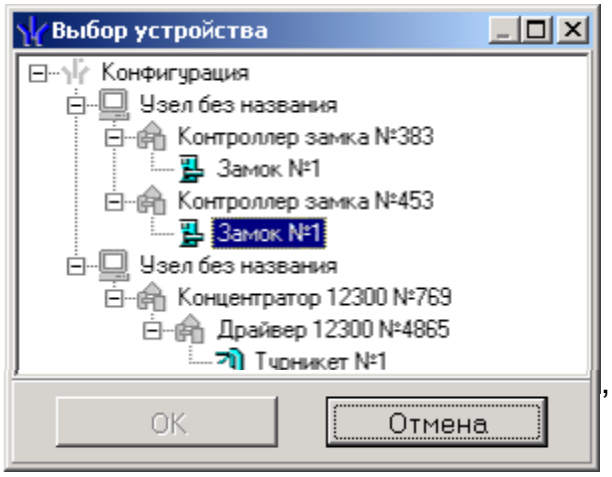


Нажмите кнопку ..., расположенную в строке «из объекта». На экран будет выведено окно, в котором следует выбрать из возможных то помещение, которое будет предшествовать охраняемому.



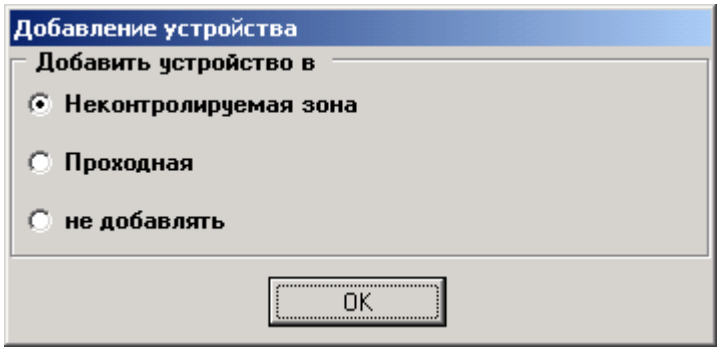
После выбора нажмите клавишу «ОК».

Далее следует нажать клавишу ... в строке «Через устройство». При этом на экран будет выведено окно, в котором следует выбрать те исполнительные устройства, которые привязываются к охраняемым объектам.

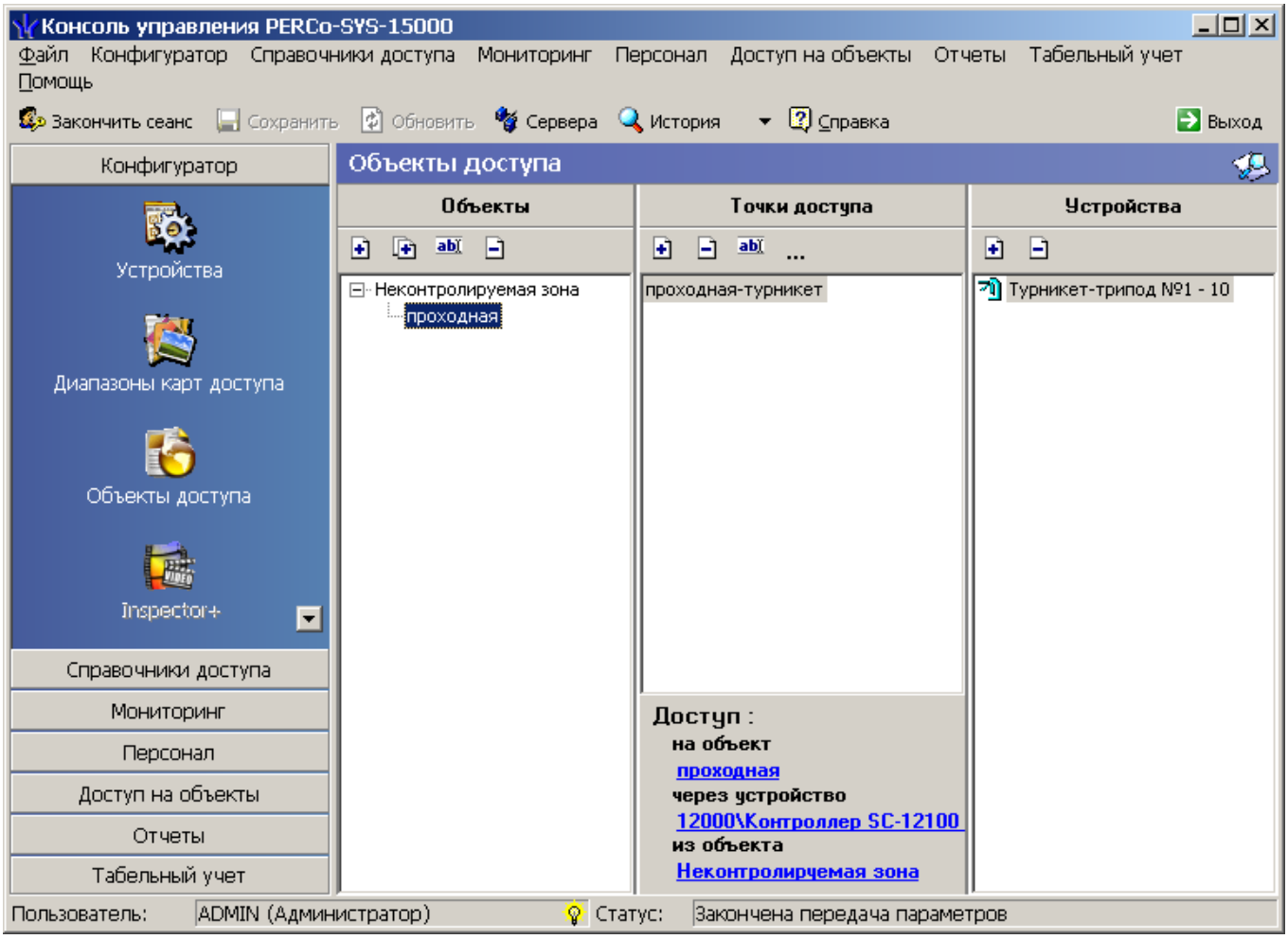


В третье поле введите название создаваемой точки доступа.

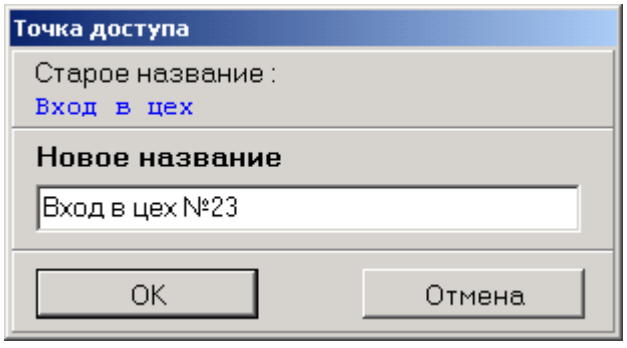
После внесения информации нажмите клавишу «ОК». Появится окно, в котором нужно указать, за каким объектом закрепляется устройство.



Новые данные отразятся в нижней части рабочего окна:



При нажатии на кнопку ab| появляется окно редактирования, в которое вводится новое название точки доступа.



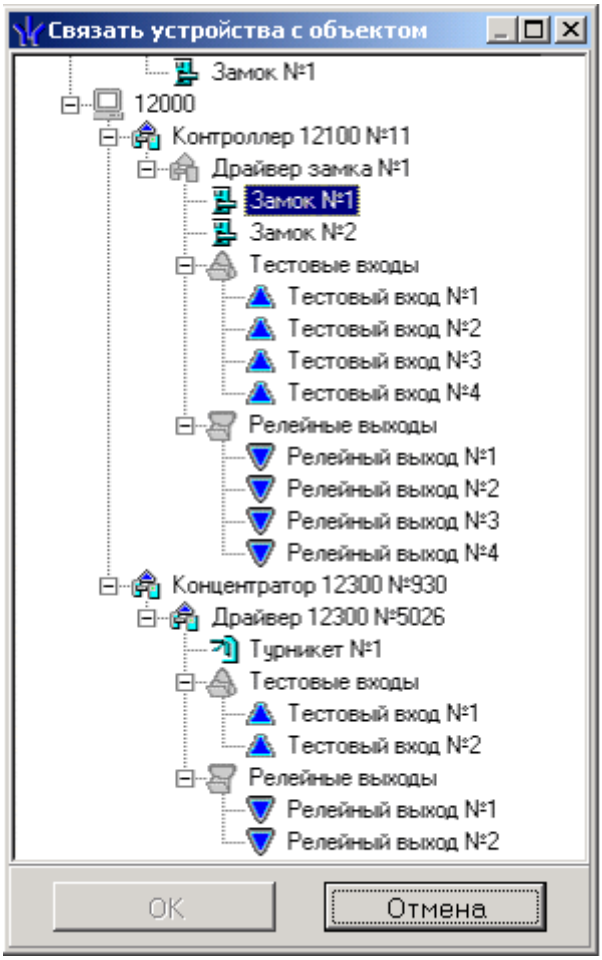
Для подтверждения изменений следует нажать клавишу «ОК».

Кнопка предназначена для удаления точки доступа.

Кнопка ... показывает название устройства и его путь в дереве конфигурации.

8.5. Установление связи между подключенным оборудованием и объектами доступа

Для привязки сконфигурированного оборудования к помещениям необходимо в поле «Устройства» нажать кнопку «Закрепить устройство за объектом» . На экран будет выведено окно с деревом устройств:



В данном окне нужно выбрать необходимое устройство и нажать кнопку «ОК». После этого устройство отразится в правом поле рабочего окна.

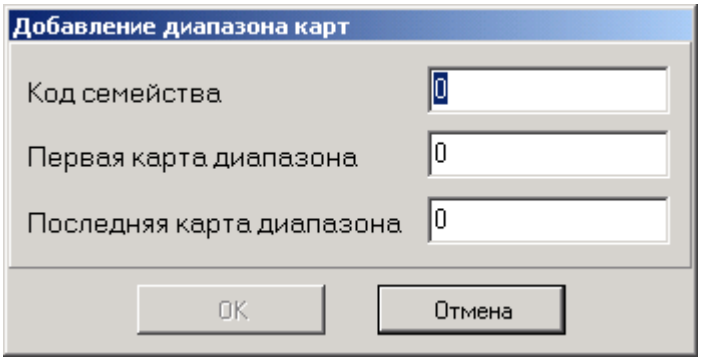
Для отсоединения устройства от объекта служит кнопка .

Таким образом, сконфигурированное оборудование ставится в соответствие с помещениями, являющимися объектами охраны.

8.6. Задание диапазонов карт доступа

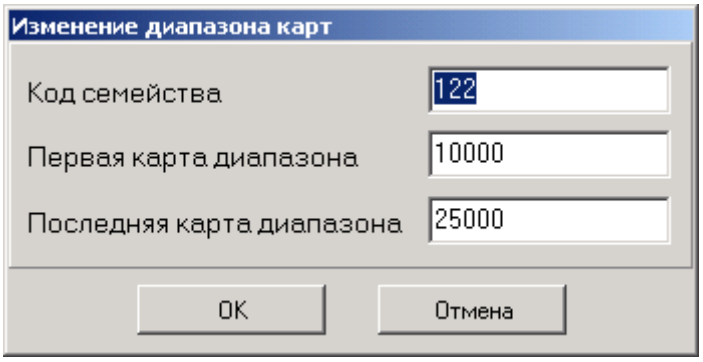
Данная операция осуществляется в окне «Диапазоны карт доступа» раздела «Конфигуратор» программы «Консоль управления»:

Для создания нового диапазона карт доступа надо нажать кнопку . Появится окно, в котором можно указать необходимые параметры:



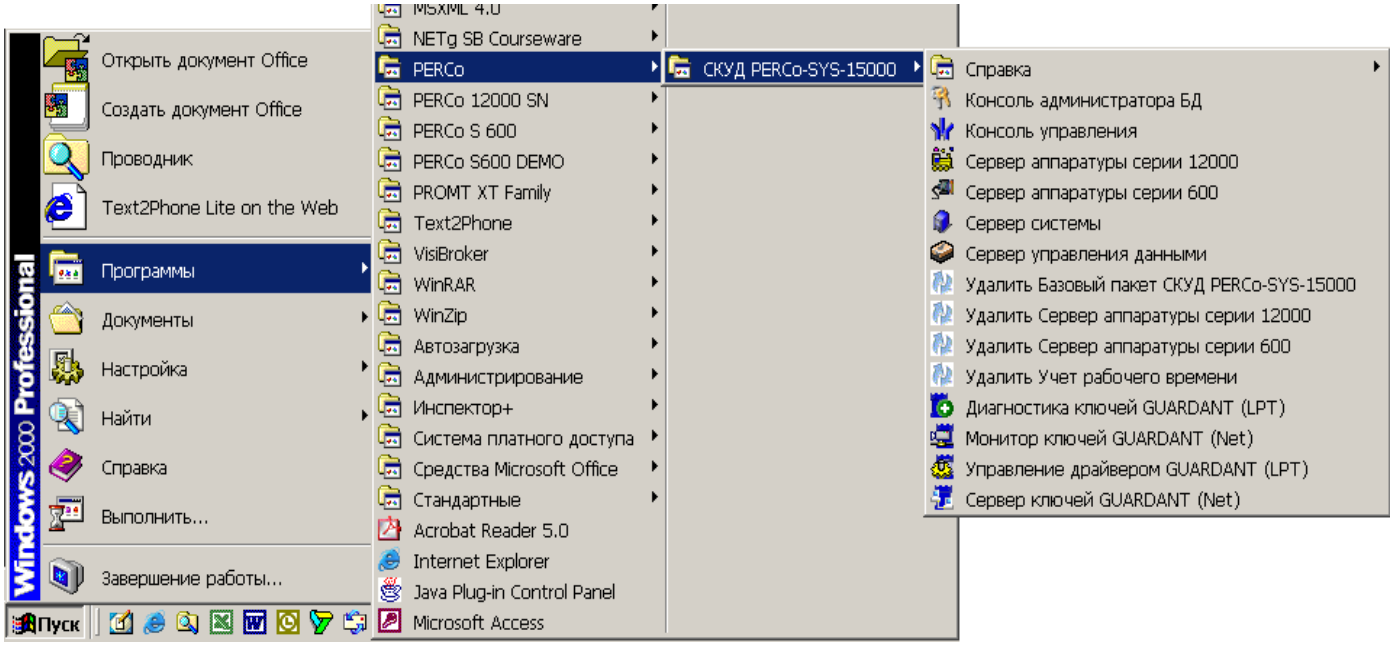
Для удаления диапазона карт доступа необходимо нажать кнопку .

Для редактирования следует нажать кнопку .



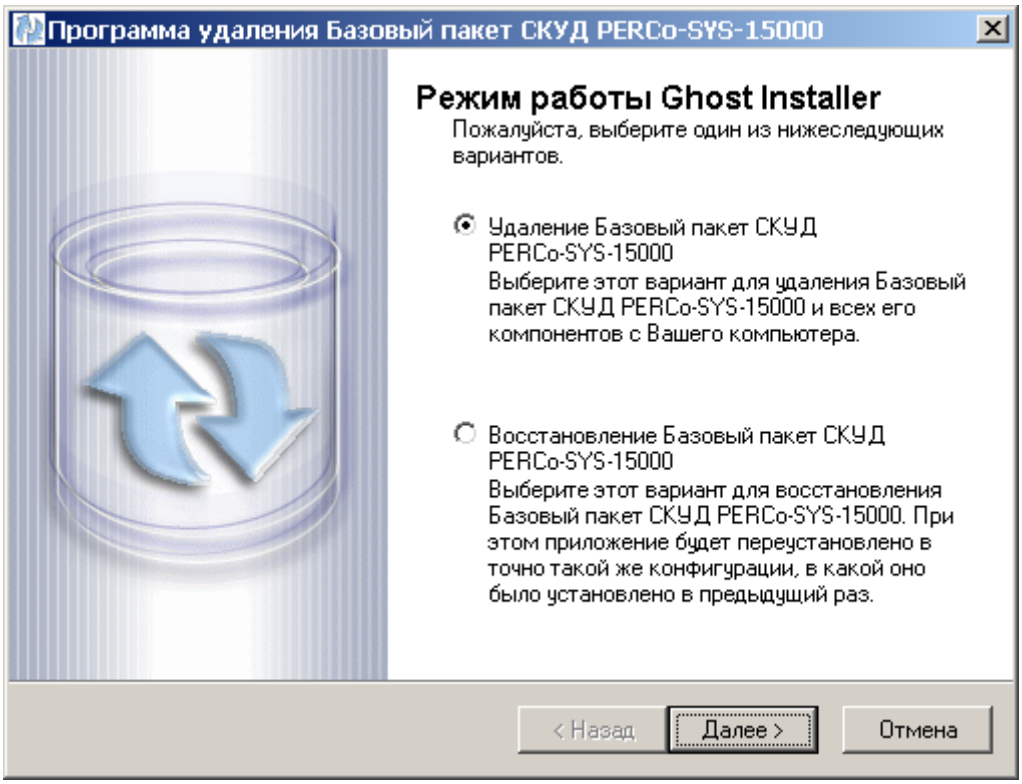
9. УДАЛЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Удалить систему можно в любой последовательности, выбрав необходимые пункты.

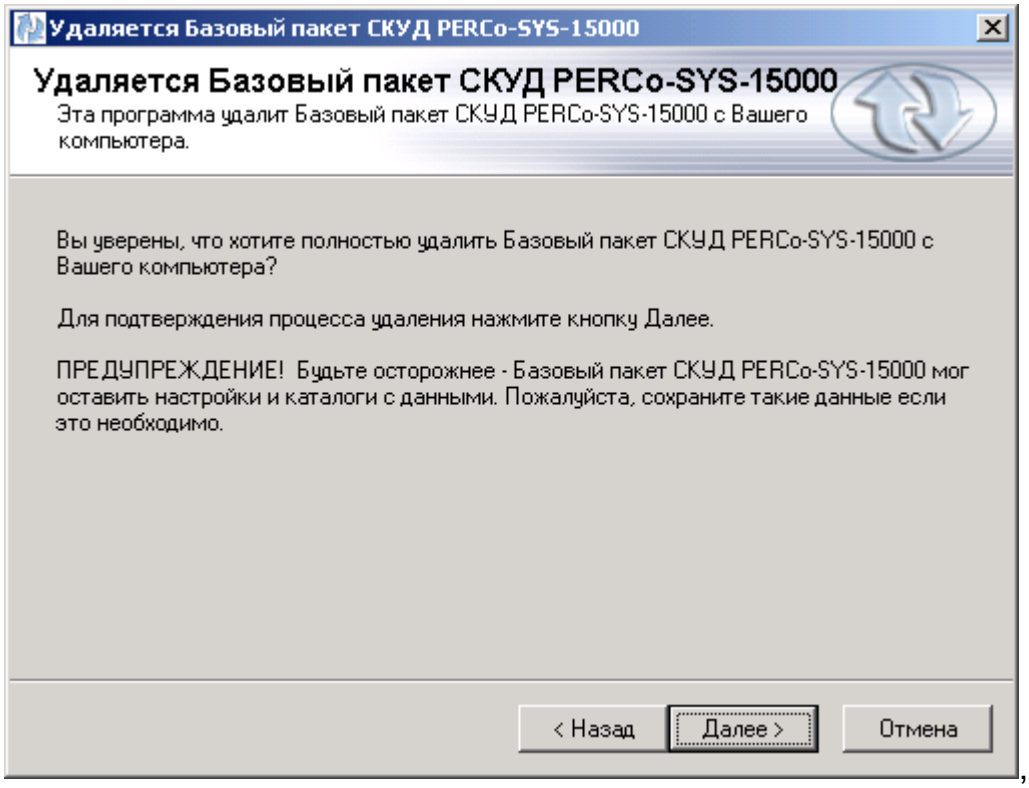


9.1. Удаление базового пакета программного обеспечения

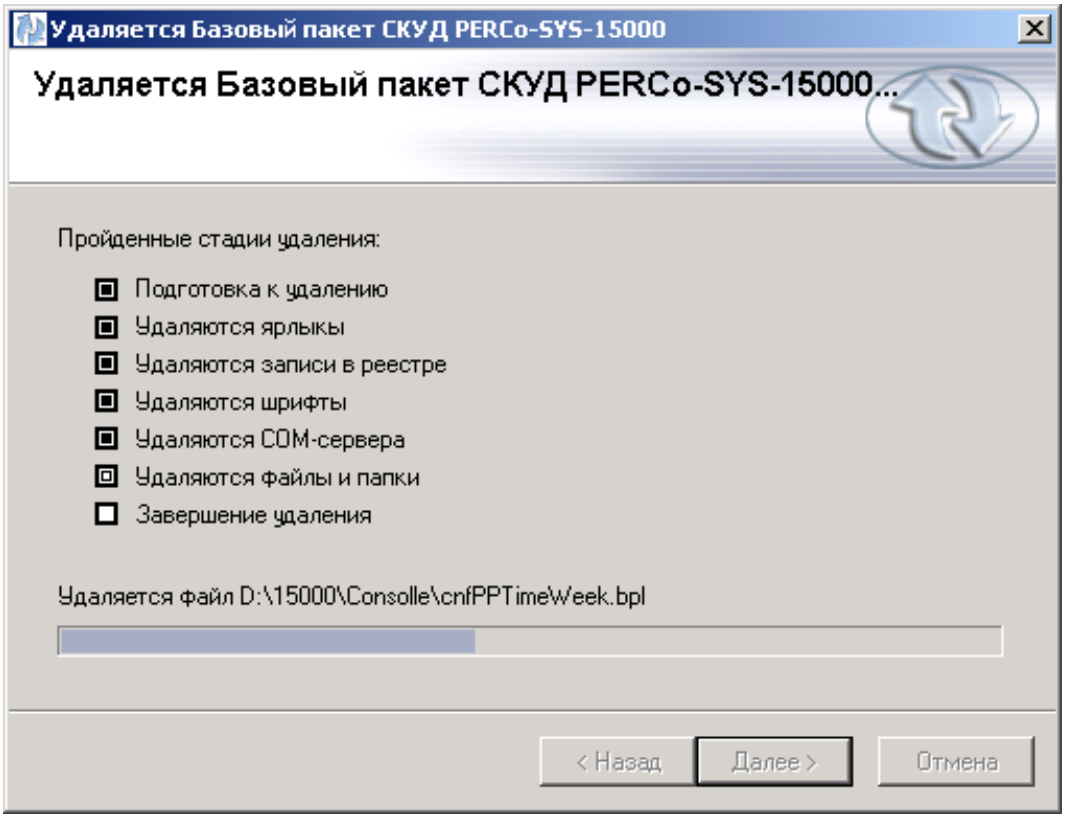
Запустите приложение «Удалить Базовый пакет СКУД PERCo-SYS-15000».



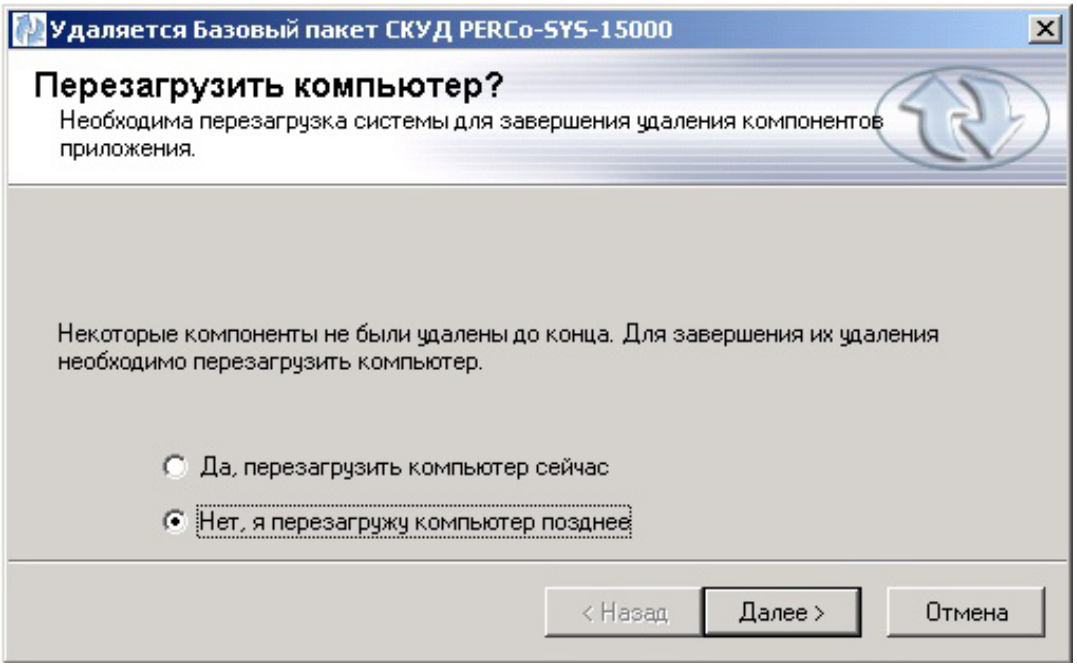
При нажатии на кнопку «Далее» появится окно, в котором нужно подтвердить согласие на удаление.



После этого последовательность удаления можно наблюдать в следующем окне:

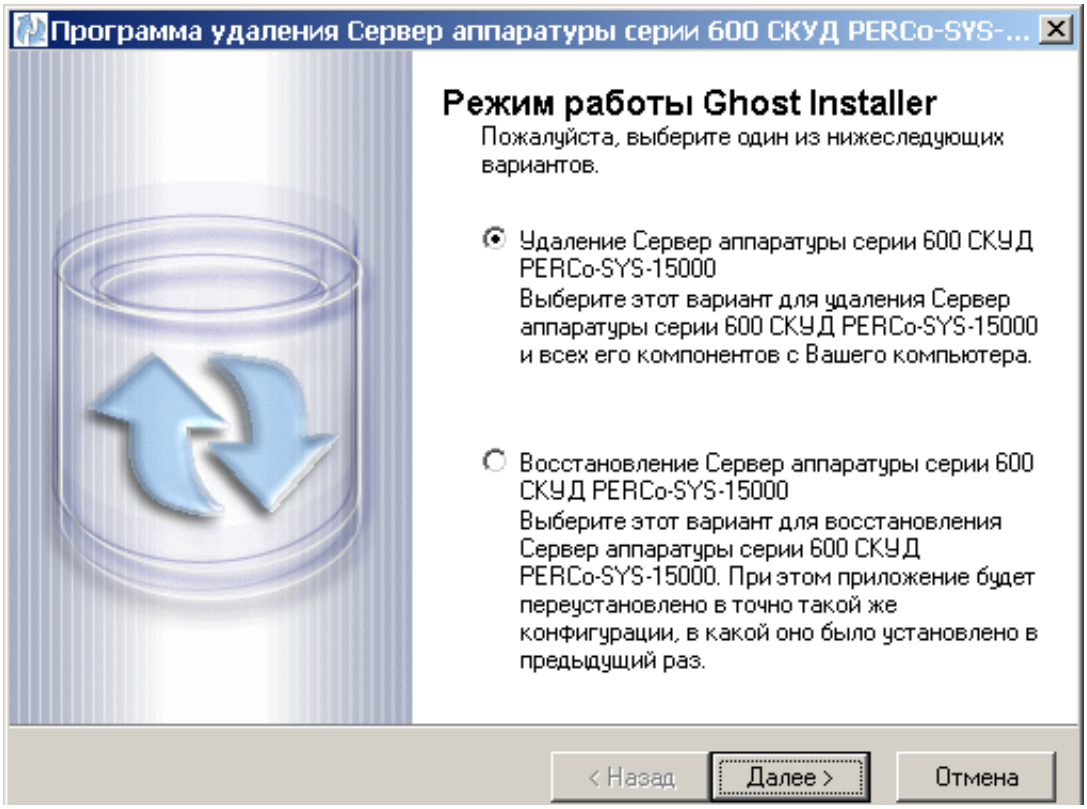


После удаления каждого из модулей предлагается перезагрузить компьютер для завершения удаления.



9.2. Удаление модуля «Сервер аппаратуры 600»

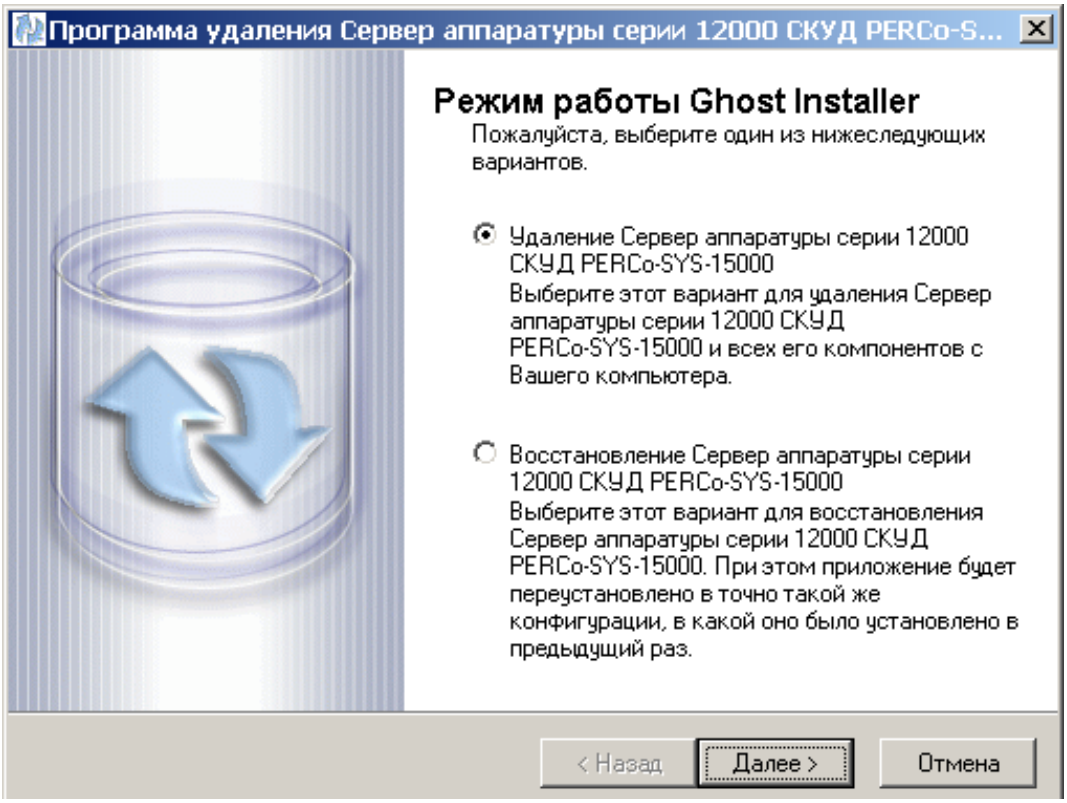
Запустить приложение «Удалить сервер аппаратуры серии 600».



Далее необходимо подтвердить удаление и для окончательного результата перезагрузить компьютер.

9.3. Удаление модуля «Сервер аппаратуры серии 12000»

Запустить приложение «Удалить Сервер аппаратуры серии 12000».



Далее необходимо подтвердить удаление и для окончательного результата перезагрузить компьютер.

ПРИЛОЖЕНИЕ 1

События мониторинга и регистрации для контроллеров 12000 серии

Событие	Категория		Причины возникновения события
	Мони-торинг	Журнал регист-рации	
Системные события узла Аутентификации			
Запрет пропуска	*		Запрет карты
Системные события контроллера			
Очистка журнала регистрации	*	*	Событие происходит после чтения переполненного журнала регистрации
Переполнение журнала регистрации	*	*	Событие возникает после заполнения в памяти контроллера предпоследней свободной страницы журнала (размер одной страницы равен 32 событиям)
Авария питания от электросети	*	*	Событие возникает в случае отсутствия внешнего сетевого питания, т.е. при переходе контроллера на питание от встроенного резервного аккумулятора
Восстановление питания от электросети	*	*	Событие возникает в случае возобновления внешнего сетевого питания
Авария питания от аккумулятора	*	*	Событие возникает при разряде встроенного резервного аккумулятора до напряжения 10±0.5 В. Это событие сопровождается автоматическим выключением контроллера
Восстановление питания от аккумулятора	*	*	Событие возникает после включения контроллера с восстановленным сетевым питанием и предельно разряженным аккумулятором. Это событие означает восстановление возможности заряда аккумулятора в фоновом режиме. Сам процесс заряда может длиться несколько часов, в зависимости от степени разряда
Тревога	*		Событие связано с возникновением тревожной ситуации в системе (см. параметры генератора тревоги)
Сброс тревоги	*		Событие связано со сбросом сигнала тревоги оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Нарушение связи	*	*	Событие относится к разряду диагностических и отражает возможное нарушение работоспособности контроллера
Восстановление связи	*	*	Событие относится к разряду диагностических и отражает возможное восстановление работоспособности контроллера
Нарушение системной конфигурации	*		Событие связано с нарушением энергонезависимости оперативной памяти контроллера и, как следствие, с потерей системных установок, необходимых для нормального функционирования. Для восстановления системной конфигурации необходимо выполнить переконфигурацию системы

Восстановление системной конфигурации	*		События связаны с восстановлением энергонезависимости оперативной памяти контроллера и, как следствие, с восстановлением системных установок, необходимых для нормального функционирования
Включение питания		*	Событие связано с включением питания контроллера
Выключение питания		*	Событие связано с выключением питания контроллера
Системные события считывателя			
Запрос на подтверждение, пропуск РАЗРЕШЕН	*		Специальное событие для видеоидентификации
Запрос на подтверждение, нарушение РЕЖИМА ВРЕМЕНИ	*		Специальное событие для видеоидентификации
Запрос на подтверждение, нарушение РЕЖИМА ЗОНАЛЬНОСТИ	*		Специальное событие для видеоидентификации
Запрос на подтверждение, пропуском снят режим доступа ОХРАНА	*		Специальное событие для видеоидентификации
Тревога, пропуск ЗАПРЕЩЕН или НЕ ЗАРЕГИСТРИРОВАН	*		Предъявленная карта запрещена или никому не выдана (если установлен параметр генератора тревоги «Причины генерации тревоги» - «Пропуск ЗАПРЕЩЕН или НЕ ЗАРЕГИСТРИРОВАН» и в параметре считывателя «Контроль РЕЖИМА ДОСТУПА установлен вариант «Жесткий без подтверждения»)
Тревога, пропуск из СТОП-ЛИСТА	*		Предъявленная карта включена в СТОП-лист (если установлен параметр генератора тревоги «Причины генерации тревоги» — «Пропуск из СТОП-листа»)
Тревога, нарушение КОМИССИОНИРОВАНИЯ	*		Нарушение комиссионирования, т.е. было зафиксировано несоответствие с комиссионирующей картой или кодовой комбинацией, или комиссионирование не было выполнено вообще (если установлен параметр генератора тревоги «Причины генерации тревоги» - «Нарушение комиссионирования»)
Тревога, пропуск вне ДИАПАЗОНОВ КАРТ ДОСТУПА	*		Предъявленная карта не относится к системным, т.е. карта не входит в сегментированный набор системных карт (если установлен параметр генератора тревоги «Причины генерации тревоги» — «Пропуск вне ДИАПАЗОНОВ КАРТ ДОСТУПА»)
Тревога, нарушение РЕЖИМА ВРЕМЕНИ	*		Несоответствие предъявленной карты временным критериям доступа (если установлен параметр генератора тревоги «Причины генерации тревоги» - «Нарушение РЕЖИМА ВРЕМЕНИ» и в параметре считывателя «Контроль РЕЖИМА ВРЕМЕНИ» выбран вариант “Мягкий” или “Жесткий без подтверждения”)

Тревога, нарушение РЕЖИМА ДОСТУПА	*		Несоответствие режима доступа предъявленной карты текущему режиму доступа контроллера (если установлен параметр генератора тревоги «Причины генерации тревоги» - «Несоответствие РЕЖИМА ДОСТУПА»)
Тревога, нарушение РЕЖИМА ЗОНАЛЬНОСТИ	*		Несоответствие текущему местоположению, т.е. предъявленная карта нарушила зональность системы (если установлен параметр генератора тревоги «Причины генерации тревоги» - «Нарушение РЕЖИМА ЗОНАЛЬНОСТИ» и в параметрах считывателя «Контроль РЕЖИМА ВРЕМЕНИ» и «Контроль РЕЖИМА ЗОНАЛЬНОСТИ» установлены варианты «Жесткий…»)
Пропуск ЗАПРЕЩЕН или НЕ ЗАРЕГИСТРИРОВАН	*		Карта запрещена или никому не выдана
Пропуск из СТОП-ЛИСТА	*		Предъявленная карта включена в СТОП-лист
Пропуск вне ДИАПАЗОНОВ КАРТ ДОСТУПА	*		Предъявленная карта не относится к системным, т.е. карта не входит в сегментированный набор системных карт
Тревога, нарушение КОМИССИОНИРОВАНИЯ	*		Нарушение комиссионирования, т.е. было зафиксировано несоответствие с комиссионирующей картой или кодовой комбинацией, или комиссионирование не было выполнено вообще
Нарушение РЕЖИМА ВРЕМЕНИ	*		Несоответствие предъявленной карты временным критериям доступа
Нарушение РЕЖИМА ЗОНАЛЬНОСТИ	*		Несоответствие текущему местоположению, т.е. предъявленная карта нарушила зональность данной системы
Нарушение РЕЖИМА ДОСТУПА	*		Несоответствие режима доступа предъявленной карты текущему режиму доступа контроллера
Пропуском снят режим доступа ОХРАНА	*	*	Установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ поднесением карты, обладающей правом автономной смены режима доступа
Пропуском установлен режим доступа ОХРАНА	*	*	Установлен режим доступа ОХРАНА поднесением карты, обладающей правом автономной смены режима доступа
Системой установлен режим доступа ОТКРЫТО	*	*	Установлен режим доступа ОТКРЫТО оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”.
Системой установлен режим доступа АВТОНОМНЫЙ КОНТРОЛЬ	*	*	Установлен режим доступа АВТОНОМНЫЙ КОНТРОЛЬ оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”.

Системой установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ	*	*	Установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Системой установлен режим доступа ОХРАНА	*	*	Установлен режим доступа ОХРАНА оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Системой установлен режим доступа ЗАКРЫТО	*	*	Установлен режима доступа ЗАКРЫТО оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Попытка доступа без совершения прохода		*	После поднесения карты, обладающей правом доступа, к считывателю, проход не был совершен
Проход		*	Проход по карте
Вход		*	Вход на объект по карте
Выход		*	Выход с объекта по карте
Проход с подтверждением от ДУ, нарушение РЕЖИМА ВРЕМЕНИ		*	Проход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ВРЕМЕНИ» - «Жесткий с подтверждением от ДУ»
Вход с подтверждением от ДУ, нарушение РЕЖИМА ВРЕМЕНИ		*	Вход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ВРЕМЕНИ» - «Жесткий с подтверждением от ДУ»
Выход с подтверждением от ДУ, нарушение РЕЖИМА ВРЕМЕНИ		*	Выход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ВРЕМЕНИ» - «Жесткий с подтверждением от ДУ»
Проход с подтверждением от ДУ, нарушение РЕЖИМА ЗОНАЛЬНОСТИ		*	Проход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ЗОНАЛЬНОСТИ» - «Жесткий с подтверждением от ДУ»
Вход с подтверждением от ДУ, нарушение РЕЖИМА ЗОНАЛЬНОСТИ		*	Вход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ЗОНАЛЬНОСТИ» - «Жесткий с подтверждением от ДУ»
Выход с подтверждением от ДУ, нарушение РЕЖИМА ЗОНАЛЬНОСТИ		*	Выход совершен при помощи ДУ при установленном параметре считывателя «Контроль РЕЖИМА ЗОНАЛЬНОСТИ» - «Жесткий с подтверждением от ДУ»
Отказ в доступе, пропуск ЗАПРЕЩЕН или НЕ ЗАРЕГИСТРИРОВАН		*	Предъявленная карта запрещена или никому не выдана
Отказ в доступе, пропуск из СТОП-листа		*	Предъявленная карта включена в СТОП-лист
Отказ в доступе, пропуск вне ДИАПАЗОНОВ КАРТ ДОСТУПА		*	Предъявленная карта не относится к системным, т.е. карта не входит в сегментированный набор системных карт

Отказ в доступе, нарушение РЕЖИМА КОМИССИОНИРОВАНИЯ		*	Нарушение комиссионирования, т.е. было зафиксировано несоответствие с комиссионирующей картой или кодовой комбинацией, или комиссионирование не было выполнено вообще
Отказ в доступе, нарушение РЕЖИМА ВРЕМЕНИ		*	Несоответствие предъявленной карты временным критериям доступа
Отказ в доступе, нарушение РЕЖИМА ДОСТУПА		*	Событие связано с предъявлением карты, не имеющей права доступа через исполнительный механизм, считыватель которого находится в режимах ОХРАНА или ЗАКРЫТО
Отказ в доступе, нарушение РЕЖИМА ЗОНАЛЬНОСТИ		*	Несоответствие текущему местоположению, т.е. предъявленная карта нарушила зональность системы
Отказ в доступе по ДУ		*	Отказ в доступе охранником с помощью ДУ при установленном параметре считывателя ”Контроль РЕЖИМА ДОСТУПА” – “Жесткий с подтверждением от ДУ”
Пропуск РАЗРЕШЕН	*		Предъявленная карта удовлетворяет всем критериям доступа, произошла разблокировка ИУ, возможен проход.
Системные события ИУ			
Заблокирован	*		Событие отражает изменение текущего состояния блокирующего контакта
Разблокирован	*		Событие отражает изменение текущего состояния блокирующего контакта
Тревога по разблокировке ИУ – ВЗЛОМ	*		Несанкционированное открытие ИУ
Тревога по разблокировке ИУ - Слишком долгое ОТКРЫТИЕ	*		Время активизации состояния блокирующего контакта превысило установленное предельное время разблокировки и для генератора тревоги установлен параметр «недопустимо долгое открытие. Если исполнительный механизм был разблокирован картой доступа, то дополнительно фиксируется и номер этой карты (или последней прошедшей карты)
Заблокирован Вход	*		Событие отражает изменение текущего состояния блокирующего контакта
Разблокирован Вход	*		Событие отражает изменение текущего состояния блокирующего контакта
Заблокирован Выход	*		Событие отражает изменение текущего состояния блокирующего контакта
Разблокирован Выход	*		Событие отражает изменение текущего состояния блокирующего контакта
Системные события Тестового входа			
Активизация	*	*	Изменение текущего уровня сигнала тестового входа
Сброс	*	*	Сброс входа
Тревога по АКТИВИЗАЦИИ входа	*	*	Если в генераторе тревоги установлен параметр «Тестовые входы, активизирующие генерацию тревоги»

Системные события Релейного выхода			
Активизация	*	*	Изменение текущего уровня сигнала релейного выхода
Сброс	*	*	Сброс выхода
Системные события драйвера			
Восстановление связи	*	*	Это событие относится к разряду диагностических и отражает возможное восстановление работоспособности структурных элементов системы
Нарушение связи	*	*	Это событие относится к разряду диагностических и отражает возможное нарушение работоспособности структурных элементов системы. Нарушение связи с драйвером влечет за собой полное прекращение управления следующими ресурсами: исполнительные механизмы, мониторинг тестовых входов, релейные выходы (соответственно, невозможна громкая тревога) и служебные выходы

ПРИЛОЖЕНИЕ 2

События мониторинга и регистрации для контроллеров 600 серии

Событие	Категория		Причины возникновения события
	Мони-торинг	Журнал регист-рации	
Системные события узла Аутентификации			
Тревога (по команде оператора)	*		Событие связано с активизацией сигнала тревоги оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Сброс тревоги (по команде оператора)	*		Событие связано со сбросом сигнала тревоги оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”.
Нарушение связи с конвертером RS232->RS485	*		Событие относится к разряду диагностических и отражает возможное нарушение работоспособности контроллера
Восстановление связи с конвертером RS232->RS485	*		Событие относится к разряду диагностических и отражает возможное восстановление работоспособности контроллера
Системные события контроллера			
Нарушение системной конфигурации	*		Событие связано с нарушением энергонезависимости оперативной памяти контроллера и, как следствие, с потерей системных установок, необходимых для нормального функционирования. Для восстановления системной конфигурации необходимо выполнить переконфигурацию системы
Восстановление системной конфигурации	*		События связаны с восстановлением энергонезависимости оперативной памяти контроллера и, как следствие, с восстановлением системных установок, необходимых для нормального функционирования
Нарушение связи	*		Событие относится к разряду диагностических и отражает возможное нарушение работоспособности контроллера
Восстановление связи	*		Событие относится к разряду диагностических и отражает возможное восстановление работоспособности контроллера
Тревога (по команде оператора)	*		Событие связано с активизацией сигнала тревоги оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг“
Сброс тревоги (по команде оператора)	*	*	Событие связано со сбросом сигнала тревоги оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Попытка доступа через заблокированное ИУ		*	Событие связано с попыткой доступа на объект при заблокированном состоянии исполнительного устройства

Нарушение режима доступа		*	Событие связано с попыткой доступа на объект при установленном режиме доступа ОХРАНА
Пропуском установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ	*	*	Установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ поднесением карты, обладающей правом автономной смены режима доступа
Пропуском установлен режим доступа ОХРАНА	*	*	Установлен режим доступа ОХРАНА поднесением карты, обладающей правом автономной смены режима доступа
Системой установлен режим доступа ОТКРЫТО	*	*	Установлен режим доступа ОТКРЫТО оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Системой установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ	*	*	Установлен режим доступа СИСТЕМНЫЙ КОНТРОЛЬ оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Системой установлен режим доступа ОХРАНА	*	*	Установлен режим доступа ОХРАНА оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
Системой установлен режим доступа ЗАКРЫТО	*	*	Установлен режим доступа ЗАКРЫТО оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг”
ТРЕВОГА по разблокировке замка — ВЗЛОМ	*	*	Несанкционированное открытие замка
ТРЕВОГА по датчику прохода		*	Тревога по датчику прохода
Системные события считывателя			
Проход		*	Проход по карте
Вход		*	Вход на объект по карте
Выход		*	Выход с объекта по карте
Отказ в доступе, нарушение РЕЖИМА ВРЕМЕНИ		*	Несоответствие предъявленной карты временным критериям доступа
Отказ в доступе, нарушение РЕЖИМА ЗОНАЛЬНОСТИ		*	Несоответствие текущему местоположению, т.е. предъявленная карта нарушила зональность данной системы
Проход от ДУ		*	Проход разрешен оператором системы под управлением ПО "Консоль управления PERCo-SYS-15000" из подраздела “Управление устройствами” раздела “Мониторинг” или нажатием соответствующей кнопки ПДУ
Несанкционированный проход		*	Событие, возникающее при проходе на объект с нарушением прав доступа (например, при поломке исполнительного механизма)