# РУКОВОДСТВО АДМИНИСТРАТОРА

**Программное обеспечение «КОДОС»**

**ИНТЕГРИРОВАННЫЙ КОМПЛЕКС БЕЗОПАСНОСТИ «КОДОС»**

# Оглавление

# 1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

Интегрированный Комплекс Безопасности «КОДОС» включает системы контроля и управления доступом, охранно-пожарной сигнализации, видеонаблюдения, жизнеобеспечения объекта и определения номеров автотранспорта, объединенные общей информационной средой.

ИКБ – это система комплексного управления безопасностью объекта. Комплекс «КОДОС» дает возможность оператору системы безопасности получать полную, достоверную и оперативную информацию о состоянии безопасности на объекте. Причем информация поступает в такой форме, которая позволяет оператору адекватно оценивать ситуацию на объекте и благодаря этому принимать своевременные безошибочные решения.

Данное руководство предназначено для инженеров монтажных организаций, системных администраторов, сотрудников IT-отделов организаций, занимающихся непосредственной установкой, настройкой и обслуживанием интегрированной системы безопасности «КОДОС». Руководство содержит сведения, необходимые для обеспечения правильной инсталляции и использования возможностей системы.

Подразумевается, что персонал, производящий настройку оборудования, имеет не только первичные знания по работе с компьютером и основные понятия о системах контроля доступа, ОПС и системах видеонаблюдения, но и представляет основные принципы построения локальной сети, умеет выполнять манипуляции по установке и настройке оборудования, программного обеспечения, его конфигурирования в соответствии с решаемыми задачами.

Данное руководство может быть использовано для обучения работы с программным обеспечением «КОДОС-ИКБ».

## 1.1 Защита по кодос от несанкционированного использования

Программное обеспечение, разрабатываемое в ООО «КОДОС» имеет защиту от несанкционированного использования. Защита реализована в виде аппаратных и программных средств, препятствующих незаконному запуску ПО и его работе.

Пользователь, приобретая программный продукт торговой марки «Кодос», получает ключ аппаратной защиты и лицензию.

**ВНИМАНИЕ!** Эксплуатация ПО семейства «КОДОС» без ключа аппаратной защиты не предусмотрена!

Ключ аппаратной защиты – техническое средство защиты на аппаратном уровне от несанкционированного копирования и эксплуатации ПО. Совместно с лицензией на использование ключ разрешает доступ к модулям программного обеспечения для использования имеющегося оборудования в полном объеме.

Ключи аппаратной защиты представляет собой USB-ключ, который постоянно должен находиться в USB-разъеме при работе ПО. Физически на один компьютер должен быть установлен только один ключ аппаратной защиты.

**ВНИМАНИЕ!** В новых версиях ПО сохранена поддержка LPT-ключей защиты.

Установка драйверов для ключей защиты выполняется в автоматическом режиме при первой установке ключа после установки программы.

Лицензия на программный продукт дает право на использование тех или иных компонентов «КОДОС» (программных модулей, режимов работы системы, количество подключаемого оборудования и т.д.) с конкретным ключом защиты, и представляет собой текстовую строку специального вида:

«XXXXXXXX-XXXXXXXX-...».

Лицензиями управляет специальная программа – «Менеджер лицензий». Она устанавливается автоматически вместе с ПО. Запустить программу можно стандартным способом, например:

Пуск → Программы (Все программы) → ИКБ КОДОС → Утилиты → Менеджер лицензий.(рисунок 1.1.1).

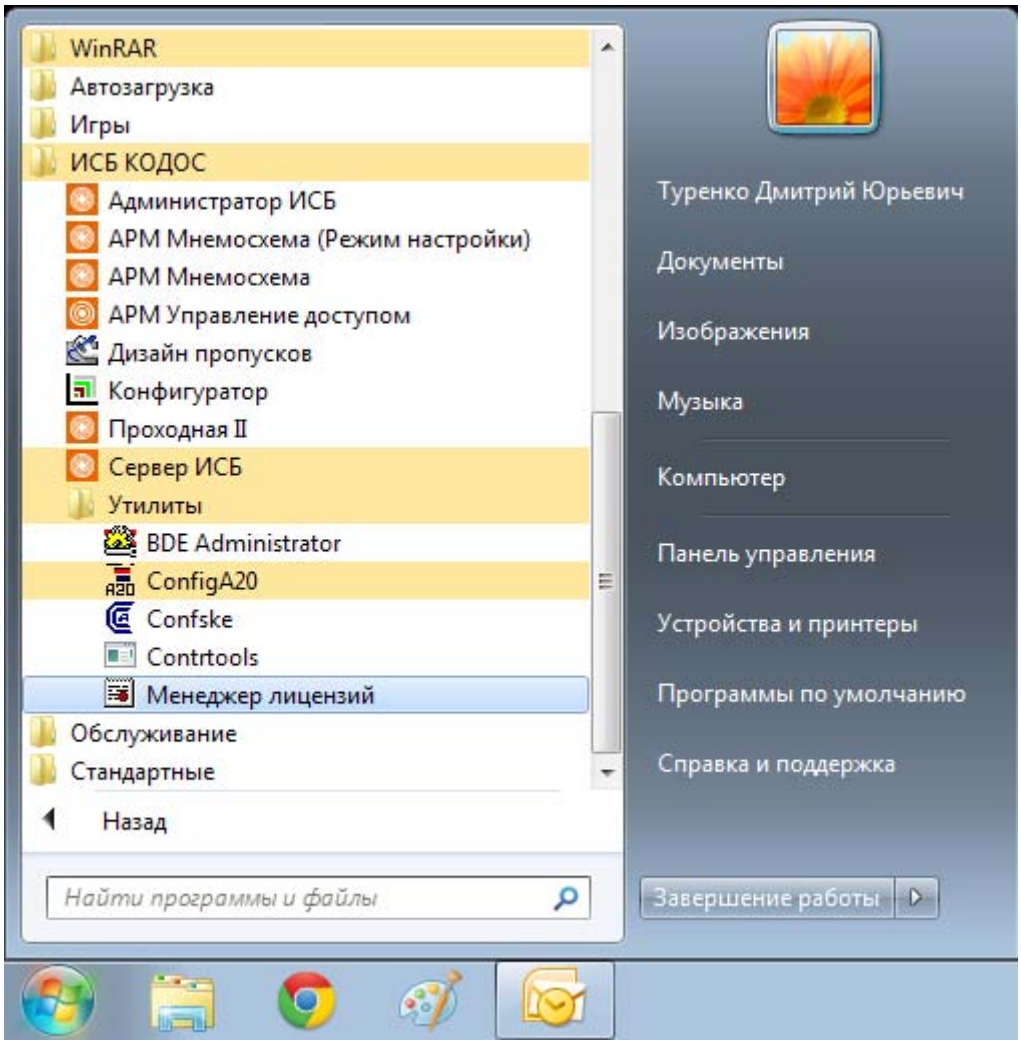



**Рисунок 1.1.1 – Запуск менеджера лицензий**

Главное окно программы представлено на рисунке 1.1.2.

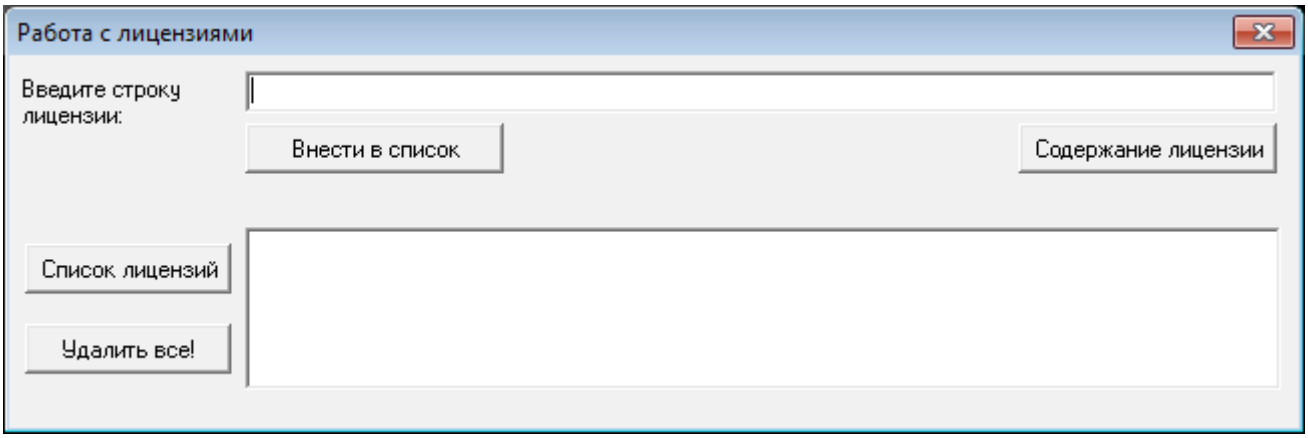



**Рисунок 1.1.2 – Главное окно менеджера лицензий**

Код лицензии необходимо внести в поле «Введите строку лицензии». При наборе символов будьте внимательны, вводите только те символы, что указаны в лицензии. После проверки правильности ввода нажмите кнопку «Внести в список» (рисунок 1.1.3).

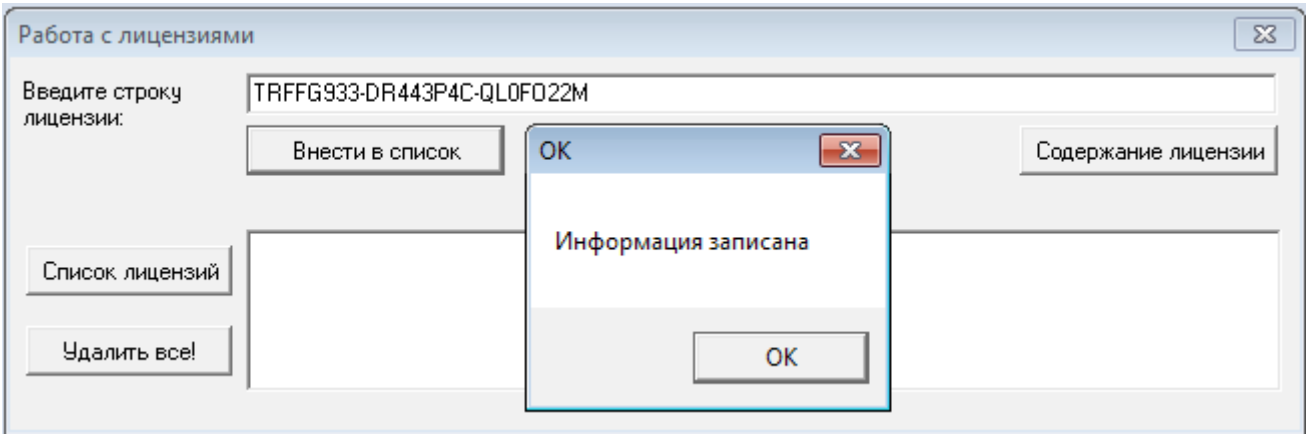



**Рисунок 1.1.3 – Запись кода лицензии**

Появится сообщение о вводе, а в списке лицензий добавится введенный код.

Если в процессе эксплуатации программного продукта возникла необходимость расширения возможностей ПО (установка дополнительных модулей, увеличение числа используемого оборудования) или установки на один ПК нескольких программных продуктов, то необходимо добавить полученный код лицензии к уже имеющемуся (рисунок 1.1.4).

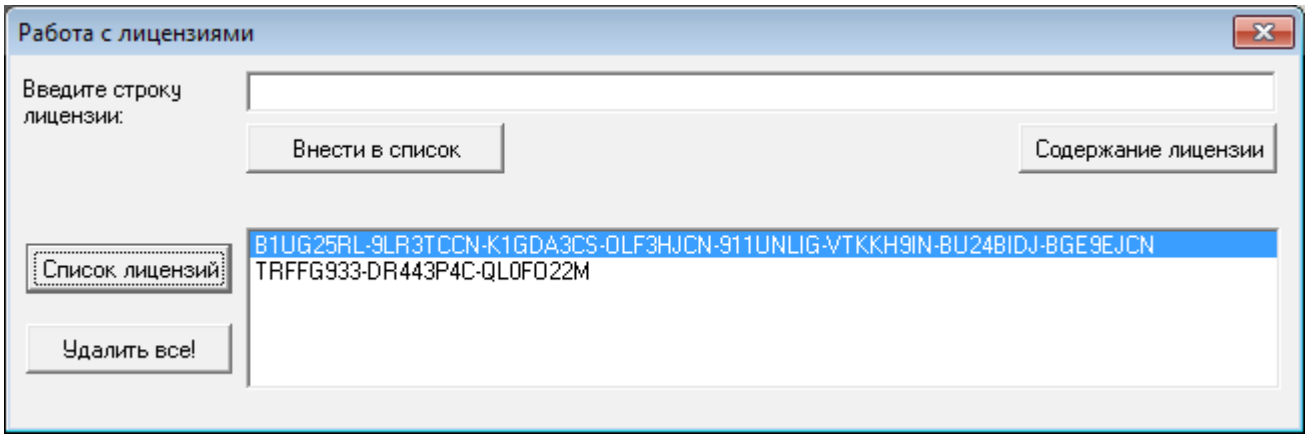



**Рисунок 1.1.4 – Несколько кодов лицензий на одном ПК**

ПРИМЕЧАНИЕ – При необходимости расширения возможностей ПО необходимо обратиться в ООО «КОДОС» или представителям компании в регионах для переоформления лицензии. При использовании нескольких программных продуктов на одном ПК необходимо проконсультироваться со специалистами об их совместимости.

Содержание введенной лицензии можно узнать, нажав кнопку «Содержание лицензии».(рисунок 1.1.5)

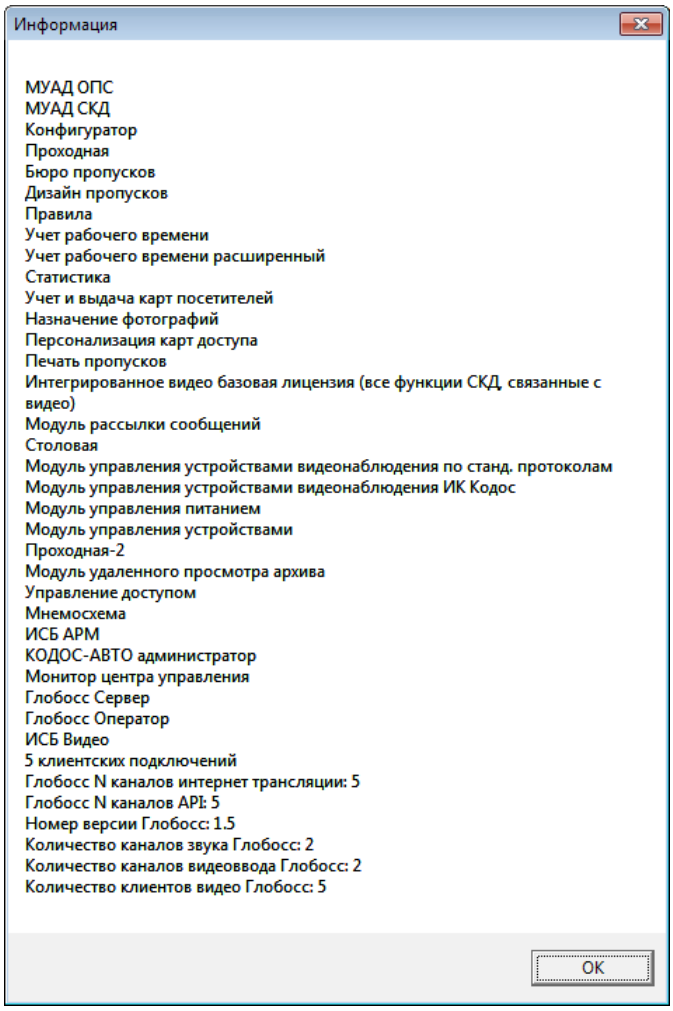



**Рисунок 1.1.5 – Вариант содержания лицензии**

**ПО Кодос-ИКБ**

После процедуры регистрации модули ПО, соответствующие ключу, становятся доступными для использования.

## 1.2 Требования к компьютеру

Рекомендуемые требования к программному обеспечению компьютера:

- ОС Windows XP SP3, с пакетом DirectX 9c, Windows 7
- Файловая система NTFS.
- Программы Microsoft Word, Excel из пакета MS Office (для работы с отчетами).

Минимальные требования к компьютеру при работе «КОДОС-ИКБ» (без видеонаблюдения):

- Процессор с частотой 1.6ГГц – 2.6ГГц ;
- Объем оперативной памяти (ОЗУ) – 1 Гб;
- Объем жесткого диска – 160 Гб.

Рекомендуемые требования к компьютеру при работе «КОДОС-ИКБ» (без видеонаблюдения):

- Процессор  с частотой от 2,83 ГГц
- Объем оперативной памяти (ОЗУ) – 2 Гб;
- Объем жесткого диска – 320 Гб.

Рекомендуемые требования к компьютеру при работе «КОДОС-ИКБ» с программой «GLOBOSS» зависят от количества видеоканалов.

| | Количество видеоканалов | | | |
|---|---|---|---|---|
| | До 4 | До 8 | До 16 | Свыше 16 |
| Процессор | Intel Core i5-670 3.46 GHz | Intel Core i5-670 3.46 GHz | Intel Core i7-2600 3.4 GHz | Intel Core i7-2600 3.4 GHz |
| Жесткий диск, Гб | 160* | 250* | 320* | 500* |
| Оперативная память, Мб | 2048(2x1024) | 2048 (2x1024) | 2048 (2x1024) | 2048 (2x1024) |
| Видеокарта | nVidia GT 240, GT 440 | nVidia GT 240, GT 440 | nVidia GT 240, GT 440 | nVidia GT 240, GT 440 |

**ВНИМАНИЕ!**

1. Требования установлены по состоянию на июнь 2012 года и могут быть изменены. При обновлении ПО с более ранних версий возможна его работа на существующей конфигурации оборудования.

2. Не рекомендуется использовать на одном ПК ПО «КОДОС-ИКБ» совместно с программой «GLOBOSS» при количестве каналов больше 16 из-за большой загрузки процессора. В этом случае программу «GLOBOSS» необходимо устанавливать на отдельный ПК.

3. Выбор объема жесткого диска определяется количеством камер видеонаблюдения и параметрами записи.

# 2 УСТАНОВКА ПРОГРАММЫ

## 2.1 Подготовка к установке

**ВНИМАНИЕ!** Устанавливать систему необходимо под профилем Администратора, устанавливаемого ОС Windows по умолчанию.

Для операционных систем Windows 2000 и Windows XP, выполнить команду: «Пуск» → «Настройка» → «Панель управления» → «Система» → «Оборудование» → «Диспетчер устройств» → «Порты(COM и LPT)» → «Последовательный порт (COM1)» → «Свойства» → «Параметры порта» → «Дополнительно».

В окне «Дополнительные параметры COM1» снять флажок «Использовать буферы FIFO» (рисунок 2.1.1).

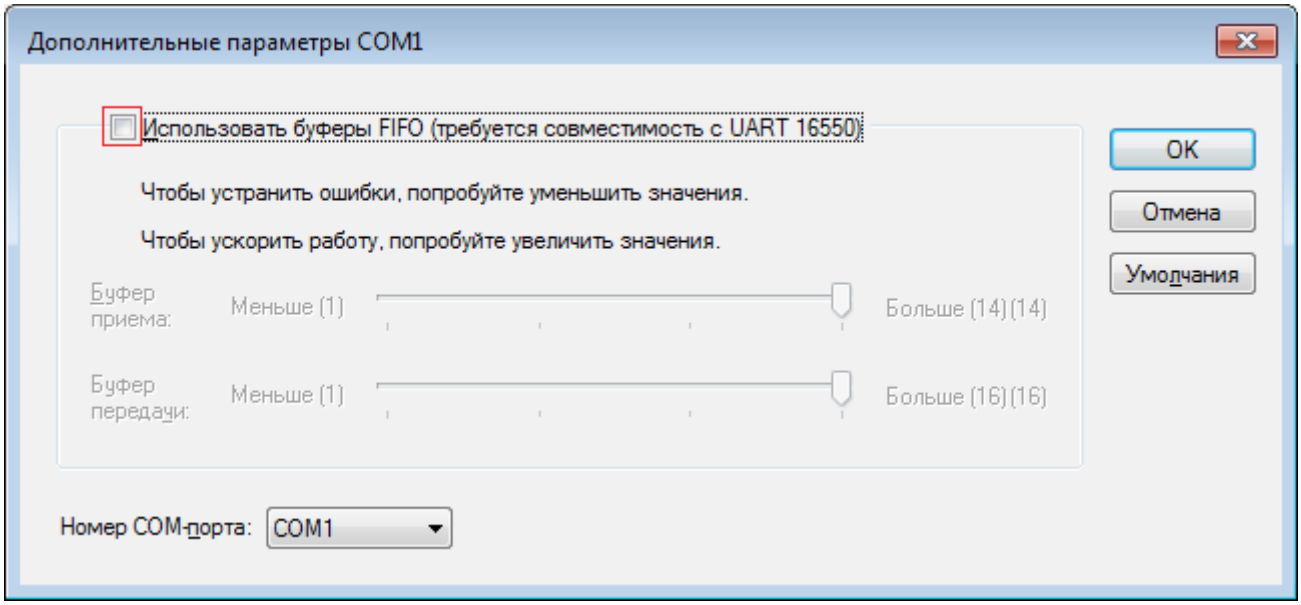



**Рисунок 2.1.1 – Дополнительные параметры COM1**

## 2.2 Организация дискового пространства

1. Для установки ПО жесткий диск ПК разбить на два раздела. ОС Windows установить в первый раздел «C».
2. Остальную часть диска отформатировать одним разделом «D:». Использовать файловую систему NTFS.
3. На диске «D:» создать каталог «D:\Install» в который копируется дистрибутив устанавливаемых продуктов, а также драйверы оборудования.
4. Продукты «КОДОС» установить в каталог «D:\SSA». Дистрибутив продуктов CCA копируется в каталог «D:\SSA\Install». Резервное копирование БД настраивается в каталог «D:\SSA\ZIP». Видеоархивы размещаются в каталогах «D:\VideoArch», «E:\VideoArch...».

## 2.3 Установка программы

Установка ИКБ КОДОС осуществляется с помощью программы инсталлятора.

1. Запустите на исполнение файл setup.exe и следуйте указаниям мастера установки:

Установка и использование программы возможна только при согласии с условиями лицензионного соглашения (рисунок 2.3.1).

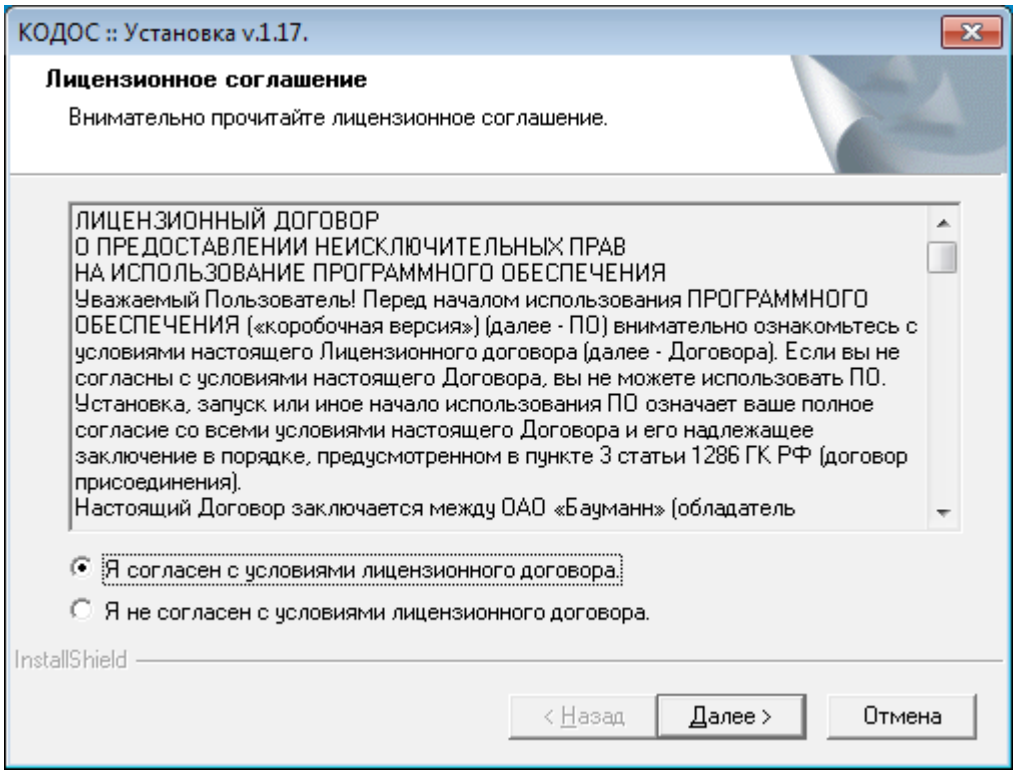



**Рисунок 2.3.1 –**

2. Укажите место установки программы, выбрать вид установки (рисунок 2.3.2).

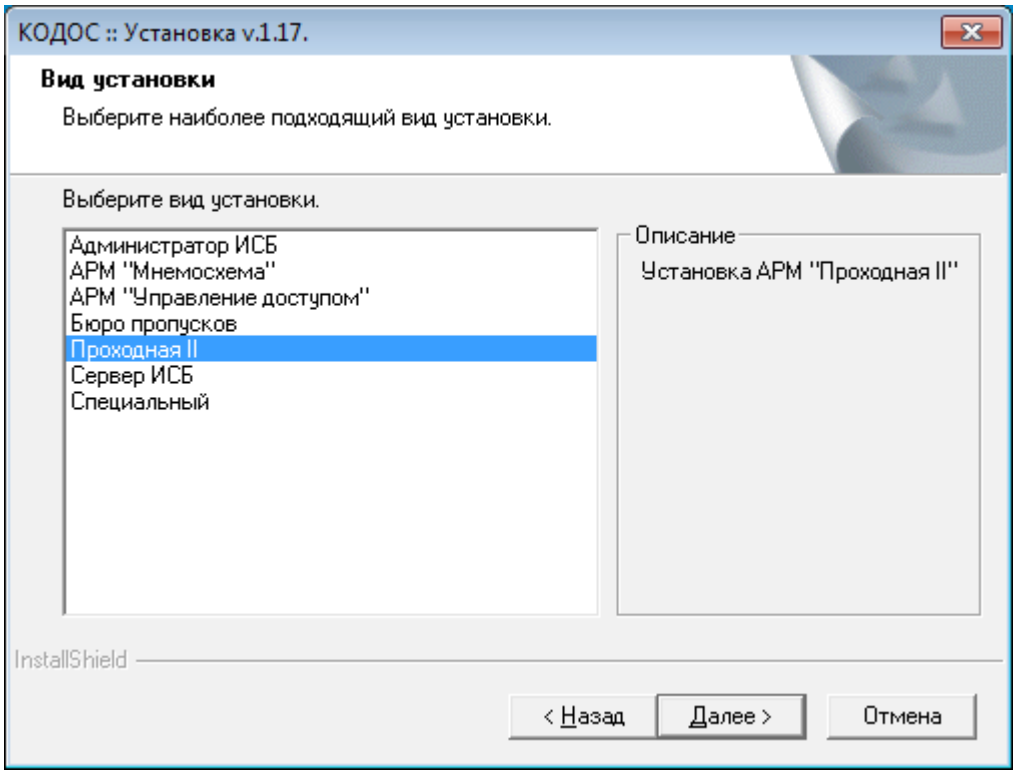



**Рисунок 2.3.2 –**

Рекомендуем воспользоваться готовыми шаблонами установки.

3. Если Вы опытный пользователь, то можно использовать вид «Специальный» и самостоятельно выбрать устанавливаемые компоненты программы (рисунок 2.3.2)

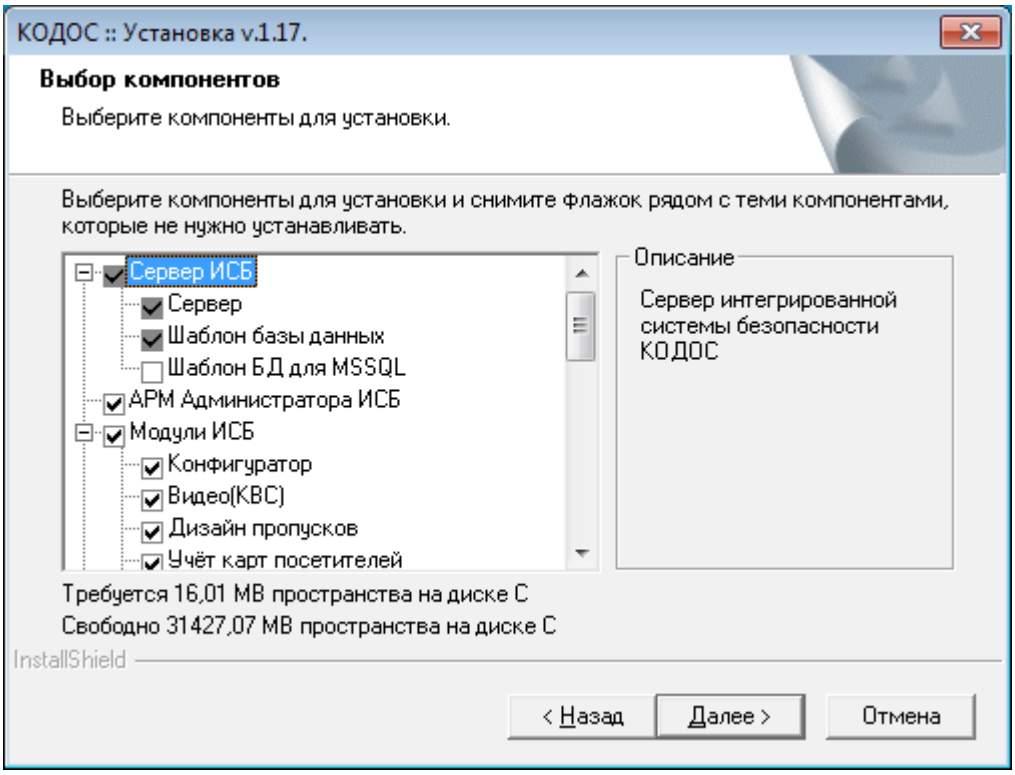



**Рисунок 2.3.3 – Выбор компонентов установки программы вручную**

При выборе устанавливаемых модулей ИКБ следует руководствоваться наличием лицензии на устанавливаемый модуль. При отсутствии лицензии установленный модуль будет недоступен.

4. Для установки серверной части СУБД FireBird в процессе установки системы «ИКБ КОДОС» установить флажок «Сервер СУБД FireBird». Установленный FireBird Server будет запускаться при загрузке Windows.

5. Если сервер СУБД FireBird установлен на другом компьютере, то достаточно установить только клиентскую часть СУБД. Для этого следует установить флажок «Клиент СУБД Firebird».

6. Установка сервера СУБД FireBird и сервера системы «ИКБ КОДОС» на разных компьютерах не рекомендуется, так как значительно уменьшается надежность работы системы в целом.

7. При интеграции ИКБ КОДОС с системой видеонаблюдения необходимо выбрать соответствующий компонент, в зависимости от используемой системы видеонаблюдения («КОДОС-ВИДЕОСЕТЬ» или «GLOBOSS»). Одновременное использование различных систем не допускается.

## 2.4 Окончание установки

1. Запустите программу «Конфигуратор» – «Пуск» → «Программы» → «ИКБ КОДОС» → «Конфигуратор» (рисунок 2.4.1)

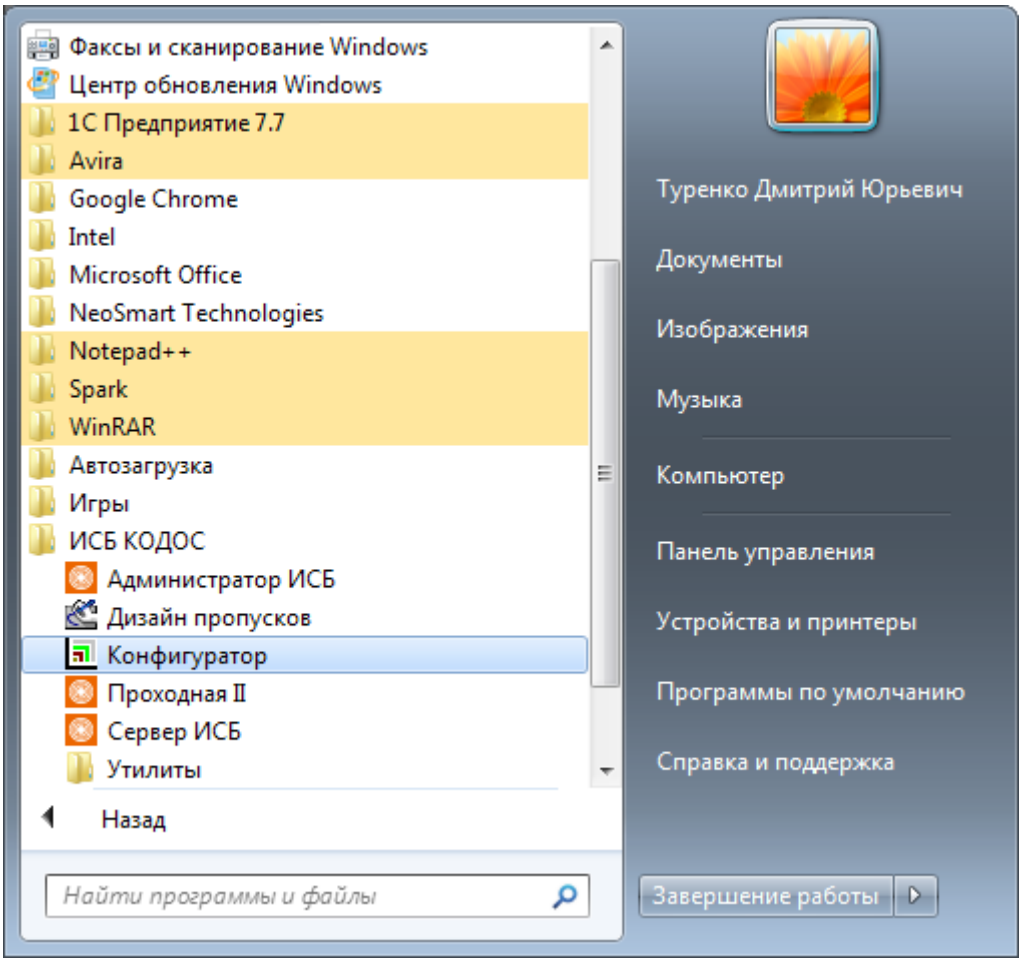



**Рисунок 2.4.1 –**

2. Выберите алиас (псевдоним) базы данных – «codos_ib» (устанавливается по умолчанию). При подключении к БД использовать имя – «sysdba», пароль – «masterkey»

**ВНИМАНИЕ!** При обновлении программы с предыдущих версий возможно появление окна с предложением обновить базу данных. В этом случае необходимо согласиться, все необходимые изменения произойдут автоматически.

3. Закройте программу «Конфигуратор»

4. Зарегистрируйте лицензионный ключ. Порядок ввода лицензионного ключа описан в п. 1.1 .

## 2.5 Особенности установки клиентских рабочих мест

1. Клиентскими рабочими местами в «ИКБ КОДОС» являются АРМ, с установленными на них программами «Администратор ИКБ», «Мнемосхема», «Проходная», «Бюро пропусков».

2. Все клиентские программы работают с базой данных, которая установлена на сервере ИКБ. Поэтому перед началом работы необходимо настроить доступ к базе данных с клиентского рабочего места.

### 2.5.1 Изменение в файле hosts

1. Найдите в системном каталоге файл hosts (C:\WINDOWS\system32\drivers\etc).

2. По аналогии с имеющимися записями добавьте в этот файл строку:

192.168.1.1 kodos_srv

В конце строки обязательно нажмите клавишу Enter!

3. Вместо указанного в данном примере IP-адреса 192.168.1.1 необходимо вписать IP-адрес компьютера, который будет использоваться в системе ИКБ "КОДОС" в качестве сервера.

4. В этот файл необходимо прописать IP-адреса всех ПК, где будет установлено ПО «КОДОС» (сервер, удаленный администратор, бюро пропусков и т.д.). Кроме этого необходимо прописать IP-адреса сетевых контроллеров и контролеров ПРО.

5. На удаленных рабочих местах в файл hosts необходимо внести аналогичные записи.

### 2.5.2 Настройки псевдонима (alias) для клиентского компьютера

Для правильного обращения программ системы «ИКБ КОДОС» к распределенной базе данных, необходимо правильно настроить псевдонимы базы данных - «alias».

При установке «ИКБ КОДОС» и СУБД FireBird с инсталляционного диска, псевдоним СУБД уже настроен, имеет имя «codos_ib» и указывает на пустой шаблон БД расположенный по адресу «localhost:D:\SSA\SKD\codos_db\codos.gdb».

**ВНИМАНИЕ!** Имя диска указано при организации пространства диска согласно п. 2.2.

Для настройки правильного обращения к базе данных с рабочего места «Администратор ИКБ» необходимо настроить путь к базе данных вручную.

Для этого

1. Запустить «BDE администратор»: «Пуск» → «Все программы» → «ИКБ КОДОС» → «Утилиты» → «BDE Administrator». Откроется окно «BDE Administrator» (рисунок 2.5.1).

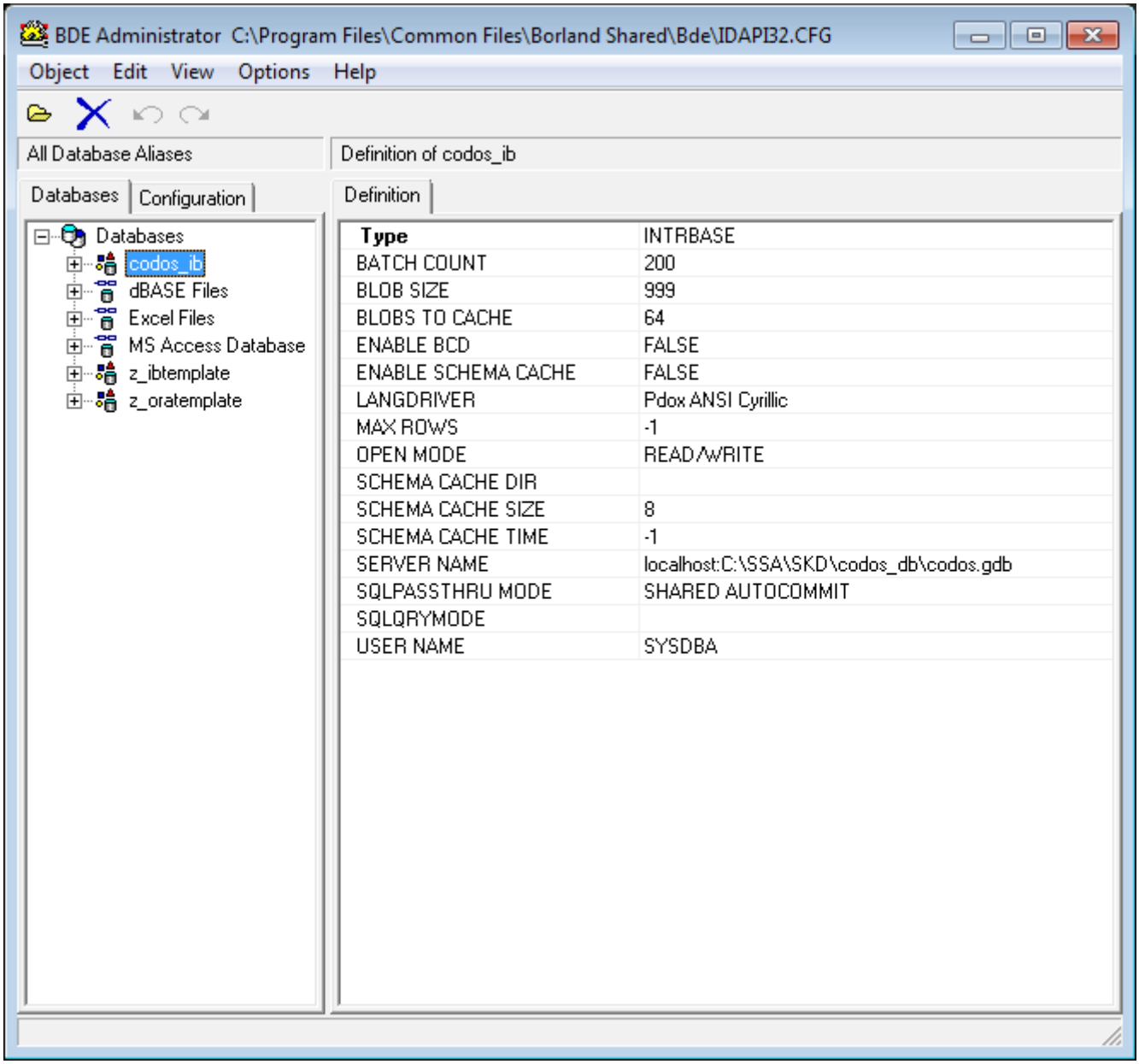



**Рисунок 2.5.1 –**

2. Выделить на вкладке «Database» имя установленного псевдонима базы данных (рисунок 2.5.1).

3. Настроить путь доступа к БД. В строке «SERVER NAME» в пустой правой части строки указать путь к файлу базы данных InterBase (FireBird). Если БД находится на сервере, то указать адрес: localhost:D:\SSA\SKD\codos_db\имя файла БД. Если БД находится на другом компьютере, то указать адрес: ИМЯ_КОМПЬЮТЕРА:C:\SSA\SKD\codos_db\имя файла БД. Вместо имени компьютера можно указать его IP-адрес. Например:192.168.111.1 :C:\SSA\SKD\codos_db\codos.gdb

4. Сохранить настройки перед выходом из BDE Administrator. В панели инструментов нажать Object□Apply.

ПРИМЕЧАНИЕ – Проверить правильность указанного пути до базы данных можно, подключившись по этому псевдониму двойным левым кликом мыши, после чего указать пароль в окне авторизации – «masterkey». Если путь до базы данных указан верно, то соединение будет установлено (см. рисунок .2.5.2).

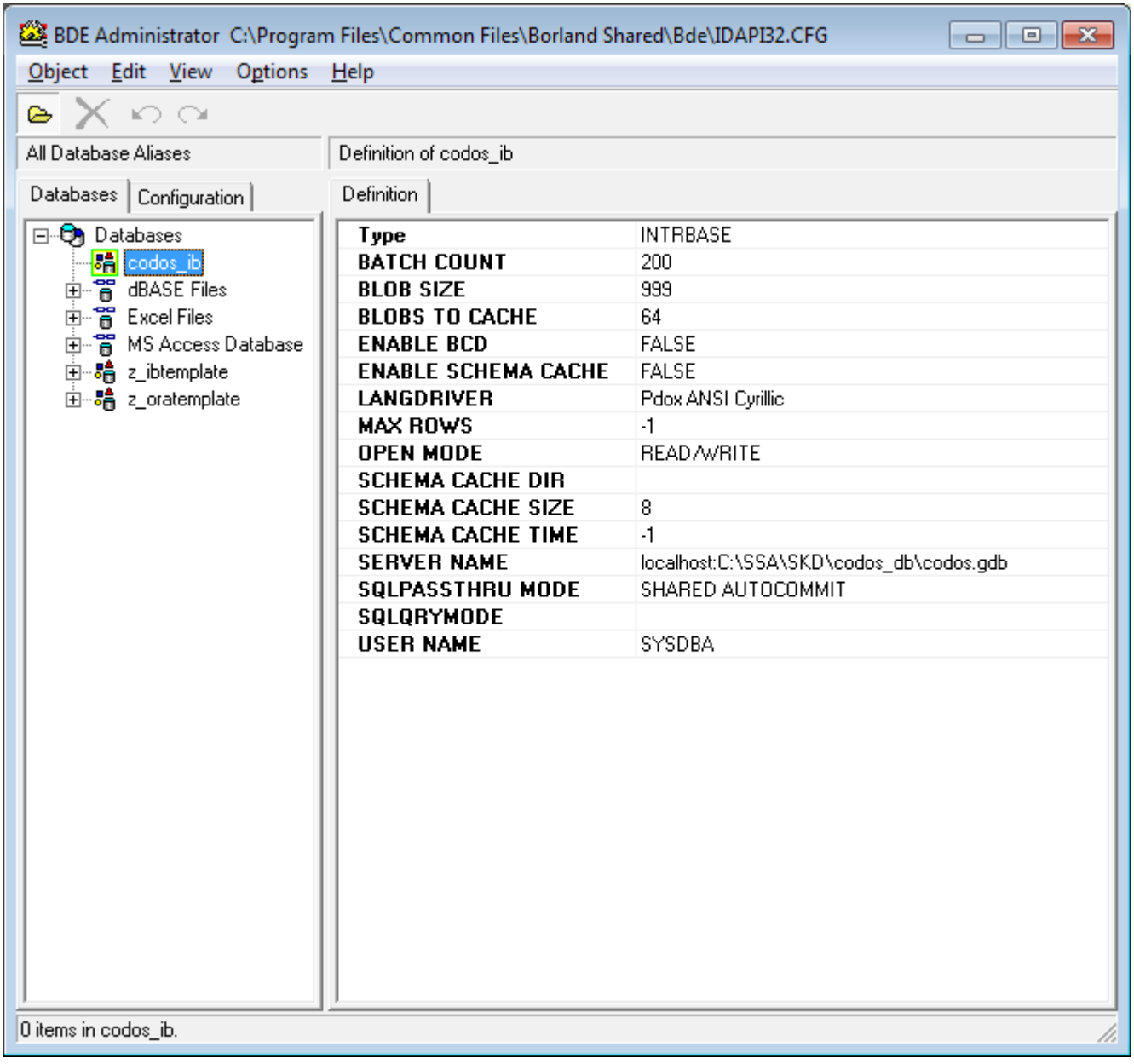



**Рисунок 2.5.2 –**

Для того чтобы программы системы «ИКБ КОДОС» правильно обращались к базе данных, необходимо указать псевдонимы базы данных - «alias» в файлах «codos.ini» на серверном и клиентских компьютерах в строке «DBAlias», например: «DBAlias=codos_ib».

## 2.6 Удаление программы

ПРИМЕЧАНИЕ – Перед удалением программы рекомендуем сохранить базу данных ИКБ КОДОС в другом каталоге.

1. Деинсталляцию рекомендуется осуществлять стандартными средствами MS Windows, например, с помощью модуля «Установки и удаления программ» (команда Пуск => Настройка => Панель управления => Установка и удаление программ).

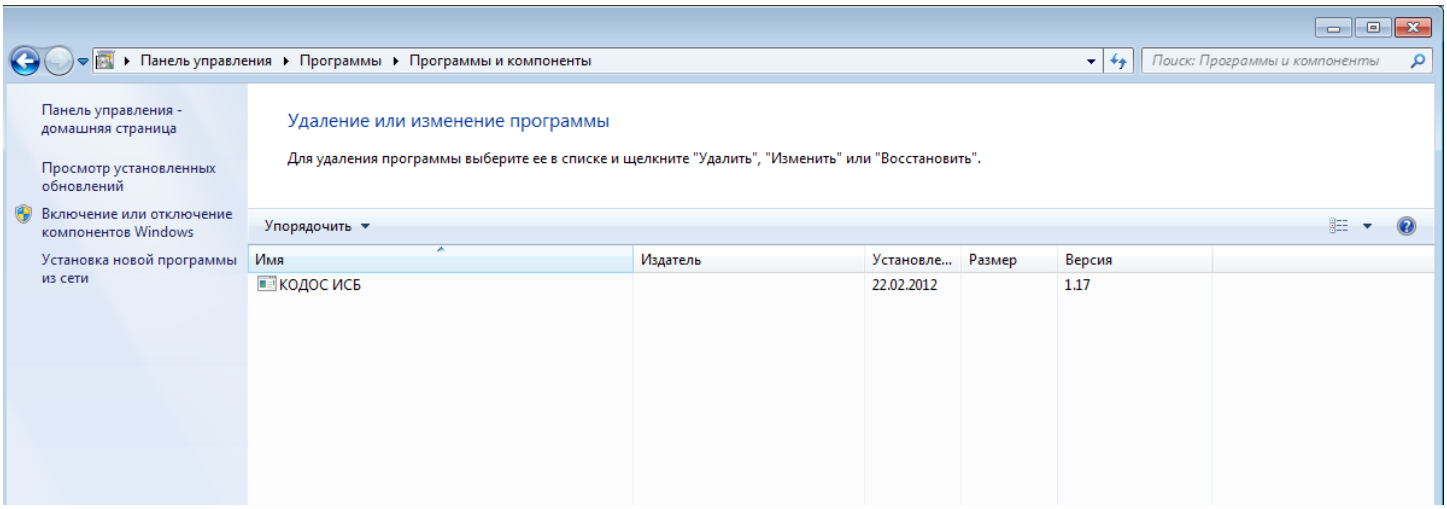



**Рисунок 2.6.1 – Окно «Установка и удаление программ»**

2. В открывшемся окне (рисунок 2.6.1) «Установка и удаление программ» во вкладке «Изменение или удаления программ» в предложенном списке необходимо выбрать «КОДОС ИКБ» и затем щелкнуть мышью по экранной кнопке «Заменить/Удалить».

3. Операционная система Windows вызовет программу «КОДОС::Установка» (рисунок 2.6.2), в окне которой (с помощью экранного переключателя) следует в качестве выбранного действия отметить «Удалить» (удаление всех установленных компонент Системы «ИКБ», в частности «Бюро пропусков»).

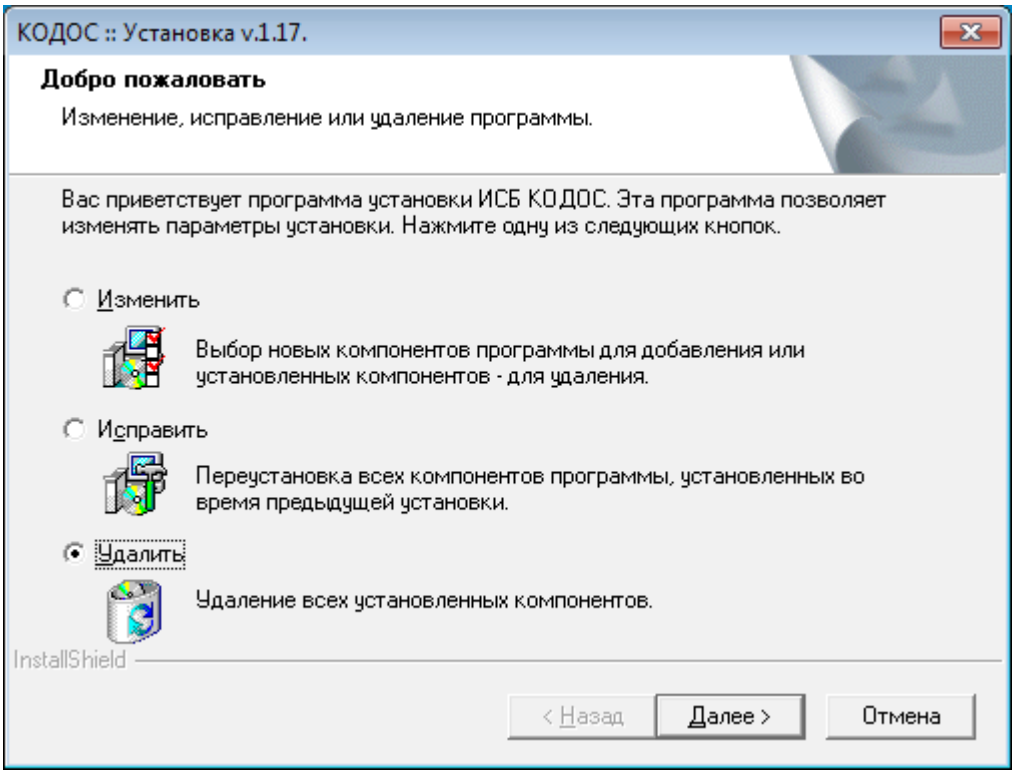



**Рисунок 2.6.2 – Окно «Удаление программы ИКБ КОДОС»**

4. При нажатии экранной кнопки «Далее>» и подтверждении решения об удалении (кнопкой «ОК») компьютер приступит к деинсталляции Системы.

5. Признаком окончания процесса деинсталляции является сообщение (рисунок 2.6.3), при появлении которого следует нажать экранную кнопку «Готово».

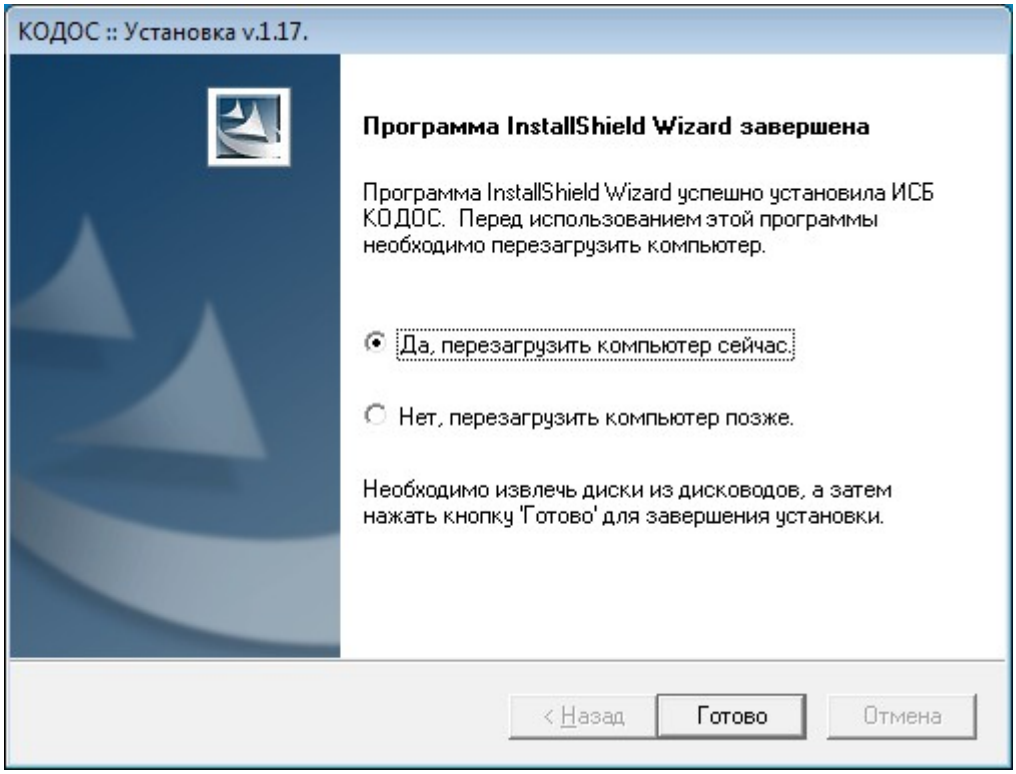



**Рисунок 2.6.3 – Окно «КОДОС::Установка». Удаление завершено**

## 2.7 Обновление программы

ПРИМЕЧАНИЕ – Перед обновлением программы рекомендуем произвести резервное копирование базы данных.

1. Перед обновлением программы необходимо сохранить текущие настройки. Для этого скопируйте файл codos.ini в резервный каталог. После окончания обновления замените файл codos.ini в каталоге программы на сохраненный.

Обновление ИКБ КОДОС осуществляется с помощью программы инсталлятора.

2. Запустите на исполнение файл setup.exe и следуйте указаниям мастера установки:

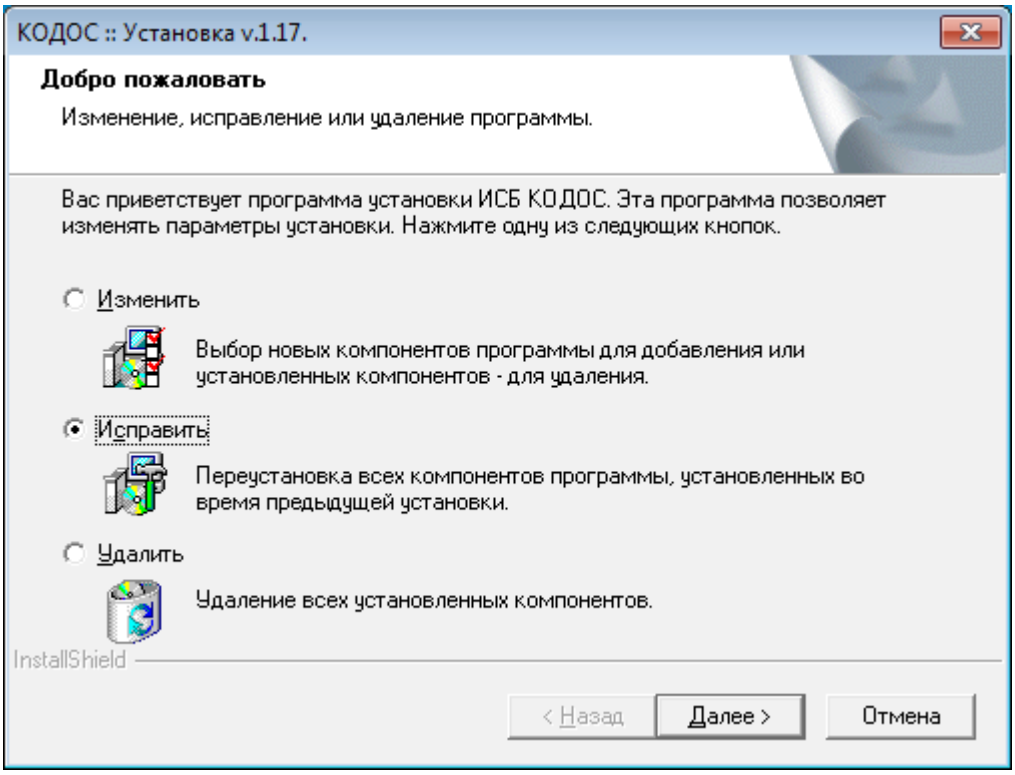



**Рисунок 2.7.1 – Окно «Обновления программы ИКБ КОДОС»**

3. В окне (рисунок 2.7.1) необходимо выбрать «Исправить». Обновление произойдет автоматически.

4. После окончания работы мастера установки необходимо запустить программу настройки системы («Конфигуратор»). При появлении предупреждения необходимо нажать «Да» для конвертирования базы данных на новый формат.

# 3 НАСТРОЙКА С ПОМОЩЬЮ ПРОГРАММЫ «КОНФИГУРАТОР»

Программа настройки систем «КОДОС» (Конфигуратор) предназначена для составления конфигурации подключенного оборудования «ИКБ КОДОС» и логической привязки этого оборудования к планам помещений.

Конфигуратор выполняет подготовительную работу и настройку перед запуском управляющих программ «ИКБ КОДОС», например, программы «Сервер ИКБ», «КОДОС-ОПС». Рекомендуется конфигурировать систему на том ПК, где планируется размещать сервер ИКБ.

**ВНИМАНИЕ!** Начиная с версии 1.16 не поддерживаются старые устройства (СК-А, СК-ЕС, Пульт А10, ЕС501, АБ А05), выпуск которых прекращен.

Подробнее о настройке системы смотрите в «РЭ ПО Конфигуратор»

# 4 НАСТРОЙКА В ПРОГРАММЕ «СЕРВЕР ИКБ»

## 4.1 Настройка списка операторов

**ВНИМАНИЕ!** Запуск ПО «сервер ИКБ КОДОС» производится с того ПК, на котором конфигурировалась система.

1. Запустить сервер «ИКБ КОДОС»
2. Нажать кнопку «Операторы» (рисунок 4.1.1).

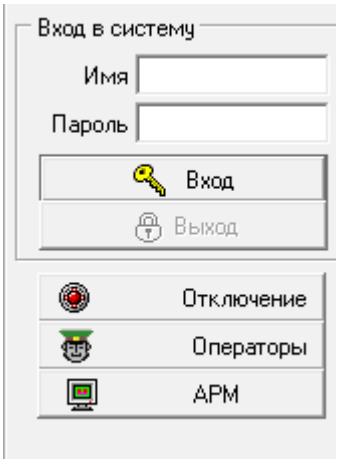



**Рисунок 4.1.1**

3. Ввести пароль администратора. По умолчанию «power» (рисунок 4.1.2)

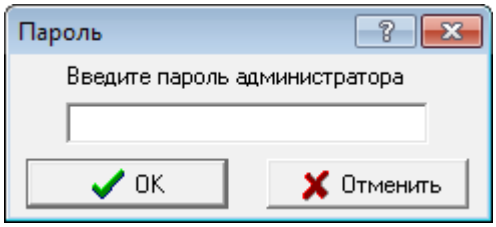



**Рисунок 4.1.2**

Откроется окно «Список операторов системы» (рисунок 4.1.3)

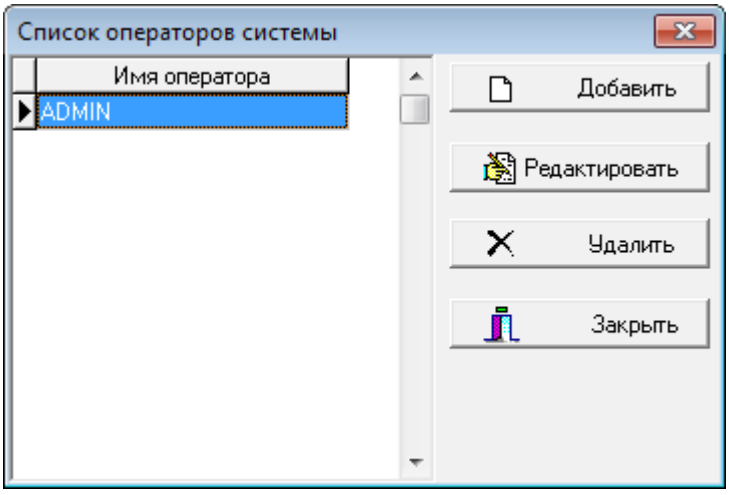



**Рисунок 4.1.3**

Кнопка «Добавить» – позволяет добавить нового оператора (рисунок 4.1.4) и выставить ему необходимые права доступа по управлению системой. Права доступа можно выставлять как группами, например «Права, связанные с видео», так и отдельно по каждому типу (например, «Снятие датчика с охраны»).

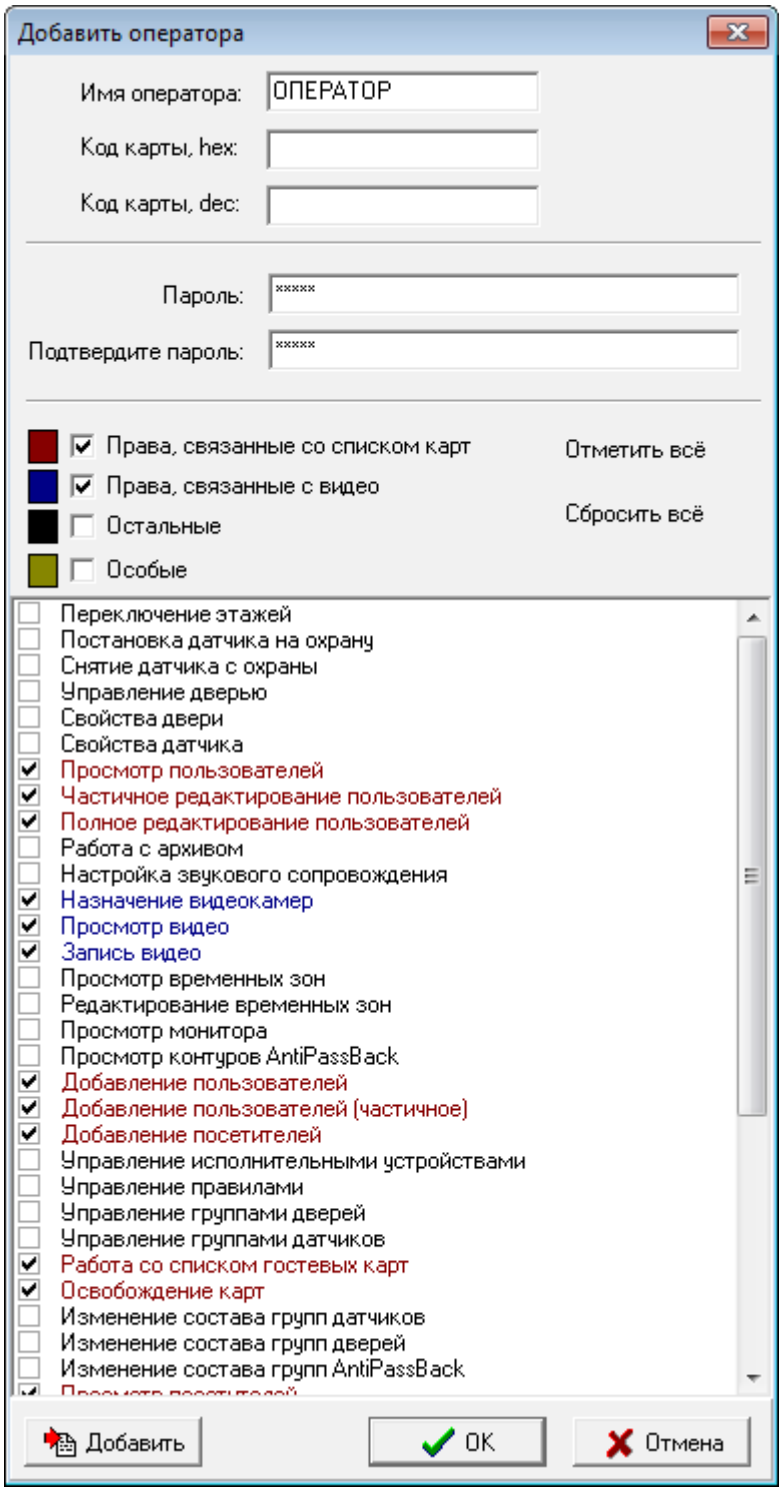



**Рисунок 4.1.4**

Кнопка «Редактировать» – позволяет отредактировать права у выбранного оператора

Кнопка «Удалить» – позволяет удалить выбранного оператора.

## 4.2 Настройка временных зон

Для настройки временных зон нажать кнопку 

.

1. В строке «Описание» (рисунок 4.2.1) ввести название временной зоны, либо оставить по умолчанию.

2. Задать временные интервалы в строках «Начало» и «Окончание» (шаг - 10 минут).

3. Установить дни действия временных интервалов флажками напротив дней недели и праздничных дней (Пр.), в которые действует данная временная зона.

4. Установить флажок «Поддержка временных зон для доступа» если требуется включить поддержку временных зон для контроля доступа, независимо от других установленных параметров, относящихся к временным зонам. В программе «Администратор ИКБ» данная функция недоступна.

5. Установить флажок «Поддержка временных зон для датчиков» если требуется включить автоматическую постановку/снятие датчиков по временным зонам, независимо от других установленных параметров, относящихся к временным зонам. В программе «Администратор ИКБ» данная функция недоступна.

6. Сохранить сделанные изменения.

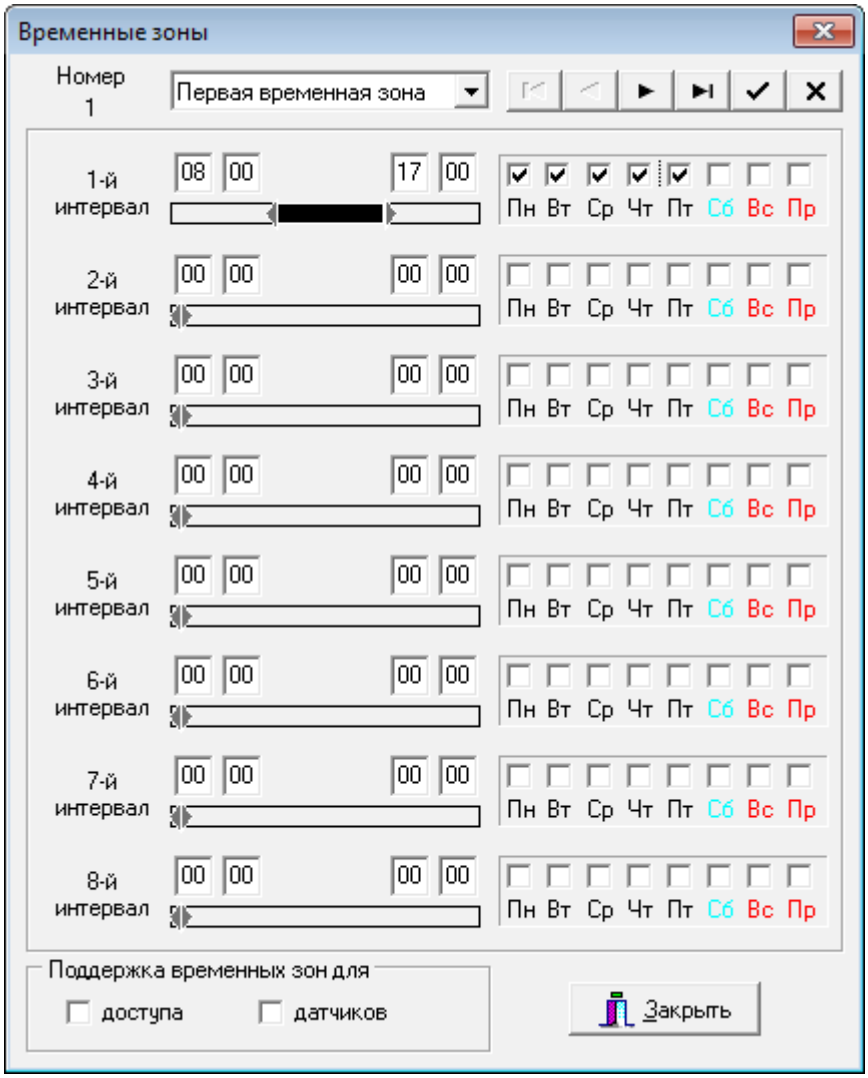



**Рисунок 4.2.1**

## 4.3 Настройка праздников

Для настройки праздничных дней нажать кнопку Праздничные дни (рисунок 4.3.1).

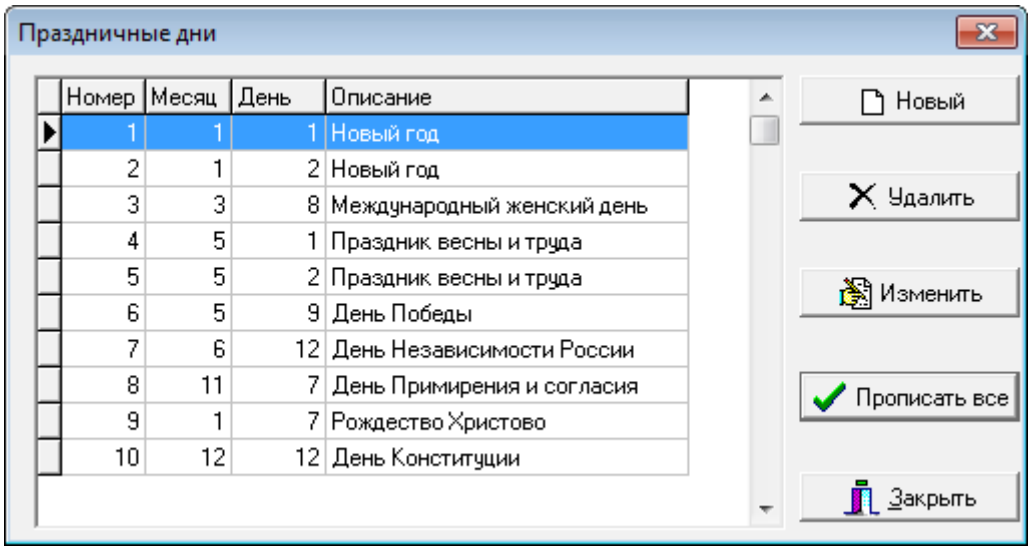



**Рисунок 4.3.1**

Кнопка «Новый» предназначена для добавления нового праздника к имеющимся по умолчанию (рисунок 4.3.2).

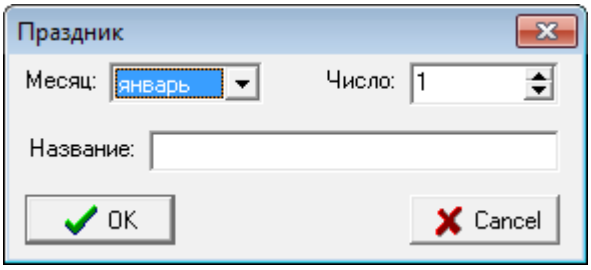



**Рисунок 4.3.2**

Кнопка «Удалить» удаляет выделенный праздник из списка

Кнопка «Изменить» позволяет редактировать имеющийся по умолчанию список государственных праздников (рисунок 4.3.3).

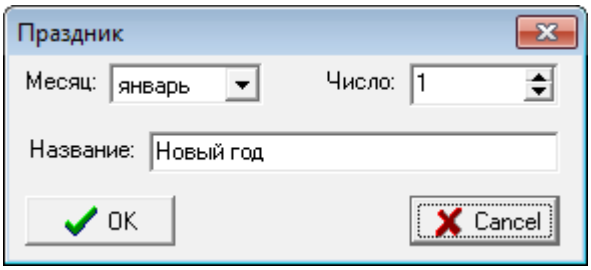



**Рисунок 4.3.3**

Кнопка «Прописать все» предназначена для ввода изменений в контроллеры, с которыми в настоящее время имеется связь.

После проведения любых изменений в списке нажать кнопку «Прописать все».

Будьте внимательны, если праздничный день попадает на будний день или выходной, то доступ определяется по настройкам доступа в праздничный день.

## 4.4 Настройка групп датчиков

Для удобства управления, при большом количестве датчиков, отдельные датчики можно объединять в группы. В качестве датчика может выступать датчики, подключенные к адресным блокам (А-06/2, А-06/8, А-07/4, А-07/8, А-09), а также датчики прохода и кнопки выхода контроллеров доступа.

Для создания групп датчиков нажать 

. «Группы датчиков» на сервере ИКБ или кнопку «Настройка групп датчиков» в программе «Конфигуратор» (рисунок 4.4.1).

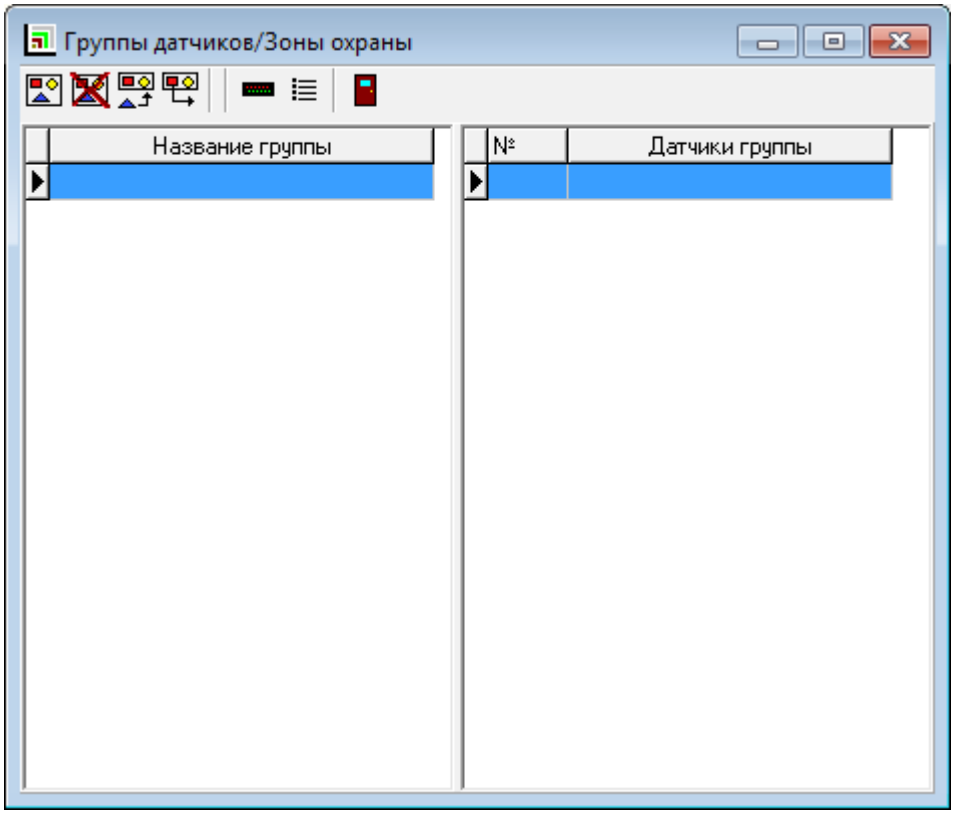



**Рисунок 4.4.1**

7. В окне «Группы датчиков/зоны охраны» (рисунок 4.4.1) нажать кнопку «Новая группа»  .

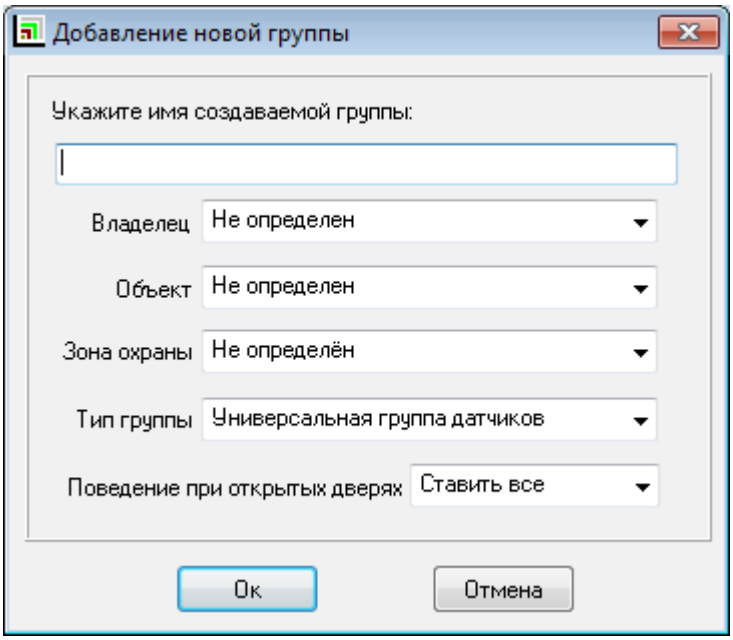



**Рисунок 4.4.2 – Создание группы датчиков**

8. В поле «Владелец» указывается признак организации, кто будет иметь право работы с данной группой датчиков.

ПРИМЕЧАНИЕ – Если модуль «Владельцы» не установлен, то данный параметр носит информативный характер, и не влияет на права доступа операторов..

9. В поле «Объект» указывается территориальная принадлежность данной группы (рисунок4.4.2).

10.В поле «Зона охраны» производится «привязка» зоны охраны к данной группе датчиков. В этом случае на планах данная группа датчиков будет иметь графическое отображение.

ПРИМЕЧАНИЕ –.Группа датчиков может не иметь привязки к зонам охраны..

11.Поле «Тип группы» принимает следующие значения:

- «Зона охранной сигнализации». Данная зона не может содержать пожарные датчики.
- «Зона тревожной сигнализации» Данная зона не может содержать пожарные датчики.
- «Зона пожарной сигнализации». Не может содержать иные датчики, кроме пожарных. Для данного типа группы невозможно выполнение команд «постановка на охрану» и «снятие с охраны».
- «Универсальная группа датчиков». Не содержит ограничений по типам датчиков.
- «Технологическая группа датчиков». Не содержит ограничений по типам датчиков. Данная группа не отображается в списке зон (групп) на вкладке «Охрана». Предназначена для создания групп датчиков, которые не предназначены для контроля состояния (норма-тревога-охрана…) оператором, но при этом позволяют создавать правила.

ПРИМЕЧАНИЕ –.Данные типы датчиков используются при конфигурировании панели А-16.

12.Нажать кнопку  «Добавить в группу» и выбрать датчики для этой группы. Нажать «ОК». Новая группа добавлена.

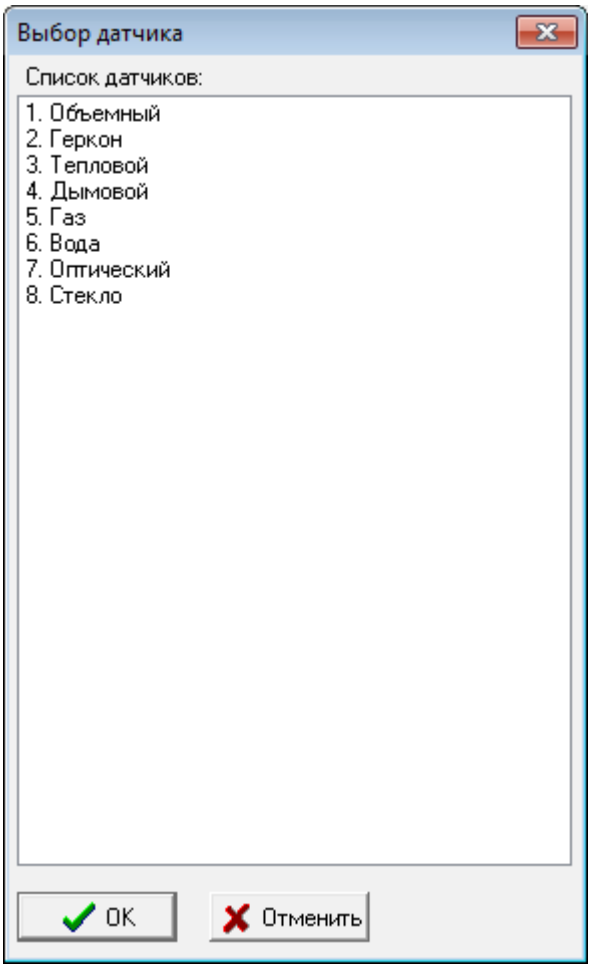



**Рисунок 4.4.3 – Создание группы датчиков**

13.Для одновременного выбора нескольких датчиков необходимо использовать кнопки «Ctrl», и «Shift»

14.Для настройки индикации выбрать группу и нажать  - «Индикация».

15.В окне «Настройка индикации для группы «Имя группы» (рисунок 4.4.4) выбрать состояния датчиков в группе и устройство индикации.

16.Нажать кнопку «Управлять» и в появившемся окне выбрать устройство индикации.

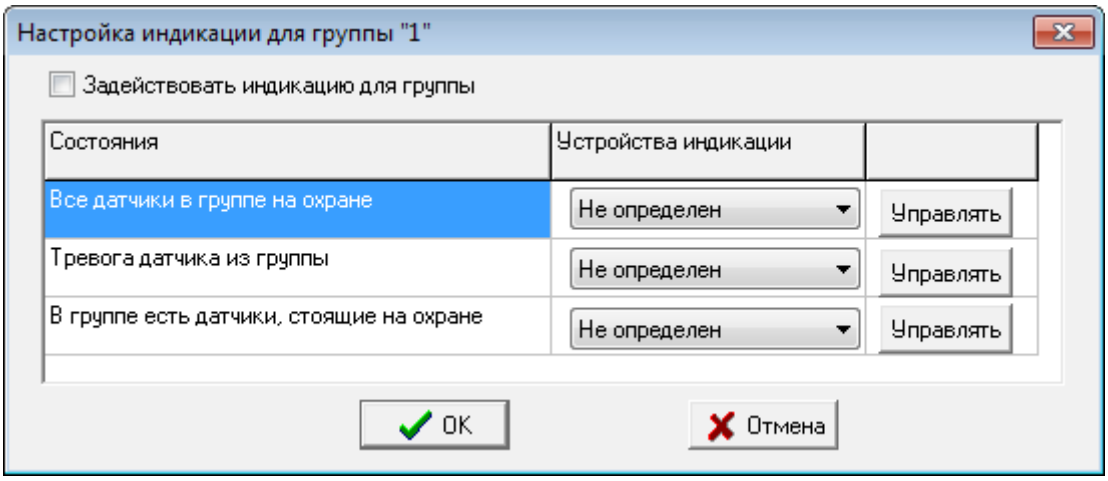



**Рисунок 4.4.4**

## 4.5 Настройка групп дверей

Для удобства управления, при большом количестве дверей, отдельные двери можно объединять в группы.

**Создание групп дверей**

1. Нажать кнопку «Группы дверей» на вкладке «Управление».

2. В окне «Группы дверей» (рисунок 4.5.1) нажать кнопку  «Новая группа» и ввести название новой группы дверей.

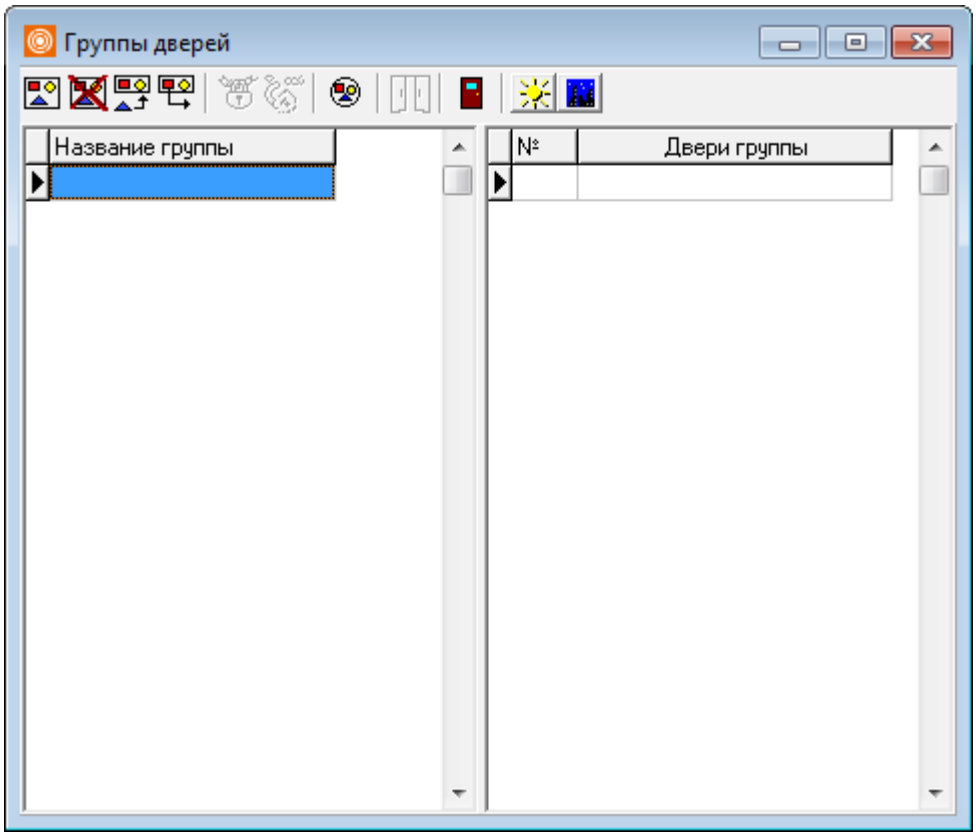



**Рисунок 4.5.1**

3. В поле «Владелец» (рисунок 4.5.2) выбирается необходимое имя владельца, указывающего принадлежность данной группы к определенной категории доступа. Для операторов, не имеющих право работать с данным владельцев, группа отображаться не будет.

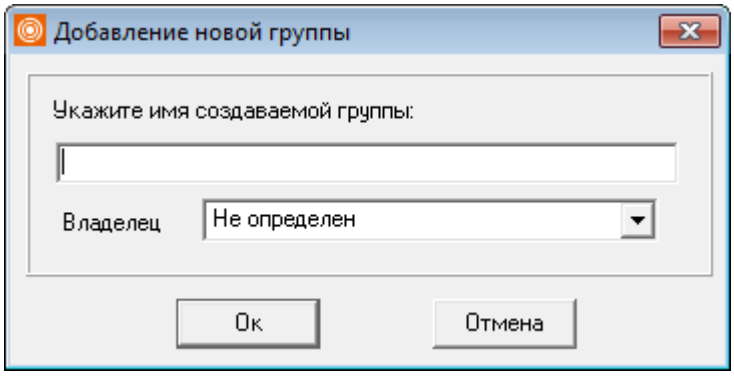



**Рисунок 4.5.2**

4. В поле «Тип группы» производится выбор из значений:

- «стандартный» –
- «проход с подтверждением»

5. Нажать  и выбрать двери для этой группы. Нажать «ОК». Новая группа добавлена.

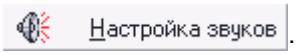
**Постановка группы дверей на охрану.**

1. Нажать «Группы дверей» и в открывшемся окне «Группы дверей» нажать кнопку  .
2. Для снятия с охраны нажать кнопку  .

## 4.6 Настройка звуков

В программе предусмотрена привязка звуковых файлов к системным событиям. Это необходимо для привлечения внимания оператора к работе системы.

Для настройки звуков:

1. Нажать 

.

2. В окне «Звуковое сопровождение событий» (рисунок 4.6.1) выбрать событие для редактирования.

3. Прослушать звук с помощью кнопок в подразделе «Тестирование звукового файла».

4. Назначить стандартный WAV файл - «Установить стандартное звуковое сопровождение» или WAV файл по выбору - «Установить новое звуковое сопровождение» и выбрать файл.

5. Если необходимо, создать новый файл в панели «Создание нового звукового сообщения»:

- Установить флажок «Режим дозаписи к файлу» и нажать «Запись».
- Продиктовать новое сообщение в микрофон и нажать кнопку «Останов записи».
- Сохранить - кнопка «Сохранение в файл», в формат WAV.

6. Если необходимо отключить звуковое сопровождение выбранного события, то надо нажать «Отключить звуковое сопровождение»

Кнопка «Очистка» удаляет временный звуковой файл.

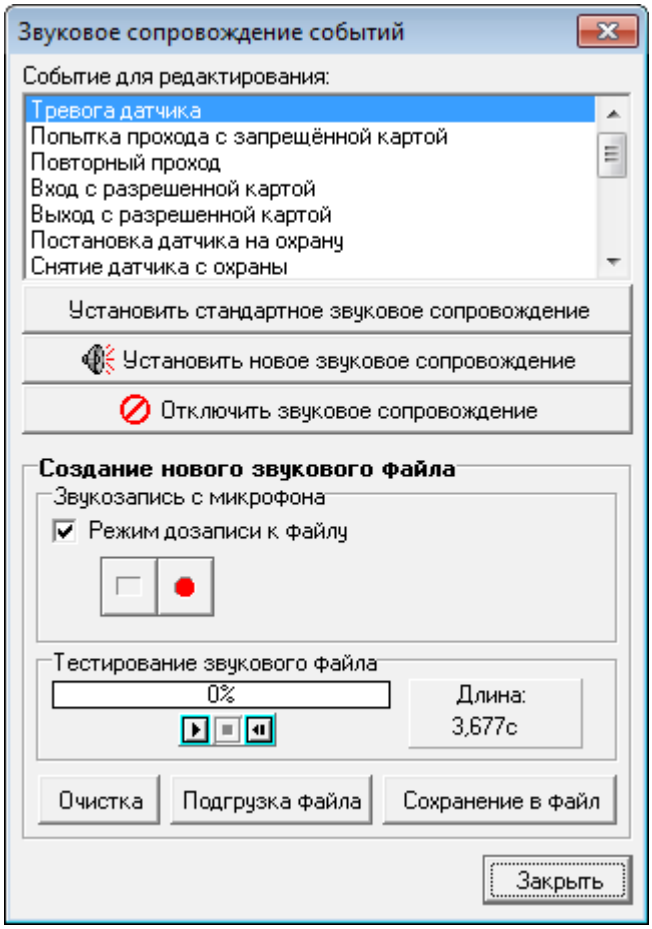



**Рисунок 4.6.1**

## 4.7 Настройка правил

В «ИКБ КОДОС» существует возможность программировать автоматическую реакцию программы на выполнение определенных действий при наступлении каких либо событий. Это достигается путем создания определенных правил.

Вызов окна настроек производится кнопкой Правила (рисунок 4.7.1)

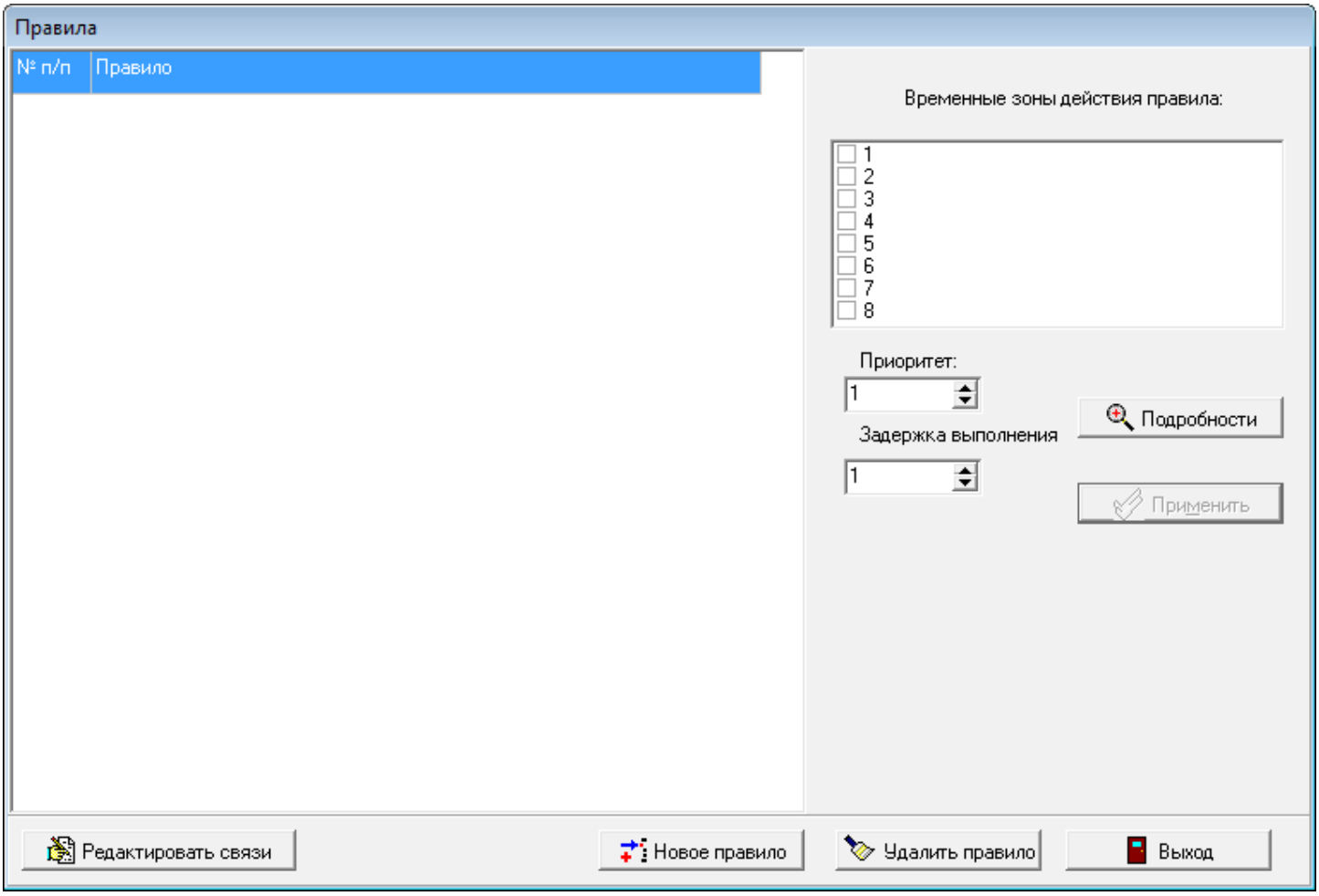



**Рисунок 4.7.1**

Кнопка Редактировать связи предоставляет возможность пользователю задать соответствие происходящим событиям в системе определенных действий. Списки событий и действий определены заранее и представлены в окне Задание связей между событиями и действиями (рисунок 4.7.2).

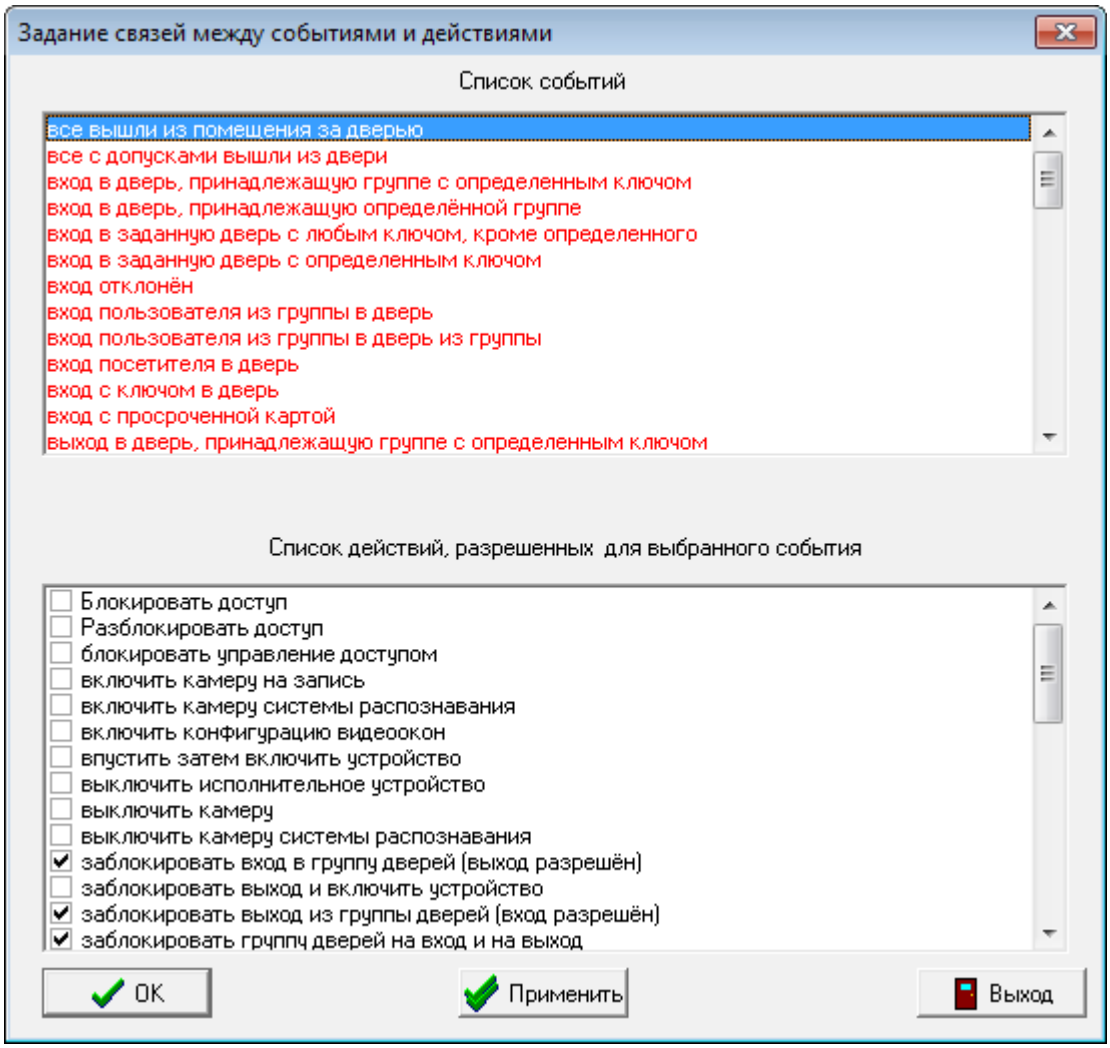



**Рисунок 4.7.2**

Одному событию можно ставить в соответствие несколько действий. Запоминание связей событий и действий осуществляется при нажатии кнопки Применить.

Заданная таким образом связь между событием и действиями является «шаблоном» для правил, который в дальнейшем можно использовать несколько раз для различных объектов при создании правила.

Создание правил осуществляется при нажатии кнопки Новое правило (рисунок 4.7.3). При этом открывается окно Доступные правила (рисунок 4.7.3). Выделив событие из списка в левой части окна, в правой части отобразятся действия, определенные при задании связей.

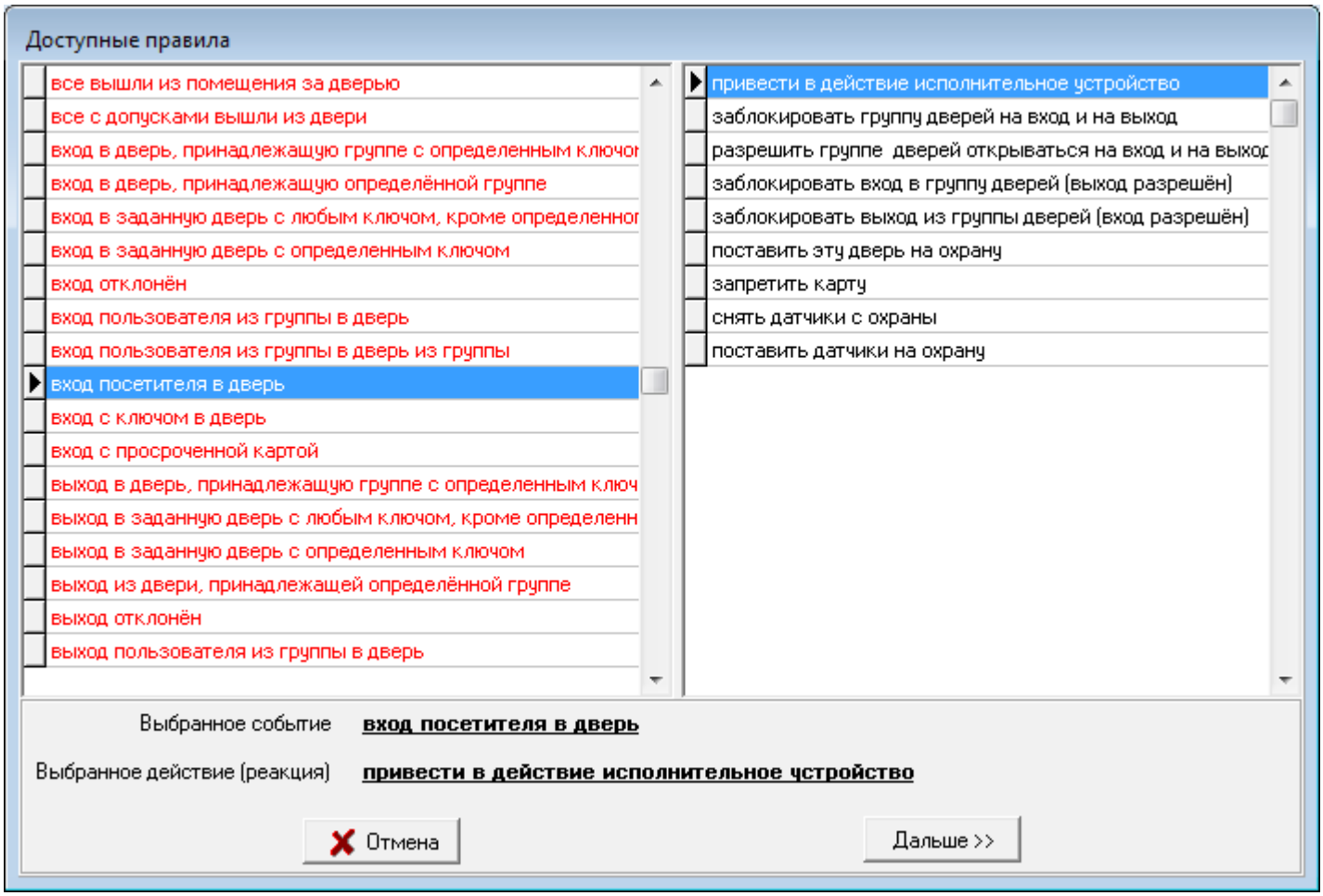



**Рисунок 4.7.3**

Выбранные событие и действие отображаются внизу окна.

Нажать кнопку Дальше >>. В окне Настройка параметров событий и действий (рисунок 4.7.4) для правила запрашиваются вспомогательные параметры его выполнения.

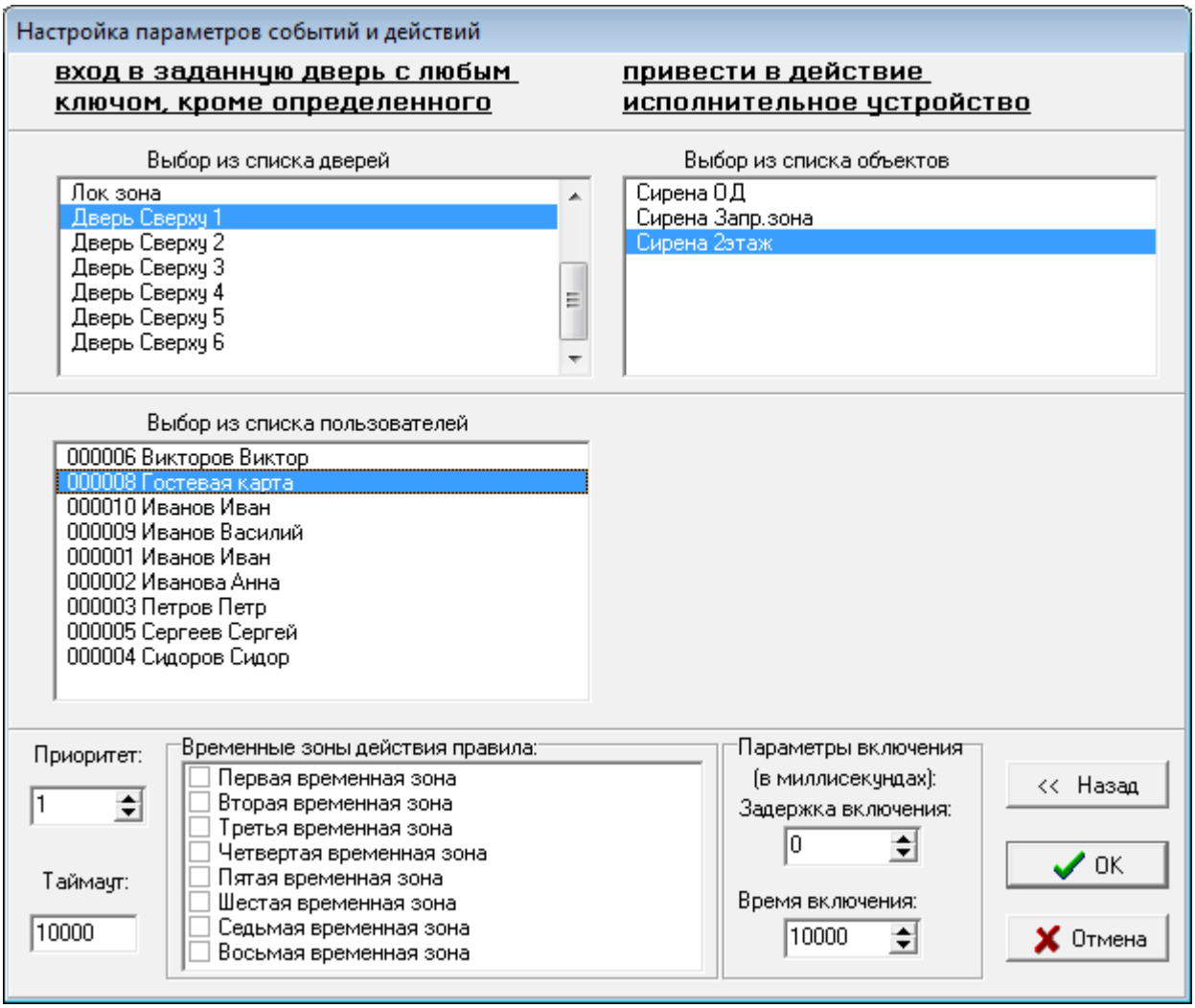



**Рисунок 4.7.4**

Внешний вид окна зависит от типа создаваемого правила и позволяет выбрать конкретный объект, пользователя или группу объектов или датчиков. При выборе списка групп будет открыто дополнительно информационное окно с составом данной группы.

Установкой флагов в панели Временные зоны действия правила: (см. рисунок 4.7.5) можно обозначить временные зоны, для которых создаваемое правило будет действовать. Если требуется, чтобы правило действовало все время, следует сбросить все флаги.

Создаваемому правилу может быть присвоен приоритет, определяющий очередность выполнения этого правила. При работе Системы в первую очередь выполняются те правила, номер приоритета которых меньше. Для создаваемого правила приоритет задается путем ввода числа от 1 до 16 в поле с пошаговым изменением значения Приоритет.

С помощью поля ввода Таймаут может быть задана величина интервала задержки (в миллисекундах) перед выполнением создаваемого правила. В этом случае действие, определяемое правилом, будет выполняться спустя заданный интервал от момента возникновения события. Если задержка не нужна, следует установить в этом поле значение 0.

Группа полей ввода Параметры включения с пошаговым изменением значения позволяет установить параметры срабатывания устройств.

В поле Задержка включения следует установить время (в миллисекундах), которое пройдет, прежде чем устройство сработает.

В поле Время включения устанавливается интервал времени (в миллисекундах), в течение которого устройство будет работать.

После того, как все необходимые настройки будут выполнены, необходимо сохранить правило в базе данных. Для этого следует нажать кнопку ОК, расположенную в правом нижнем углу окна. В случае успешного сохранения правила будет выдано соответствующее сообщение (см. рисунок 4.7.5.):

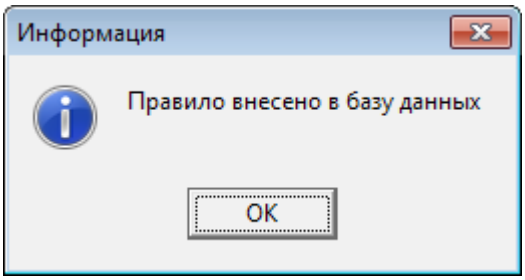



**Рисунок 4.7.5**

Выполнение созданных правил происходит автоматически, под управлением программного обеспечения, и не требует дополнительных действий со стороны оператора.

Существует возможность определить период времени, в течение которого программа будет реагировать на произошедшее событие. Если разница во времени между совершенным событием и его приходом на сервер ИКБ превысит установленное значение, то правило выполнено не будет. Это удобно применять, когда выполнение правил нецелесообразно. Например, при подключении к объекту (ППКОП А-20, контроллер ПРО, контроллеры доступа), с которым временно отсутствовала связь, и который определенное время работал в автономном режиме. В этом случае при восстановлении связи происходит «слив событий», быстрая передача на сервер ИКБ всех накопленных событий, большинство из которых уже потеряла свою актуальность.

Настройка времени выполнения правил производится в файле codos.ini. Для этого в разделе [Config] установите значение параметра MaxEventTime. Значение выставляется в секундах, причем оно должно быть кратно 60 (при выставлении некратного значения оно округляется в меньшую сторону).

Например, MaxEventTime= 600

Пример создания правила приведен в Приложении В

## 4.8 Настройка видеозаписи

В программе предусмотрена возможность производить видеозапись при наступлении какого либо события в системе.

Вызов окна настроек производится при нажатии кнопки «Видеозапись» (рисунок 4.8.1)

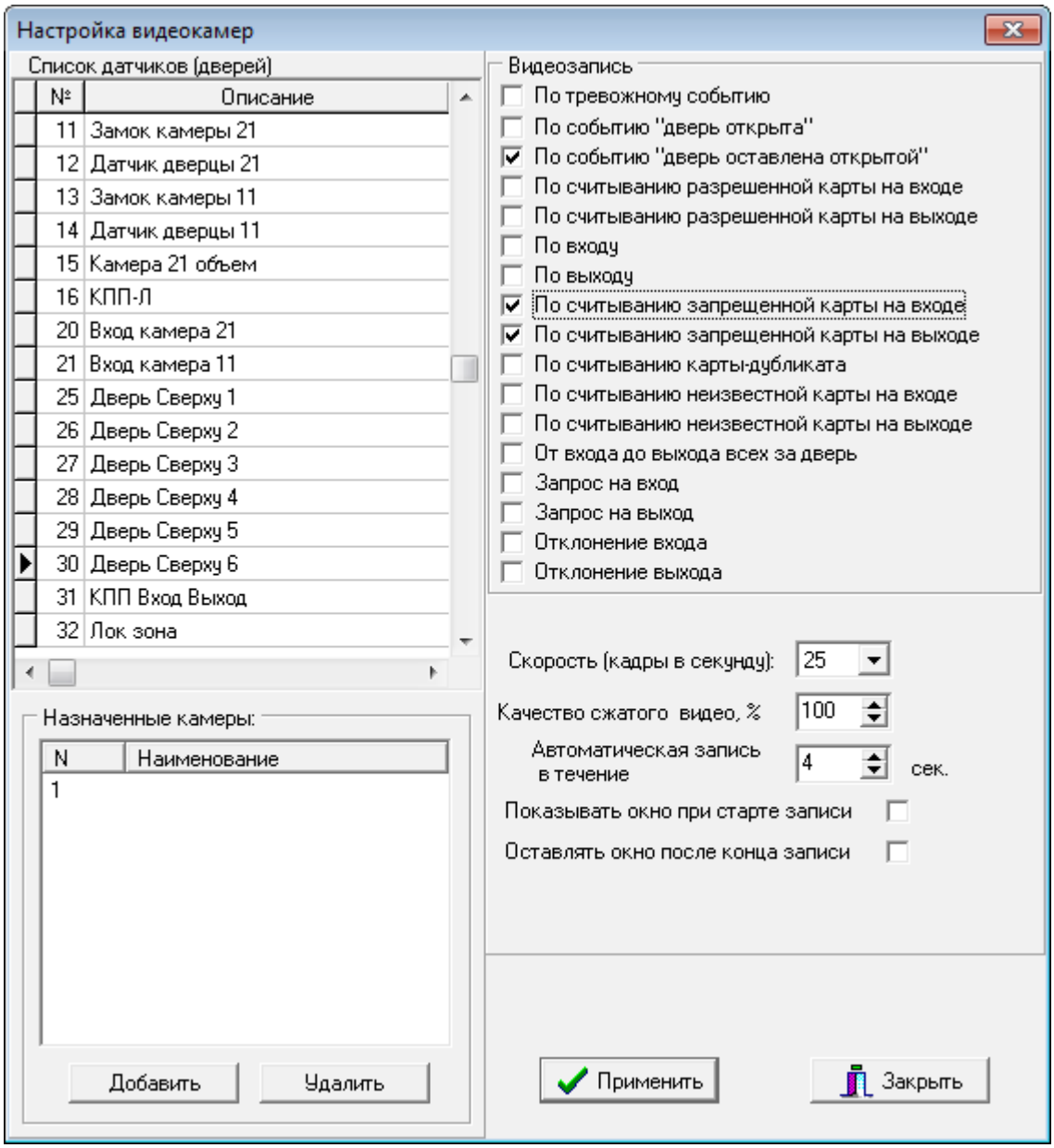



**Рисунок 4.8.1**

В списке датчиков(дверей) представлены все устройства, имеющиеся в системе, и по событиям от которых может производиться видеозапись.

В панели видеозапись представлены события, которые могут приходить от выбранного датчика. Список событий меняется, в зависимости от выбранного датчика.

Список имеющихся камер представлен в раскрывающемся списке Назначена камера. К одному датчику можно «привязать» не более одной камеры. К одной камере можно «привязать» несколько событий.

Выбор параметров записи Скорость, Качество сжатия, Автоматическая запись в течение выставляется исходя из необходимости.

При выставлении значения Показывать окно при старте записи, на экране будет появляться окно видеоизображения при наступлении события.

При выставлении значения Оставлять окно после конца записи окно видеоизображения останется на экране. В дальнейшем его можно будет закрыть вручную.

Окно Настройка видеокамер появляется так же и при выборе в контекстном меню значка камеры на планах помещений значения Назначение камеры

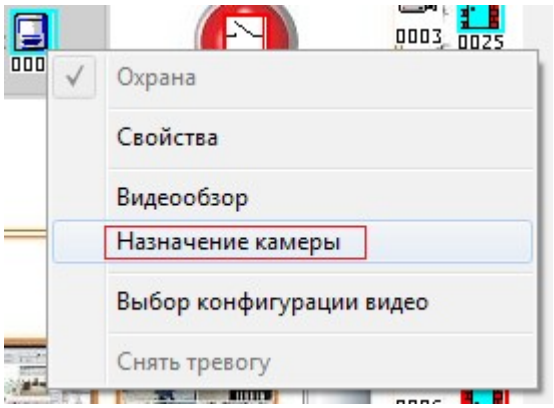



**Рисунок 4.8.2**

## 4.9 Настройка режима запрета повторного прохода

Режим запрета повторного прохода (далее ЗПП) запрещает пользователю пройти через и одну и ту же точку доступа (дверь, турникет) более одного раза подряд в одном направлении. Для корректной работы данного режима необходима установка на всех точках доступа считывателей с двух сторон (на «вход» и на «выход»).

При проходе через дверь, на которой установлен считыватель, обязательно «отмечаться» на вход и на выход. Фактором прохода будет считаться поднесение ключа к считывателю и открытие двери. (Если дверь уже открыта, достаточно поднести кодоноситель к считывателю, и факт прохода то же будет зафиксирован системой). В случае повторного прохода (например, отметились на «вход», а при «выходе» не отметились и снова пытаетесь войти на «входе») проход будет заблокирован, и считыватель будет мигать поочередно красно-зеленым светом, информируя о попытке повторного прохода.

Режим ЗПП может быть глобальным и локальным. При локальном ЗПП запрет повторного прохода контролируется только на одной точке доступа. Если необходимо контролировать повторный проход на нескольких точках доступа одновременно (например, большое помещение с несколькими дверями, этаж здания и т.п.), то необходимо настроить контур, и включить в него точки доступа, которые ограничивают в него проход. При этом не должно быть других способов попадания в данный контур, кроме как через эти точки доступа.

### 4.9.1 Настройка глобального ЗПП

Для настройки контуров нажать кнопку Контуры ЗПП.

1. В окне Настройка контуров контроля повторного прохода (рисунок 4.9.1) нажать  и ввести название нового контура.
2. Нажать  и выбрать двери, входящие в данный контур. Нажать ОК. Новая группа добавлена.

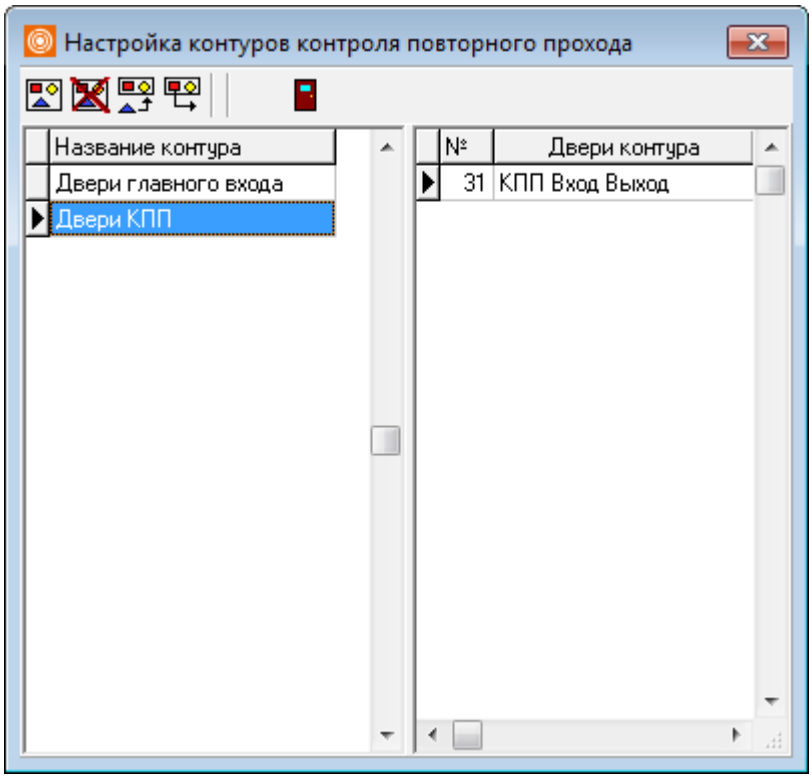



**Рисунок 4.9.1**

Кроме этого необходимо произвести настройку локального ЗПП на каждой двери, входящей в контур.

### 4.9.2 Настройка локального ЗПП

Выбрав дверь из списка и нажав кнопку «свойства» откроется окно «Настройка двери» (рисунок 4.9.2)

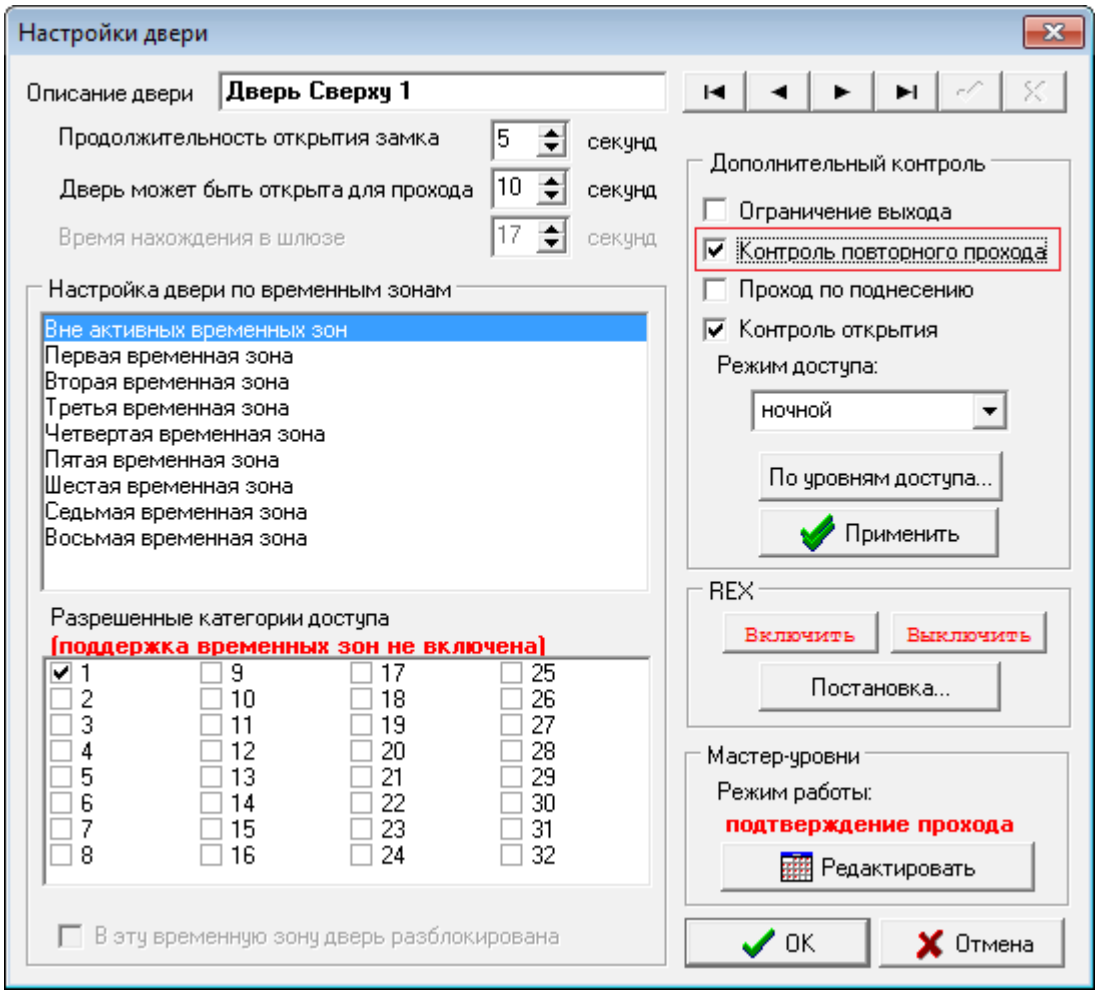



**Рисунок 4.9.2**

В настройках двери выставить флажок Контроль повторного прохода и, нажав на кнопку По уровням доступа, выбрать уровни доступа (рисунок 4.9.3), для которых будет действовать контроль повторного прохода.

Нажать на кнопку Применить для сохранения настроек.

ПРИМЕЧАНИЕ – В случае потери связи с контроллером доступа при работе глобального ЗПП, данная дверь автоматически перейдет в режим локального ЗПП.

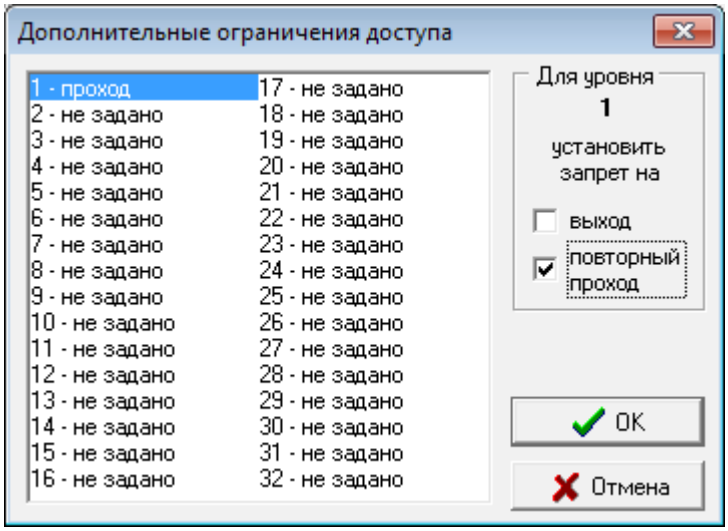



**Рисунок 4.9.3**

## 4.10 Настройка режима контроля оператора

Режим контроля оператора предназначен для периодического автоматического контроля присутствия оператора на рабочем месте.

При включении данного режима на экране мониторе через заданные промежутки времени появляется окно (рисунок 4.10.1), которое будет закрыто при правильной реакции оператора.

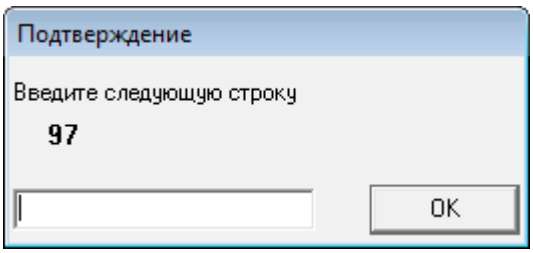



**Рисунок 4.10.1**

В случае игнорирования подтверждения со стороны оператора в архиве событий появится событие Обнаружено отсутствие оператора.

В случае ошибки ввода строки в архиве событий появится сообщение Подтверждение оператора с ошибкой.

При выборке данных из архива за определенный период по этим событиям можно судить о дисциплинированности и внимательности операторов.

Для настройки контроля оператора нажать кнопку Контроль оператора.

1. В открывшемся окне Настройка функции контроля оператора (рисунок 4.10.1) снять флажок Выключить контроль наличия оператора.
2. Установить Интервал и Задержку активизации функции контроля оператора.
3. Установить продолжительность Дневного режима и Ночного режима. Если диапазоны дневного и ночного режимов пересекаются, то будут действовать установки параметров имеющие наименьшие значения.

По умолчанию программа настроена так, что через заданный промежуток времени (по умолчанию 10 минут), при отсутствии каких либо действий со стороны оператора, она переходит в безоператорный режим.

Для отключения выхода в безоператорный режим необходимо снять флажок Отключить выход в безоператорный режим (рисунок 4.10.2).

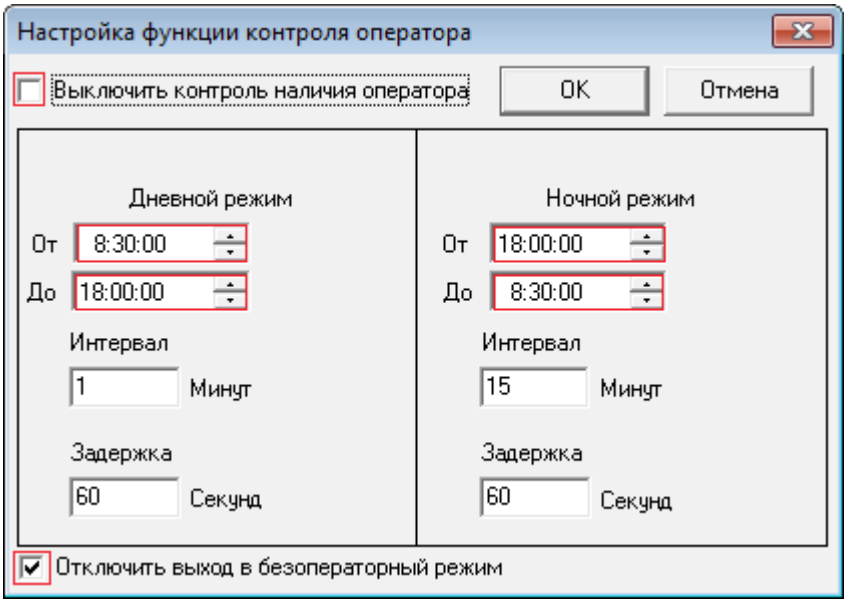
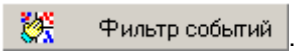



**Рисунок 4.10.2**

## 4.11 Настройка фильтра отображаемых событий

В программе имеется возможность скрывать определенные события, выводимые в списке «текущих событий» на вкладке «События в системе»

Чтобы настроить выводимые события нажать 

.

1. В появившемся окне «Настройка фильтра событий» (рисунок 4.11.1) выбрать «События в системе» либо флажками по группам, либо по одному, в отображении которых нет необходимости.

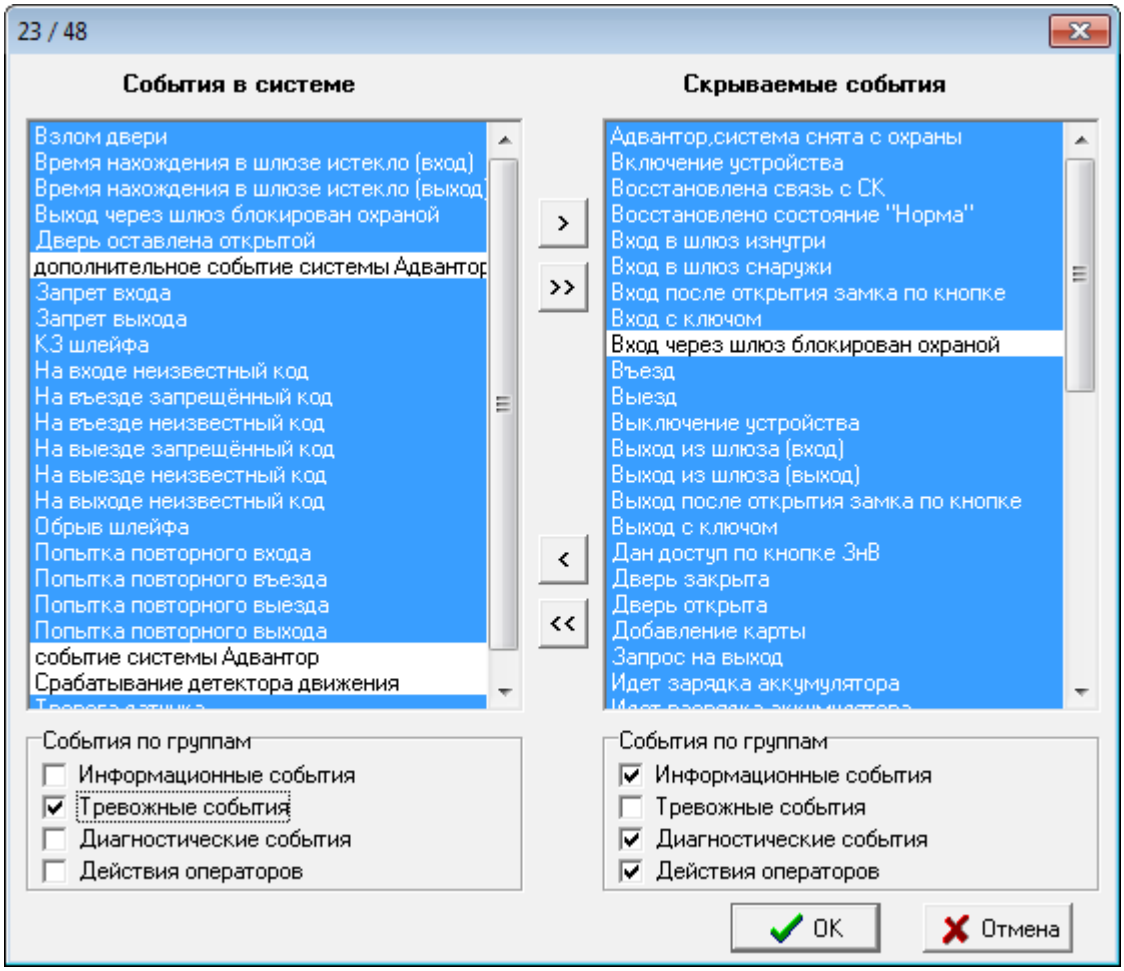



**Рисунок 4.11.1**

2. Нажать 

и перенести их в «Скрываемые события». Нажать «ОК». «Скрываемые события» не будут выводиться во вкладке «События в системе».

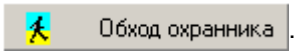
Для возврата событий в отображаемые, выделить «Скрываемые события» и нажать 

. События будут перенесены их в «События в системе».

## 4.12 Настройка функции контроля обхода охранника

Часто возникает необходимость кроме дистанционного контроля состояния объекта, производить обход (объезд) объекта в назначенное время. Для контроля выполнения этих действий предназначена функция «контроля обхода охранника». При совершении обхода маршрута в указанное время в списке событий появится сообщение «Обход охранника ЧЧ:ММ», с указанием места и времени отметки. В случае опоздания охранника к месту отметки появится сообщение «Охранник опоздал» с указанием места и назначенным временем отметки. Если опоздание превысило разрешенный интервал, то сформируется сообщение «Неявка охранника».

Для настройки функции «Обход охранника»

1. Нажать 

.

2. В окне «Настройка обходов охранника» (рисунок 4.12.1) названия и характеристики маршрутов обхода охранников можно установить двумя способами: Назначить новый маршрут - нажать , Скорректировать маршрут, выделенный курсором, - нажать в панели «Маршруты».

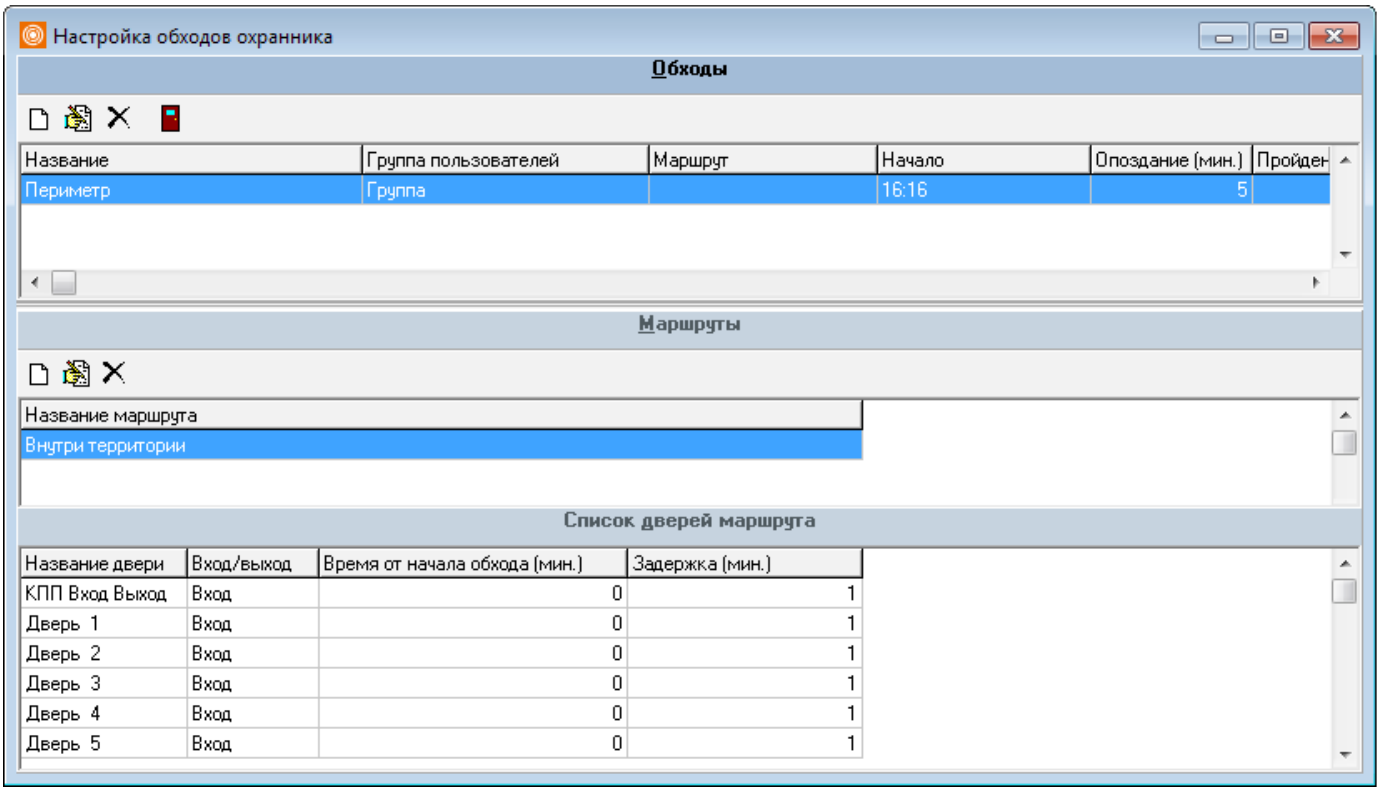



**Рисунок 4.12.1**

3. В окне «Настройка свойств маршрута» (рисунок 5.6.6) в строке «Маршрут» ввести название маршрута.

4. Выбрать контрольные точки для каждого маршрута из списка «Состав дверей маршрута».

5. Переключателем «Место отметки» определить, какой считыватель выбранной точки прохода использовать для контроля охранника на маршруте обхода.

6. Каждой выбранной контрольной точке, кроме первой, установить:

- «Допустимая погрешность, мин: » - промежуток времени, в течение которого охранник должен пройти через заданную точку прохода и отметиться.
- «Время от начала а, по прошествии которого охранник должен п

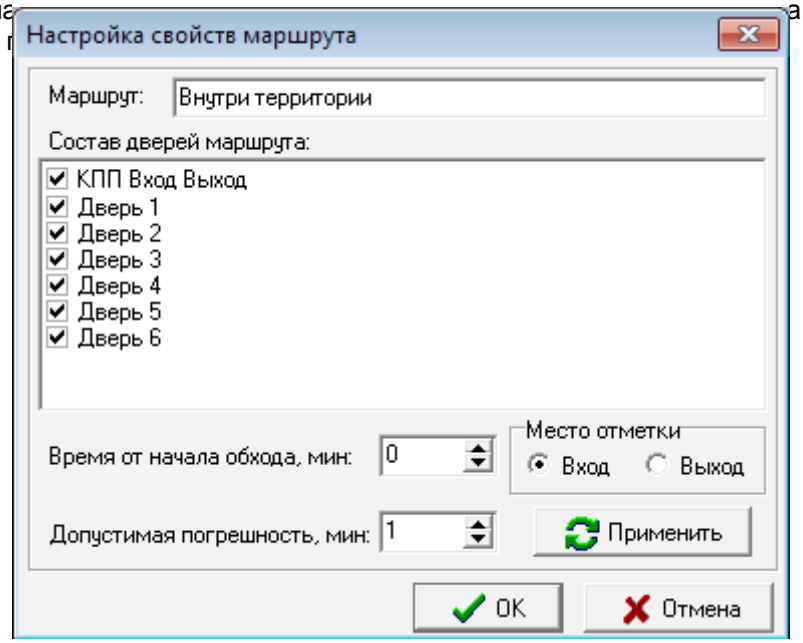



**Рисунок 4.12.2**

**ВНИМАНИЕ!**

1. В один маршрут нельзя дважды включить одну и ту же контрольную точку.
2. Считыватели на вход/выход одной точки прохода – рассматриваются как один считыватель.
3. В качестве контрольной точки может использоваться считыватель любой двери, в том числе и помещения, в которое охранник не имеет доступа. При выборе контрольных точек необходимо быть внимательным, во избежание недоразумений и ложных тревог.

7. Названия и характеристики обходов охранников можно установить двумя способами: Назначить новый обход - нажать , Скорректировать обход, выделенный курсором, - нажать в панели Обходы.
8. Периодичность обходов назначить в окне Настройка свойств обхода охранника (рисунок 4.12.3).
9. В строке Обход ввести номер или название очередного обхода.
10. В поле Назначенная группа: выбрать группу пользователей, из состава которого назначается лицо, совершающее обход.
11. В поле Время начала обхода: установить время начала обхода по одному из маршрутов, который был сформирован в начале работы с функцией. Выбор маршрута осуществляется в поле Маршрут:. Учитывая, что маршруты устанавливаются с учетом ряда ограничений, в один обход могут быть включены несколько маршрутов.

**ВНИМАНИЕ!** Во избежание конфликтов данных и появления ложных тревог следует внимательно отнестись к назначению времени начала обходов.

Условия обхода задаются флажками Соблюдать порядок дверей и Обходит начавший обход. В первом поле устанавливается порядок обхода контрольных точек. Во втором – определяется допустимость выполнения запланированных обходов разными охранниками.

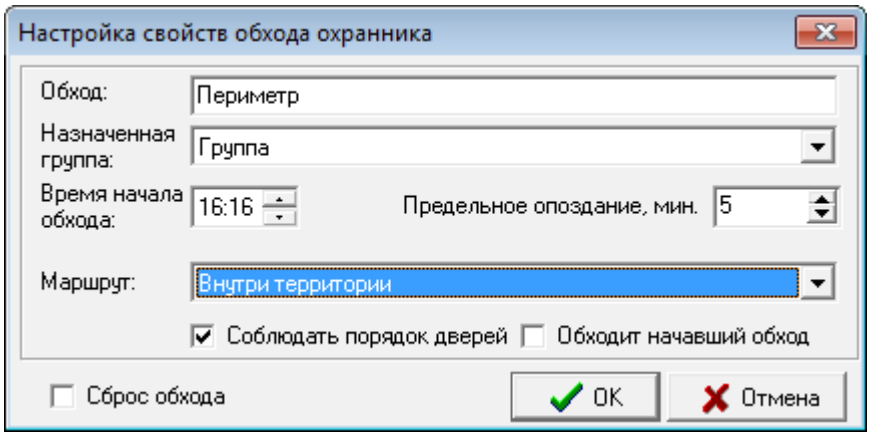



**Рисунок 4.12.3**

## 4.13 Настройка свойств двери

Прежде чем начинать эксплуатировать систему контроля доступом необходимо произвести настройку всех точек доступа (дверей, турникетов, шлагбаумов и т.д.).

Для этого необходимо открыть окно «Настройки двери» (рисунок 4.13.1). Это можно сделать двумя способами: выбрать нужную дверь из списка на вкладке «Управление» и нажать кнопку «Свойства» или двойным щелчком по описанию двери.

Установить значения «Продолжительность открытия замка» – время, в течение которого замок остается открытым. Если в течение этого времени происходит срабатывание датчика контроля прохода, то замок блокируется. Изменяется в диапазоне от 1 до 30 секунд.

Параметр «Дверь может быть открыта для прохода».определяет интервал времени, по истечении которого формируется сообщение «Дверь оставлена открытой», если после совершения прохода обнаружено что «дверь открыта». Изменяется в диапазоне от 1 до 30 секунд.

При установке параметра «Проход по поднесению» фиксация прохода пользователю будет производиться по факту поднесения карты к считывателю. При этом дополнительное действие по открытию двери (срабатыванию датчика прохода) необязательно. Данный режим используется при оборудовании мест учета рабочего времени, без монтажа оборудования СКУД (дверей, замков, герконов).

Настройка доступа по временным зонам производится отдельно для каждой временной зоны указанием тех уровней доступа, которым разрешен доступ.

Если в текущее время ни одна временная зона не активна, то применяются настройки «Вне активных временных зон».

Для разблокировки отдельной двери в конкретный временной интервал применяется параметр «В эту временную зону дверь разблокирована».

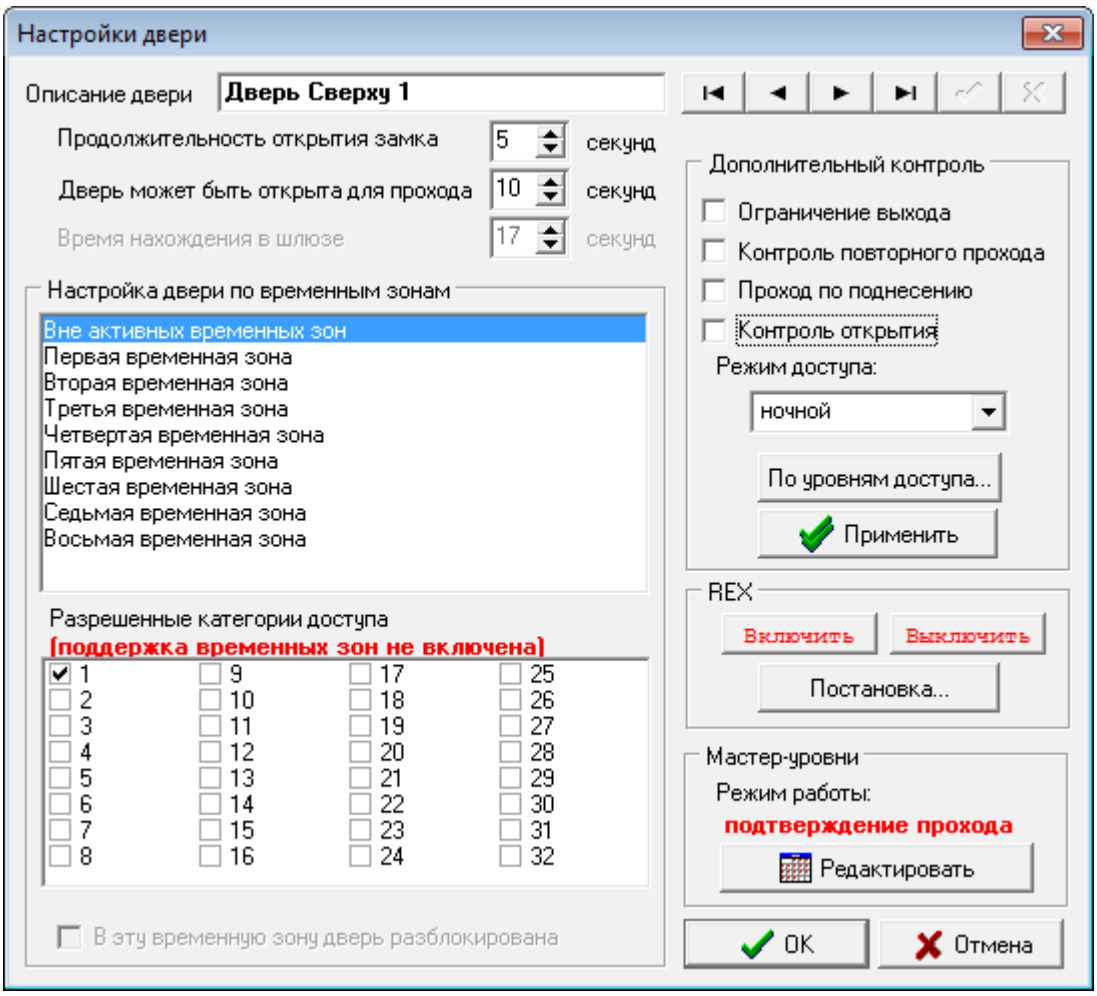



**Рисунок 4.13.1**

С помощью параметра «Ограничение выхода» возможно настроить запрет на выход определенных категорий пользователей, определенных в указанных группах «По уровням доступа» (рисунок 4.13.2)

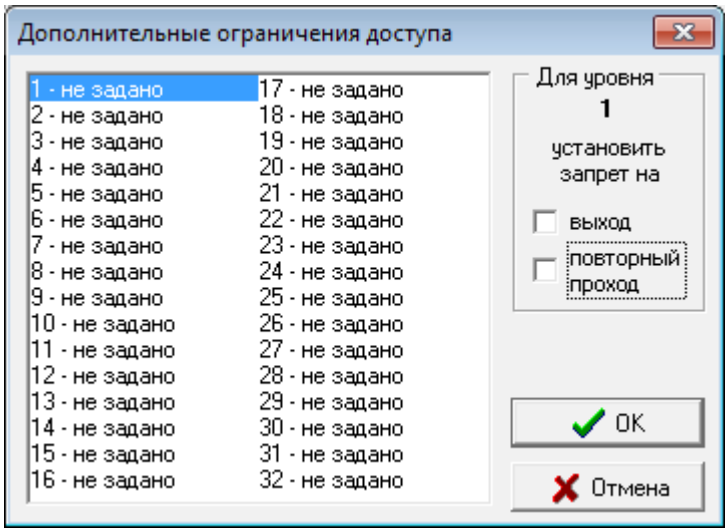



**Рисунок 4.13.2**

Параметр «Контроль повторного прохода» включает режим локального ЗПП для указанных групп доступа.

Кнопки «Включить» или «Выключить» кнопку REX соответственно разрешают или запрещают использовать кнопку, подключенную к входу 2 (входу 2 и 4 для контроллеров, сконфигурированных как двухдверные) для открытия двери.

### 4.13.1 Особенности настройки контроллера шлюза

Настройка контроллера шлюза осуществляется аналогично контроллеру двери. Кроме этого в окне Настройка двери становится активным параметр Время нахождения в шлюзе.

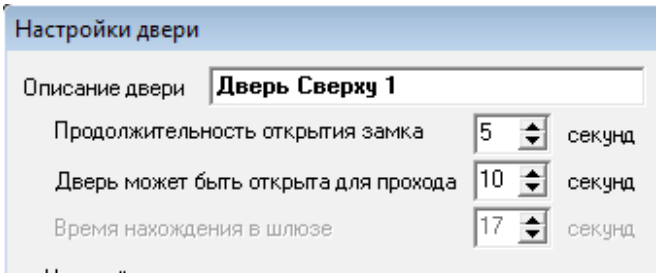



**Рисунок 4.13.3**

Время нахождения в шлюзе устанавливает максимальное время, в течение которого должна быть закончена процедура прохода через шлюз. В течение этого времени происходит блокировка считывателей дверей, и вход в шлюз с обеих сторон запрещен. Логика работы данной конфигурации реализована на аппаратном уровне и заключается в следующем: при прохождении на охраняемый объект владелец электронной карты, идентифицировав себя поднесением ее к входному считывателю, заходит внутрь шлюза и закрывает за собой дверь. В этот момент работа считывателей обеих дверей на определенное время (Время нахождения в шлюзе) блокируется контроллером. В этот момент считывание карты другого пользователя (как со стороны входа, так и со стороны выхода) и, соответственно, проход пользователя в шлюз невозможны;

После того как владелец электронной карты зашел в шлюз, обязательным условием дальнейшего прохода является закрытие за собой входной двери. До тех пор, пока входная дверь остается открытой, кнопка REX выходной двери заблокирована, проход на объект невозможен. Считыватель с внешней стороны выходной двери в этот момент также заблокирован.

Затем, после выполнения вошедшим (либо сотрудником службы безопасности), каких-либо дополнительных процедур, предусмотренных режимом охраны объекта, сотрудник службы безопасности, в зависимости от принятого решения, нажимает одну из кнопок открытия двери (REX):

- либо кнопку открытия второй двери для дальнейшего прохода владельца электронной карты;
- либо кнопку первой двери – для того, чтобы вошедший покинул шлюз, не заходя на охраняемый объект;

После прохода владельца карты через шлюз и закрытия выходной двери (либо входной двери при запрещении доступа на объект и выходе в обратном направлении) блокировка считывателей снимается и становится возможной идентификация кода электронной карты следующего проходящего через шлюз.

При выходе владельца электронной карты с охраняемого объекта алгоритм прохода через шлюз аналогичен вышеприведенному.

Так же возможна и программная реализация шлюза. Данная конфигурация строится на контроллерах доступа (EC-202, EC-502) и основана на реализации правил (см.п. 4.7 ).

Для этого необходимо:

1. создать группу дверей (туда должны войти 2 или более дверей шлюза);
2. создать 2 правила для этой группы:

- «открыта дверь группы (тамбура)» – «заблокировать группу дверей на вход и выход»;
- «закрыты все двери группы» – «разрешить группе дверей открываться на вход и на выход».

Алгоритм работы можно понять из содержания этих правил: когда одна дверь в шлюзе открыта, то остальные нормальным путем открыть нельзя, они разблокируются только после закрытия этой двери.

ПРИМЕЧАНИЕ – Для программной реализации работы шлюза прошивка контроллеров должна быть версии 1.6 и более новой. Так как данная логика работы реализована на программном уровне, то она будет работать только в он-лайн режиме (при запущенной программе «Сервер ИКБ» и наличии с ним связи).

## 4.14 Настройка картоприемника

Открыть окно свойств турникета и установить необходимые категории доступа и параметры Ограничение выхода и Контроль повторного прохода (рисунок 4.14.1).

ПРИМЕЧАНИЕ: – Уровни доступа у карт сотрудников и гостевых карт должны быть различны. Уровень доступа для гостевых карт должен совпадать с группой доступа, установленной в программе «Бюро пропусков» (по умолчанию – 25).

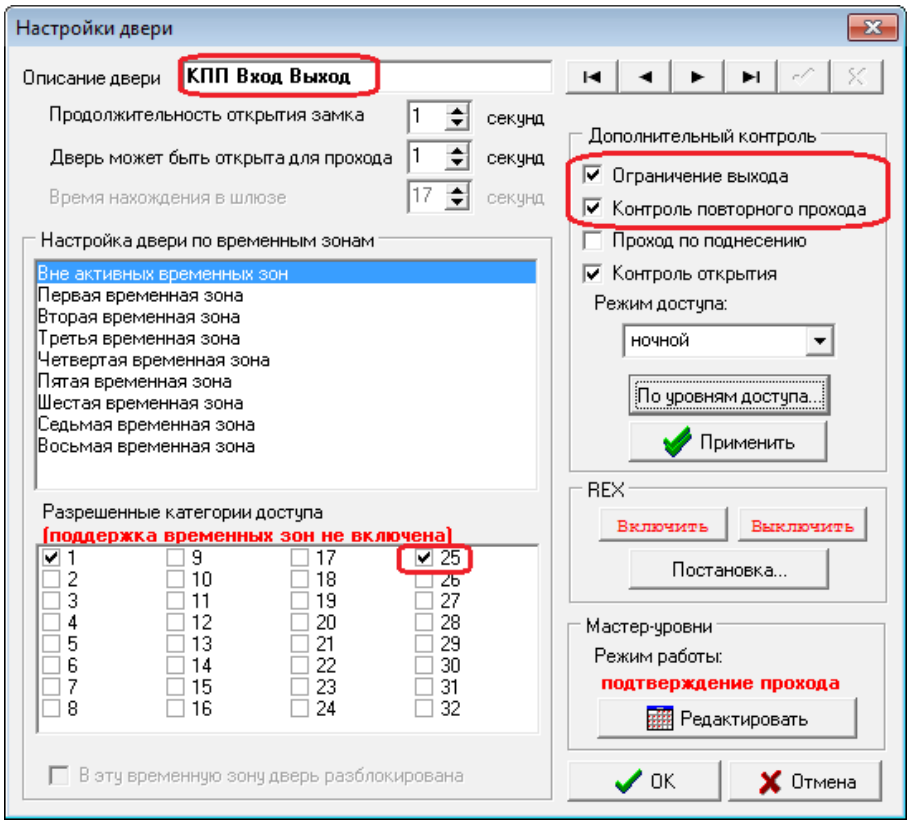



**Рисунок 4.14.1**

Нажать кнопку По уровням доступа (рисунок 4.14.1). В открывшемся окне установить запрет на выход для гостевых карт (рисунок 4.14.2).

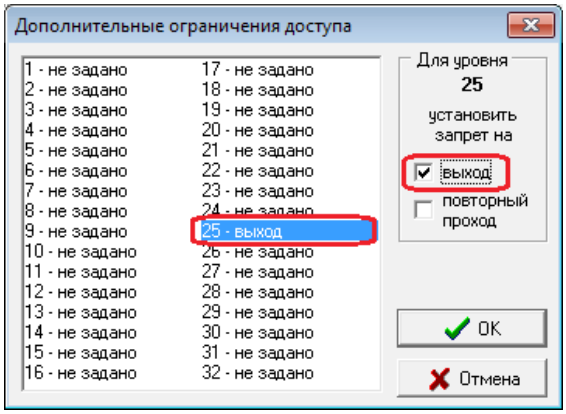



**Рисунок 4.14.2**

ПРИМЕЧАНИЕ – Запрет на повторный проход для гостевых карт устанавливать нельзя. Выход для гостевых карт через данную точку прохода осуществляется через отдельный контроллер (контроллер картоприемника). Поэтому для контроллера доступа всегда проход осуществляется в одном направлении.

Запрет на повторный проход для сотрудников выставляется в зависимости от режима, установленного на объекте.

ПРИМЕЧАНИЕ – При работе контроллера в автономном режиме, выходы через картоприемник не отрабатываются.

## 4.15 Планировщик задач

В «ИКБ КОДОС» существует возможность программировать выполнение определенных действий при наступлении заданного момента времени.

Для настройки планировщика задач нажать кнопку Задачи на вкладке Управление.

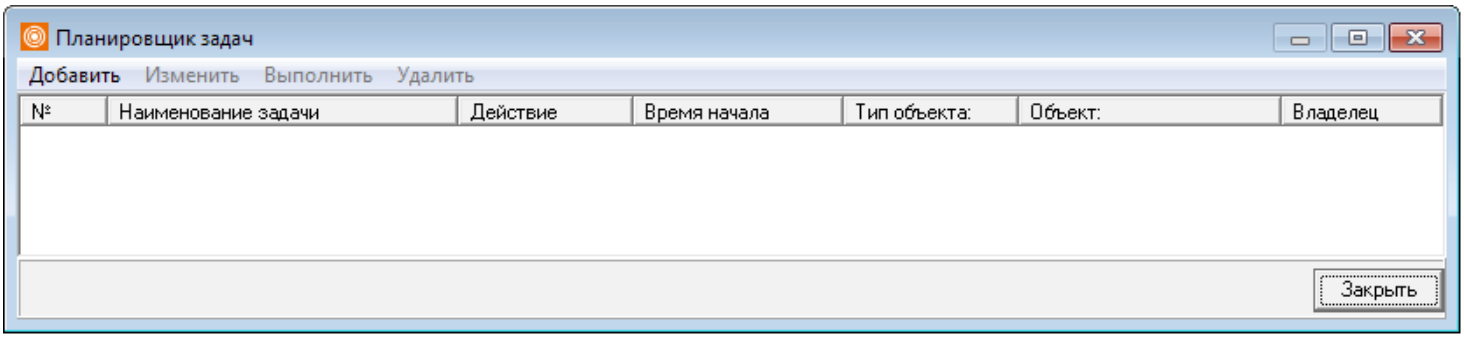



**Рисунок 4.15.1**

Для создания новой задачи нажать кнопку Добавить (рисунок Ошибка: источник перекрестной ссылки не найден).

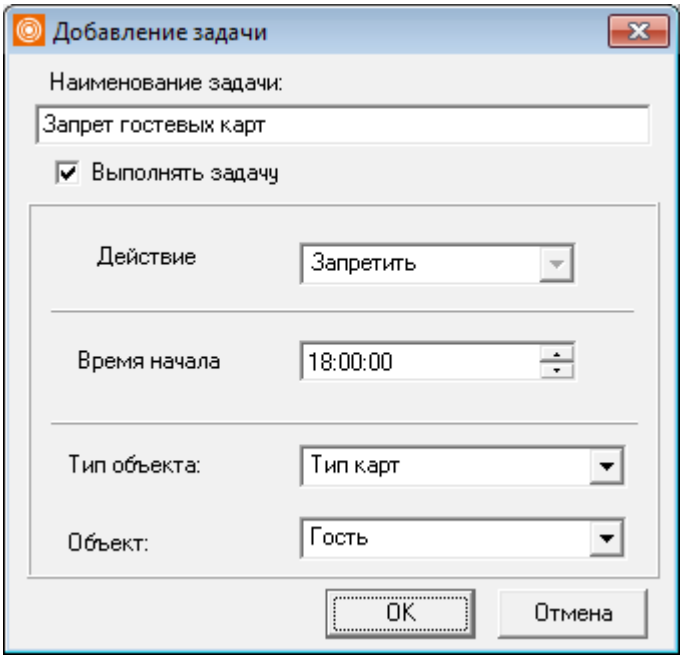



**Рисунок 4.15.2**

Параметр Выполнять задачу (рисунок 4.15.2) определяет, будет ли выполняться задача или нет. При снятии галочки, задача останется в базе данных, но при наступлении указанного момента времени, выполняться не будет.

В поле Выбор действия выбирается выполняемое действие.

ПРИМЕЧАНИЕ – В текущей версии программы доступно только одно действие - Запретить.

Для установки времени выполнения задачи установите его значение в поле Время начала. Задание будет выполняться ежедневно в указанное время.

В поле Тип объекта доступны следующие значения: тип карт, группа пользователей, карта.

В поле Объект доступны значения, соответствующие выбранному типу объекта.

Для выполнения любой задачи в текущий момент времени необходимо нажать кнопку Выполнить (рисунок Ошибка: источник перекрестной ссылки не найден).

# 5 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ ПРОГРАММЫ

## 5.1 Настройка USB считывателя

При большом количестве карт и большом расстоянии от считывателя до компьютера с соответствующим ПО, определение номеров карт может быть связано с рядом неудобств и большой вероятностью ошибки.

В этом случае целесообразно использовать считыватель, подключаемый через USB порт компьютера.

Установка и настройка USB считывателя.

1. Подключить USB считыватель к USB порту компьютера.

2. Мастер подключения оборудования обнаружит новое устройство и предложит установить для него драйвера (рисунок 5.1.1). Нажать «Далее».

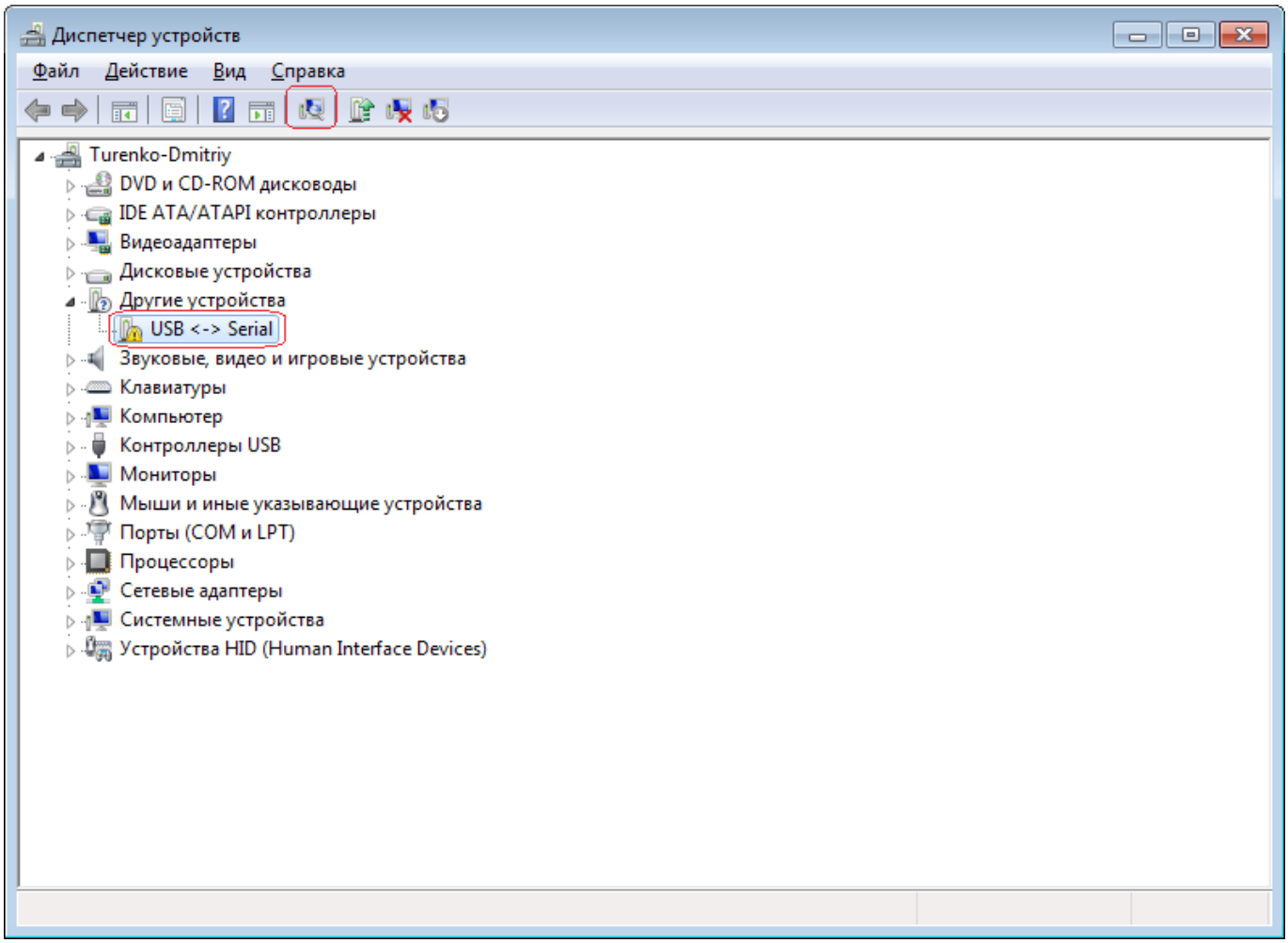



**Рисунок 5.1.1**

3. В окне «Установка драйверов оборудования» выбрать «Провести поиск подходящего драйвера для устройства (рекомендуется)». Нажать «Далее» (рисунок 5.1.2).

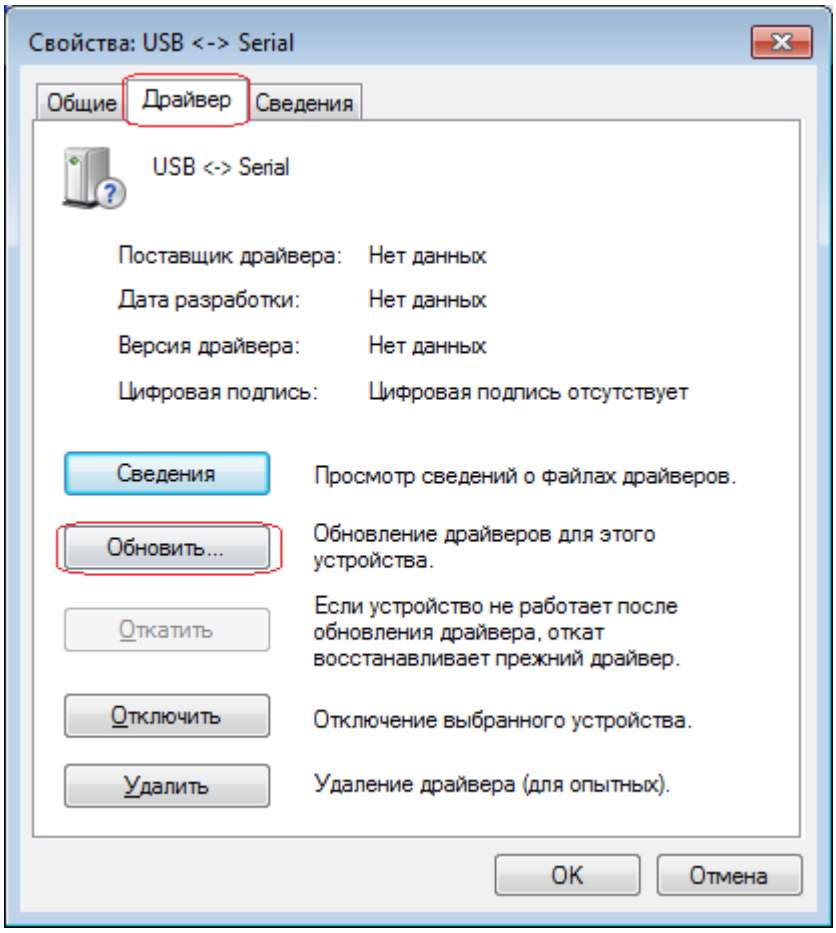



**Рисунок 5.1.2**

4. В окне «Поиск файлов драйвера» поставить флажок в строке «Размещение будет указано». Нажать кнопку «Далее» (рисунок 5.1.3).

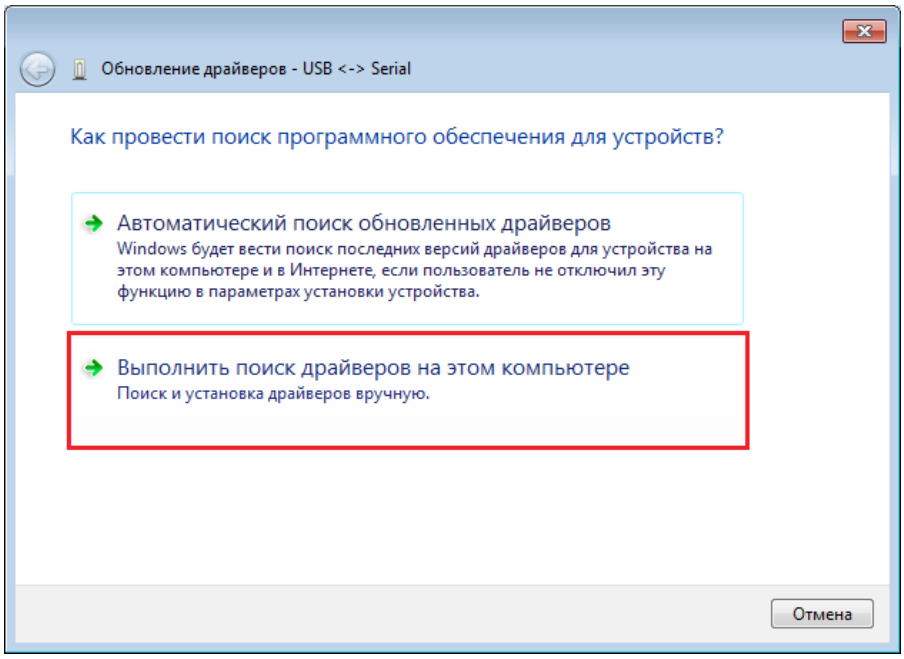



**Рисунок 5.1.3**

5. Вставить диск с драйверами в дисковод. В окне выбора места размещения драйверов указать путь к диску с драйверами «Диск:\ Drv». Нажать кнопку «ОК» (рисунок 5.1.4).

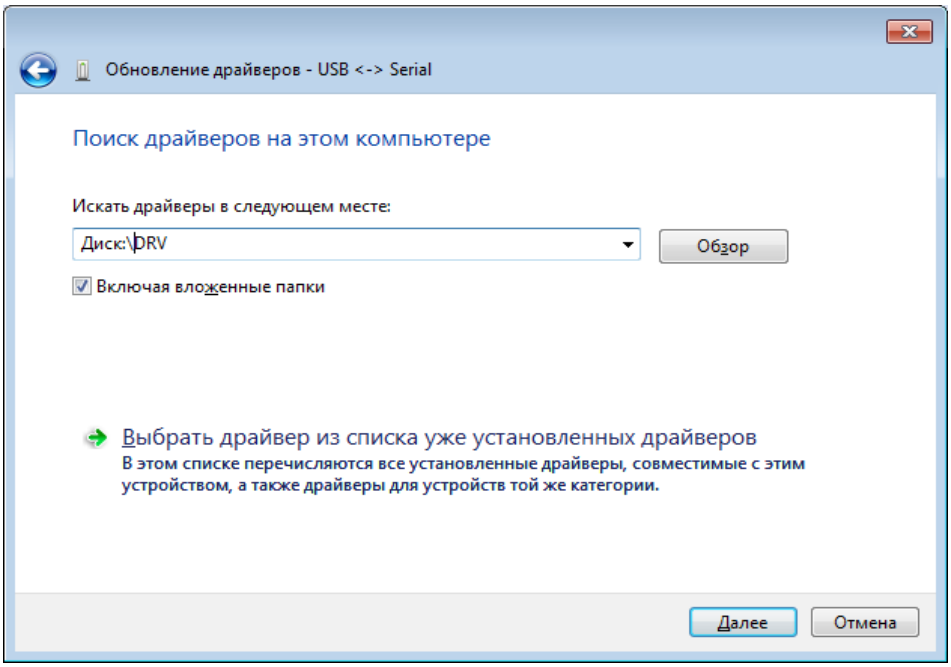



**Рисунок 5.1.4**

6. После того, как мастер подключения оборудования выдаст сообщение о нахождении драйвера и готовности к установке, нажать кнопку «Далее», после чего начнется установка ПО. По окончании установки драйверов необходимо проверить новое устройство: на рабочем столе, щелчком правой кнопки вызвать контекстное меню «Моего компьютера», затем «Свойства»→«Оборудование»→«Диспетчер устройств»→«Порты (COM и LPT)»→«USBSerialPort(COM_)». Считыватель, подключенный к USB порту, идентифицируется как еще один COM порт с очередным номером (рисунок 5.1.5)

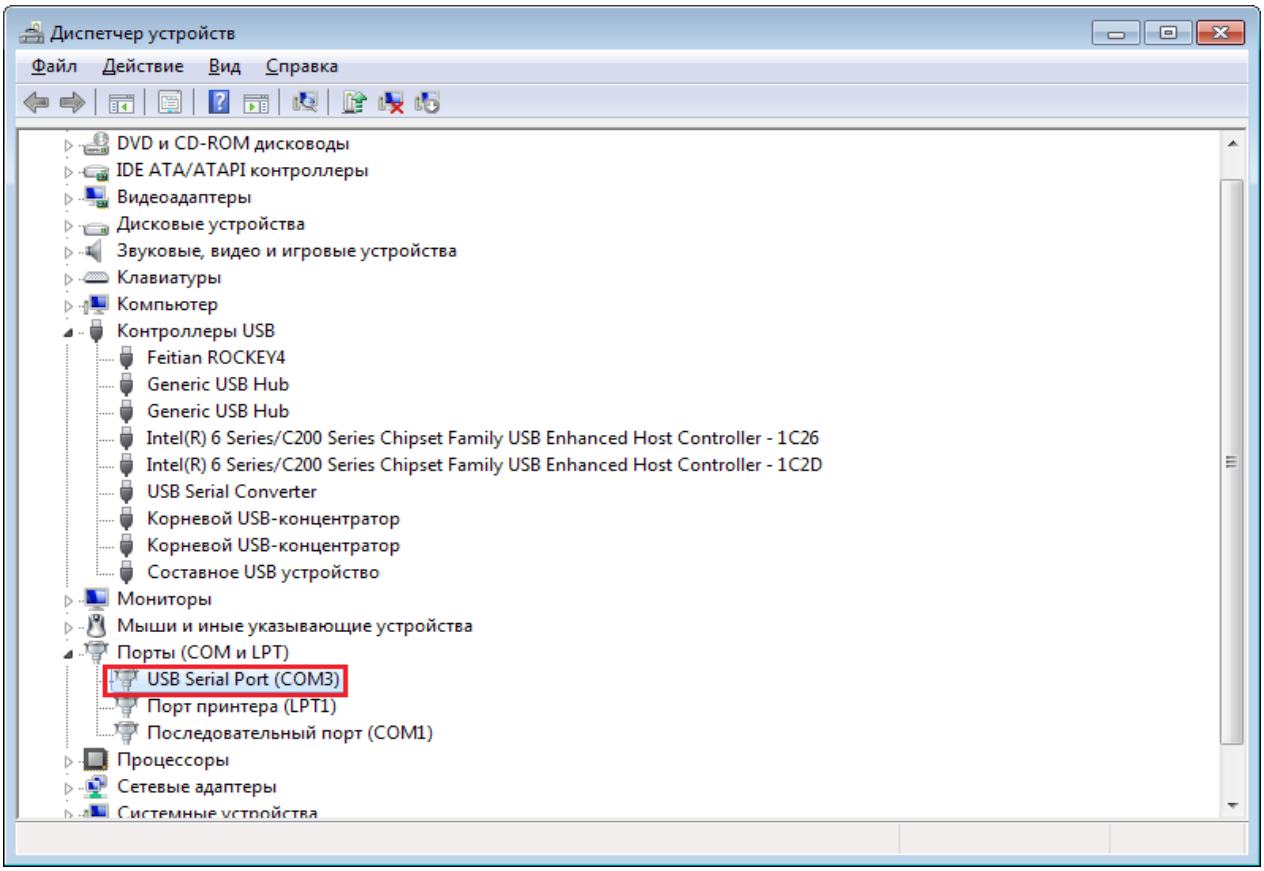



**Рисунок 5.1.5**

7. Далее необходимо перейти в корневую папку программы «КОДОС ИКБ», расположенную, в зависимости от диска установки: диск установки□SSA□SKD□codos.ini (рисунок 5.1.6). Открыть файл codos.ini в текстовом редакторе «Блокнот».

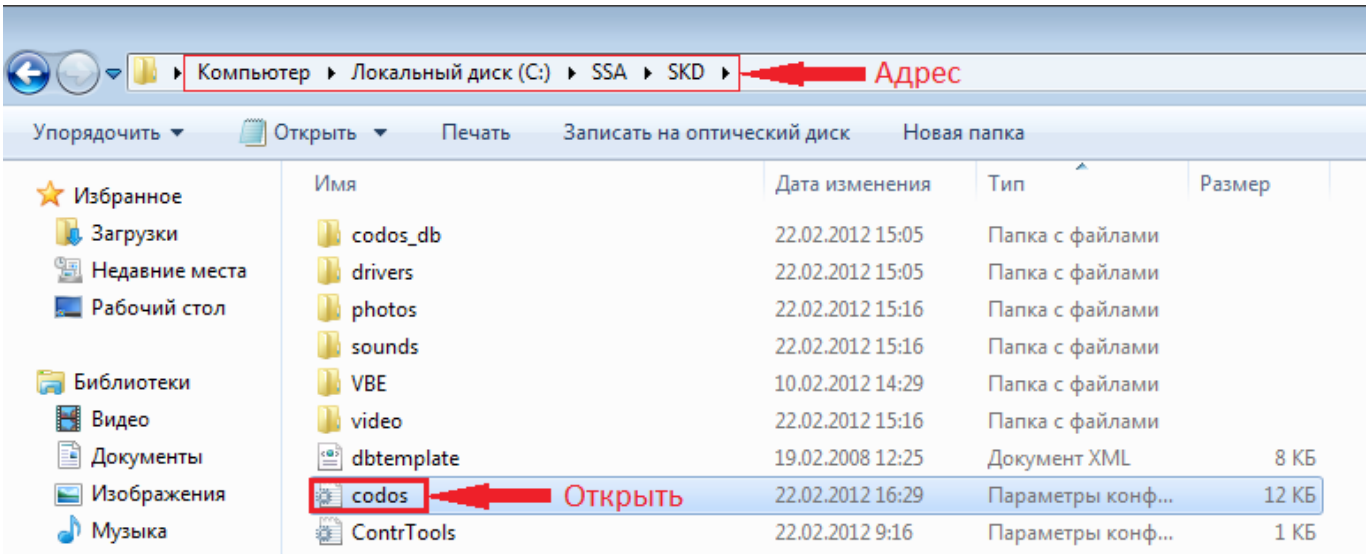



**Рисунок 5.1.6**

8. В разделе [Hardware] прописать следующие строки: «ReaderPort=COM_» и «ReaderPortBaud=9600». Номер COM порта указать тот, который указан в «Диспетчере устройств» (рисунок 5.1.7), например «ReaderPort=COM3» (рисунок 5.1.7).

**ВНИМАНИЕ!** Следует обратить особое внимание на регистр букв, а также на отсутствие пробелов при написании добавляемых строк. При ошибочном вводе изменения учитываться не будут.

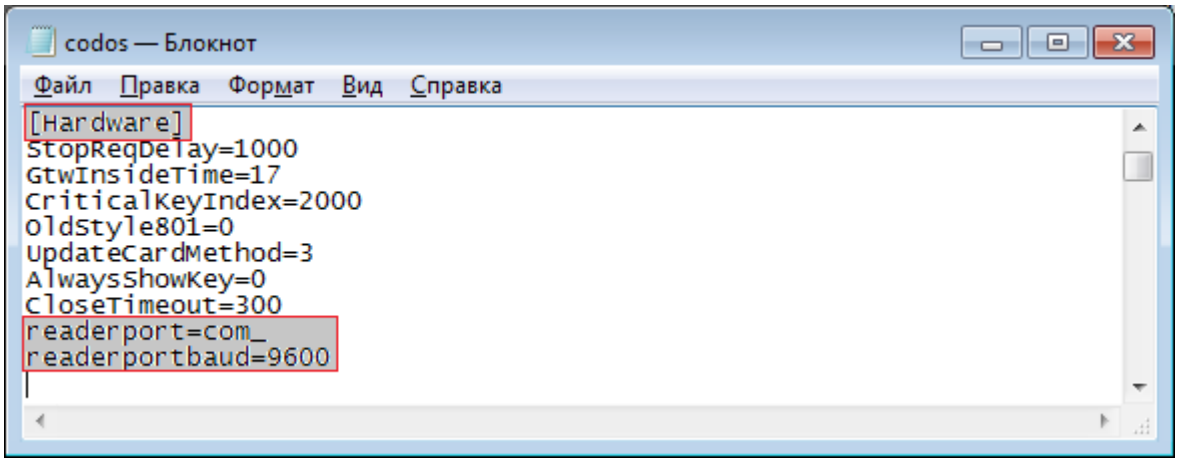



**Рисунок 5.1.7**

9. После того, как строки будут добавлены, файл codos.ini следует сохранить и закрыть. Перезапустить «Сервер ИКБ», чтобы изменения в файле codos.ini вступили в силу.

## 5.2 Настройка модуля персонализации

ПРИМЕЧАНИЕ – Возможность добавления фотографии пользователю определяется наличием лицензии на «модуль персонализации карт доступа и печати пропусков». При отсутствии лицензии на данный модуль функция недоступна. При необходимости добавления данного модуля необходимо обратиться к представителям ООО «КОДОС».

Если предполагается создавать фотографии с помощью видеокамеры, то предварительно должно быть настроено видеооборудование и подготовлено место для фотографирования, обеспечивающие требуемое качество изображения.

☑ В свойствах видеоисточника при их редактировании с помощью Конфигуратора должен быть поставлен флаг «Источник модуля персонализации» (рисунок 5.2.1).

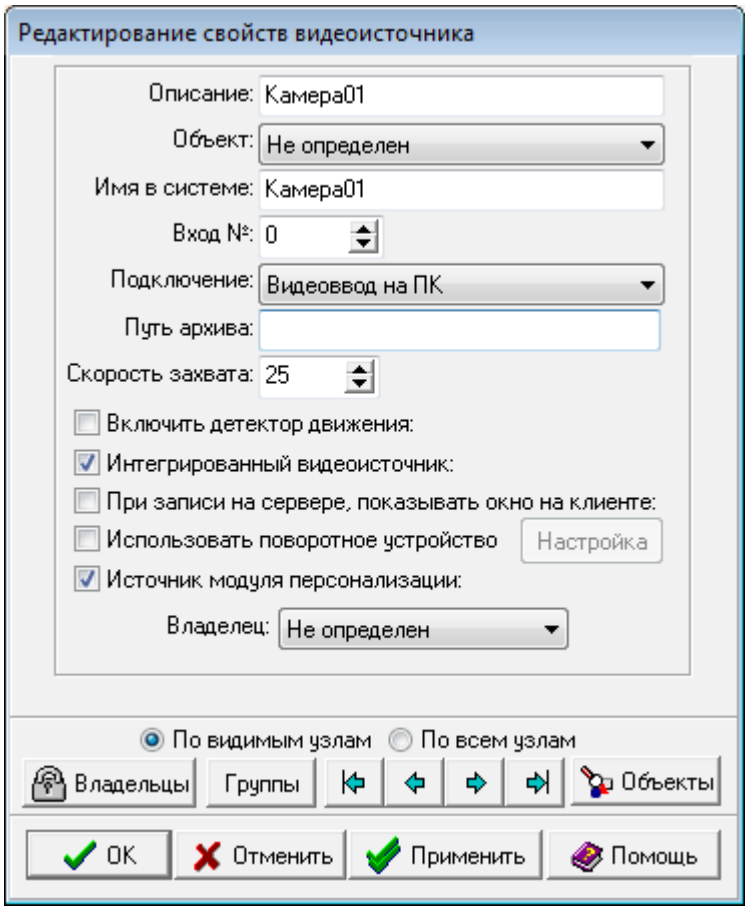



**Рисунок 5.2.1**

При использовании сетевой видеокамеры в качестве видеоисточника модуля персонализации, в ходе конфигурирования Системы, к ПК, на котором установлен сервер ИКБ «КОДОС», необходимо добавить ПК-видеосервер (на рисунке 5.2.1 – PC), а уже к нему – видеоисточник (на рисунке 5.2.2 – Персонализация).

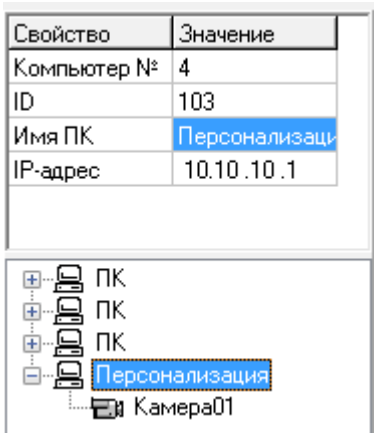



**Рисунок 5.2.2**

ПРИМЕЧАНИЕ – Дополнительно в файле codos.ini необходимо в секции [PhSelectPhoto] в параметре CamSysName указываеть имя источника видеоизображения. Например:

[PhSelectPhoto]
CamSysName=snd2

## 5.3 Настройка модуля учета и выдачи карт посетителям

ПРИМЕЧАНИЕ – «Модуль учета и выдачи карт посетителям» доступен только при наличии лицензии на данный модуль. Процесс проверки и ввода лицензии описан в разделе.1.1. При отсутствии лицензии на данный модуль функция недоступна. При необходимости добавления данного модуля обратиться к представителям ООО «КОДОС».

«Модуль учета и выдачи карт посетителям» (далее Модуль) предназначен для организации учета выданных посетителям охраняемого объекта карт доступа – пластиковых кодоносителей, позволяющих осуществлять вход на охраняемый объект. К функциям модуля относятся:

- просмотр в базе данных списка посетителей и перечня выданных карт,
- поиск посетителя или карты в списках по заданным критериям,
- изменение статуса карт доступа и т.п.

Модуль может работать как на сервере Интегрированного Комплекса Безопасности (ИКБ), так и на компьютере с программным обеспечением (ПО) «Модуля удаленного администрирования».

Принципы работы Модуля в Системе.

- Объектами учета Модуля являются временные посетители.
- Для входа на охраняемый объект каждому посетителю выдается карта доступа – гостевая карта.
- Коды выдаваемых карт, соответствующие им уровни доступа учитываются в базе данных ИКБ (в СКУД).
- Каждый проход посетителя через точки доступа фиксируется в архиве событий Системы.
- Покидая объект, посетитель возвращает карту, которая может быть использована для повторной выдачи с соответствующим изменением учетной записи в базе данных.

С помощью функций Модуля информация о посетителе, например ФИО, фотография или копия документа, удостоверяющего личность, заносится в базу данных учета и выдачи карт, что дает возможность охраннику, сотруднику службы безопасности предприятия:

- однозначно идентифицировать человека, проходящего через точки доступа;
- вести статистику посещений;
- отследить по архиву событий Системы маршрут и график перемещений каждого из посетителей;
- оперативно менять статус карт доступа и т. п.

## 5.4 Настройка модуля дизайна пропусков

При установке программы пользователю доступно только две схемы пропусков: «Голубая1» и «Голубая2». Однако существует возможность создать и собственную схему.

ПРИМЕЧАНИЕ – Создание собственных схем пропусков возможно только при наличии лицензии на «Модуль дизайна пропусков». Процесс проверки и ввода лицензии описан в «Руководстве администратора ИКБ КОДОС». При отсутствии лицензии на данный модуль функция недоступна. При необходимости добавления данного модуля необходимо обратиться к представителям ООО «КОДОС».

Установка «модуля дизайна пропусков возможна как на компьютере с установленными программами Сервер ИКБ, Администратор ИКБ, так и на любой другой компьютер организации (предприятия). Необходимым условием является наличие доступа по локальной сети к базе данных ИКБ КОДОС.

Установка модуля дизайна пропусков осуществляется в процессе установки программы Сервер ИКБ или Администратор ИКБ. Для этого необходимо отметить флагом соответствующий компонент (рисунок 5.4.1).

Если модуль используется автономно на локальном компьютере, то необходимо произвести настройку связи с БД (смотри раздел «ОСОБЕННОСТИ УСТАНОВКИ КЛИЕНТСКИХ РАБОЧИХ МЕСТ»).

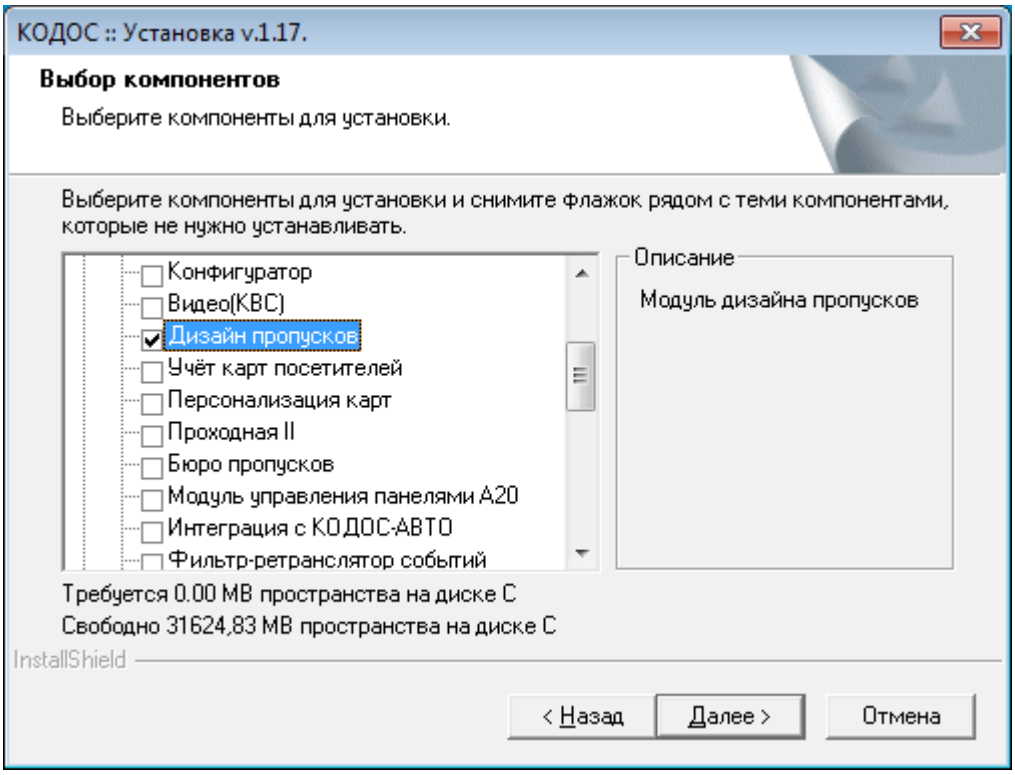



**Рисунок 5.4.1**

## 5.5 Настройка программы «Проходная»

АРМ, где установлена программа «Проходная», является клиентом ИКБ и осуществляет обмен данными с сервером ИКБ по локальной сети.

Для настройки программы «Проходная» нажать кнопку «Настройка» в строке меню главного окна программы. Доступ к настройкам конфигураций имеет только администратор системы, оператору АРМ разрешен выбор одной из заранее настроенных конфигураций. Создание, удаление и изменение конфигураций становится возможным после ввода пароля администратора.

В появившемся окне ввести имя и пароль администратора, затем нажать «Вход» (рисунок 5.5.2). По умолчанию заданы имя - «admin», пароль – «power». По окончанию настройки программы «Проходная» имя и пароль администратора рекомендуется сменить.

ПРИМЕЧАНИЕ – При вводе пароля учитывается регистр и раскладка клавиатуры (RU-EN).

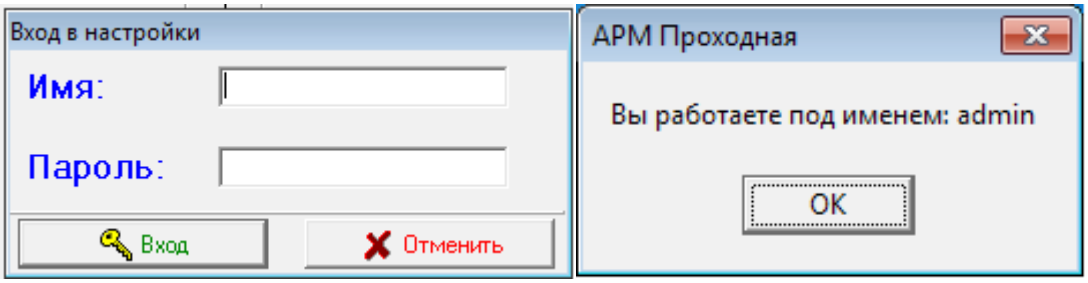



**Рисунок 5.5.1**

После ввода пароля администратору будет показан список конфигураций (рисунок 5.5.3), используемая конфигурация в этом списке выделена.

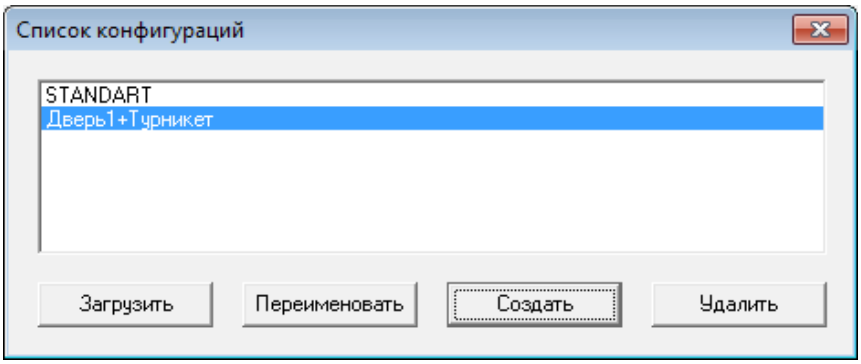



**Рисунок 5.5.2**

Для выполнения настройки выбранной из этого списка конфигурации нажать кнопку Загрузить.

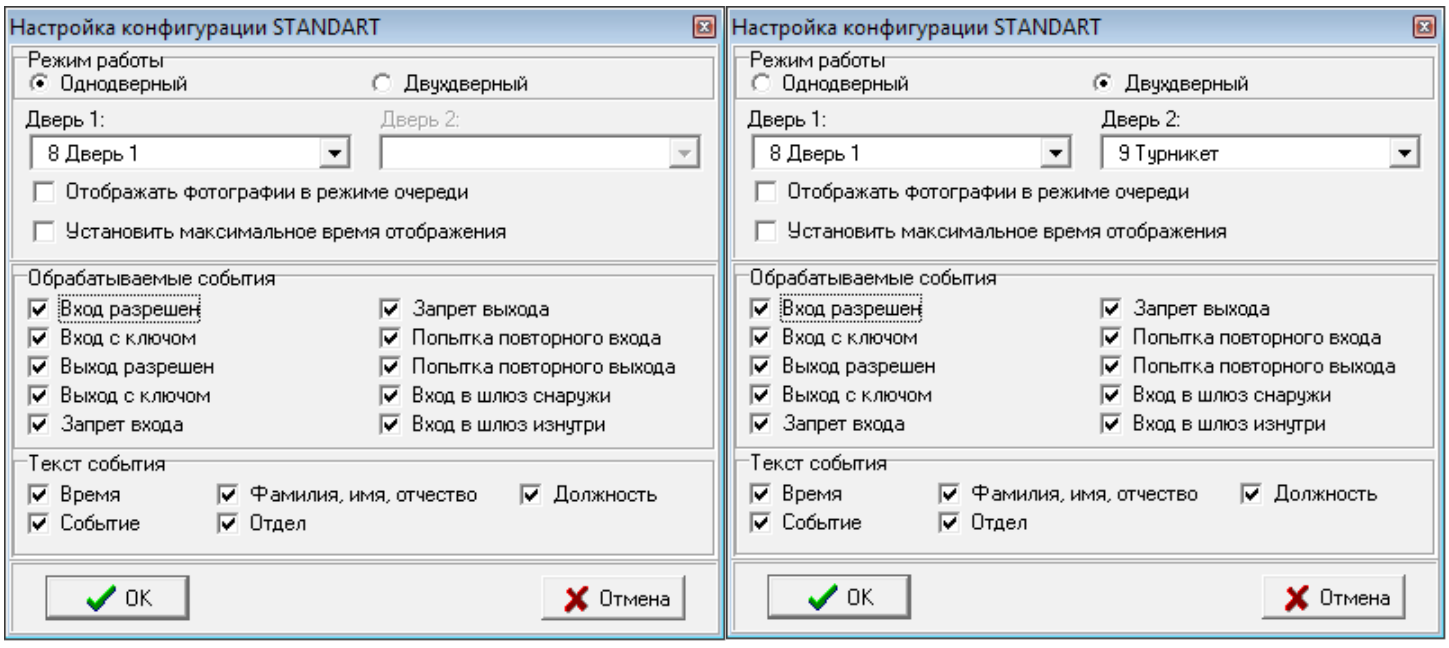
Кнопка Переименовать позволяет изменить имя выбранной конфигурации, не изменяя ее настроек.

Кнопка Создать предназначена для создания новых конфигураций.

Кнопка Удалить позволяет исключить из списка те конфигурации, дальнейшее использование которых представляется нецелесообразным. Любая конфигурация из списка может быть удалена, в том числе предопределенная конфигурация STANDART.

Удаление невозможно, если в списке останется только одна конфигурация. При удалении используемой конфигурации от администратора потребуется подтвердить решение об удалении. Если такое подтверждение будет сделано, то помимо удаления конфигурации произойдет перенастройка программы в соответствии с первой конфигурацией списка.

В окне Настройка (рисунок 5.5.4) выполняются настройки программы Проходная на выборку контролируемых событий, происходящих в системе.




**А) Однодверный режим** **Б) Двухдверный режим**

**Рисунок 5.5.3**

Программа позволяет:

- устанавливать однодверный или двухдверный режим работы программы,
- выбирать точки доступа из числа зарегистрированных в ИКБ;
- начинать или прекращать отображение фотографий в режиме очереди;
- устанавливать максимальное время отображения фотографий;
- вносить изменения в список обрабатываемых событий;
- регулировать содержание текста, характеризующего события.

Существует два режима пропуска пользователей через двери:

- Однодверный.
- Двухдверный.

Однодверный режим работы предполагает настройку АРМ для контроля за одной точкой доступа (рисунок 3.6А).

Флажок Отображать фотографии в режиме очереди в однодверном режиме установлен по умолчанию. При этом в левой панели главного окна выводится фото посетителя, проходящего через дверь. При проходе следующего посетителя предыдущее фото смещается в правую панель окна. Обе панели окна имеют общее название по наименованию точки доступа.

В двухдверном режиме работы осуществляется контроль за двумя точками доступа (рисунок 3.6Б).

Флажок Отображать фотографии в режиме очереди может быть:

- не установлен – текущее событие для каждой точки доступа отображается в своей панели независимо, каждая панель будет иметь название, соответствующее наименованию точки доступа ( Рисунок 3.7).
- установлен – на левой панели отображается текущее событие, на правой – предыдущее, независимо от точки доступа.

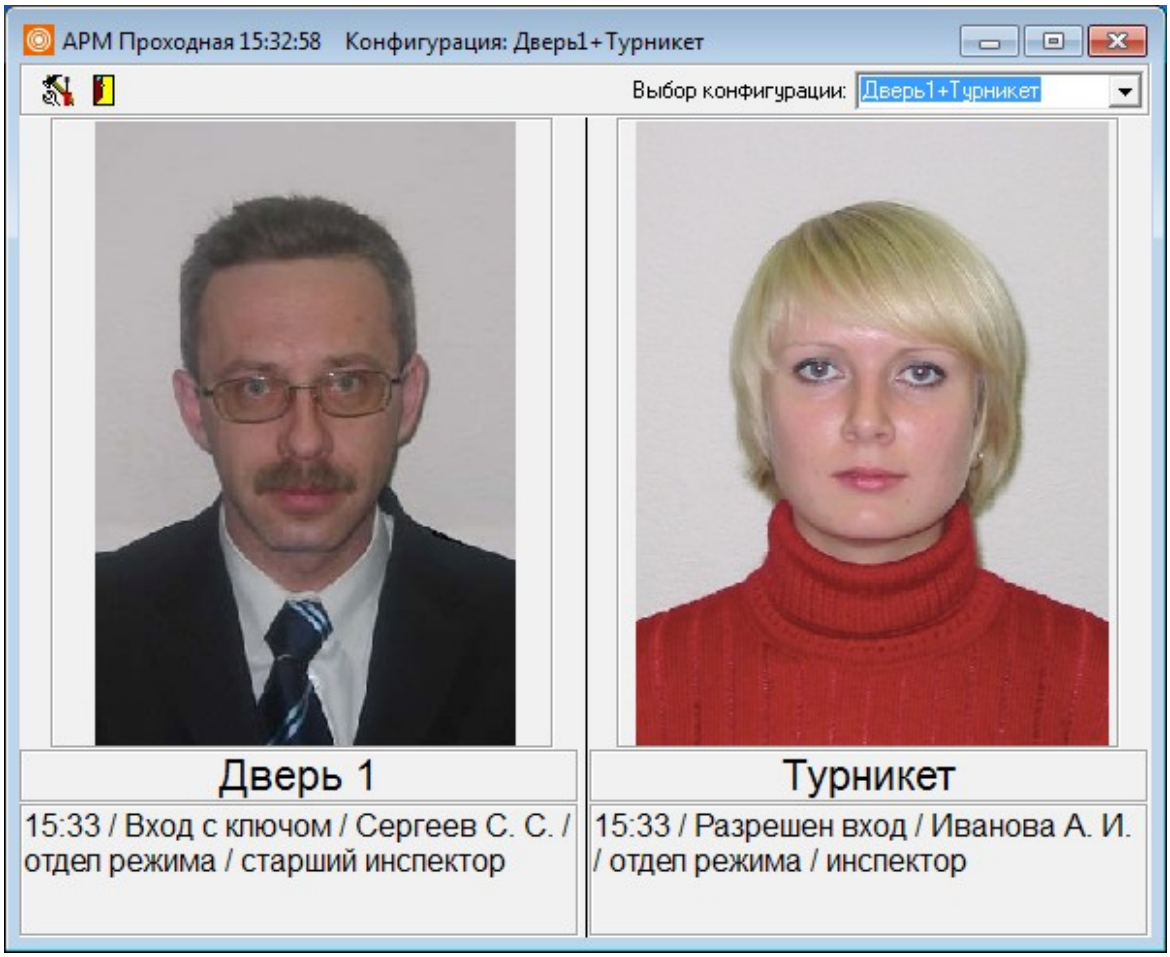



**Рисунок 5.5.4**

ПРИМЕЧАНИЕ – Чтобы не вводить оператора в заблуждение, режим Отображать фотографии в режиме очереди целесообразно использовать только в том случае, когда точки доступа образуют шлюз, не допускающий одновременного открытия двух дверей.

Строки Дверь 1 и Дверь 2 служат для выбора точек прохода: дверей, турникетов, контролируемых АРМ «Проходная».

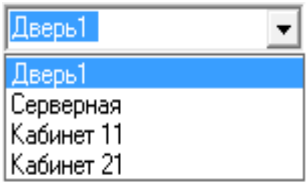



**Рисунок 5.5.5**

Щелчок мышью по кнопке , расположенной справа от поля ввода, раскрывает весь список дверей, сформированный при конфигурировании Системы (рисунок 5.5.5). Нужную точку доступа выбирать щелчком левой кнопки мыши.

Установка флажков в разделе Текст событий определяет перечень сообщений, которые выводятся в качестве комментария к фотоизображениям.

В разделе Обрабатываемые события, необходимо выбрать события которые необходимо контролировать:

- Вход/Выход разрешен - пользователь имеет право доступа/выхода через данную точку прохода.
- Вход/Выход с ключом - для доступа/выхода в данной точке прохода использован разрешенный ключ.
- Запрет входа/выхода - пользователь не имеет права доступа через данную точку прохода.
- Попытка повторного входа/выхода - попытка постороннего пройти контур ЗПП с ключом пользователя, уже прошедшего контролируемый контур в этом направлении.
- Вход в шлюз снаружи/изнутри - индикация направления прохода шлюза пользователем, имеющим право доступа через данную точку.

По окончании настройки нажать кнопку ОК.

Если в созданную ранее конфигурацию администратором системы были внесены изменения, то будет предложено подтвердить сохранение настроек программы. Можно отказаться от внесенных в конфигурацию изменений.

Для ограничения доступа оператора АРМ к настройкам программы кнопка Настройка может быть скрыта. Для этого следует произвести корректировку файла «codos.ini» в директории (папке) C:\SSA\SKD следующим образом: в разделе [PassFunc] параметру setupvisible присвоить значение, равное «0»:

[PassFunc]

Setupvisible=0

Для отображения этой кнопки параметру Setupvisible  нужно присвоить значение, равное 1.

Сохранить изменения файла codos.ini и перезапустить программу Проходная. Изменения будут приняты.

## 5.6 Настройка бюро пропусков

### 5.6.1 Установка программы

Перед установкой ПО Системы должно быть смонтировано и подключено все ее оборудование: компьютер Бюро пропусков, устройство фотографирования документов, считыватель и др. Порядок и схемы подключения оборудования описаны в документации на соответствующие устройства.

Подготовить и зафиксировать (прописать) в базе данных системы СКУД комплект карт, которые предполагается выдавать посетителям. Картам должны быть назначены соответствующие посетителю уровни доступа. Порядок прописывания кодоносителей изложен в «Руководстве пользователя ИКБ КОДОС».

Перед началом работы необходимо прописать путь к базе данных «ИКБ КОДОС». Порядок настройки описан в п.2.5.2 «Настройки псевдонима (alias) для клиентского компьютера»

Если при запуске программы «Бюро пропусков» появляется окно сообщения об ошибке связи с базой данных, то это может быть следствием либо неверной установки параметров связи с базой, либо отсутствия связи с удаленным по сети компьютером, на котором эта база размещена.

Запуск программы на выполнение (загрузочный модуль buro.exe) может осуществляться любым из известных для Windows способов, например, через главное меню рабочего стола (Пуск => Программы => => ИКБ КОДОС => Бюро пропусков).

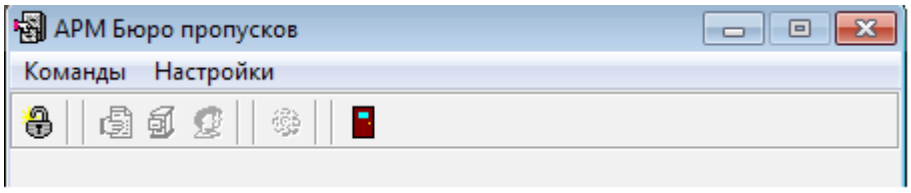



**Рисунок 5.6.1**

Главное окно программы представлено на рисунке 5.6.1. Под заголовком окна "АРМ бюро пропусков" расположено основное меню программы ("Команды" и "Настройки"), все пункты которого продублированы экранными кнопками панели инструментов.

Кнопка панели инструментов ("Регистрация в системе") служит для вызова диалога (рисунок 5.6.2) ввода имени пользователя и пароля, подтверждающих права доступа оператора к работе с Системой.

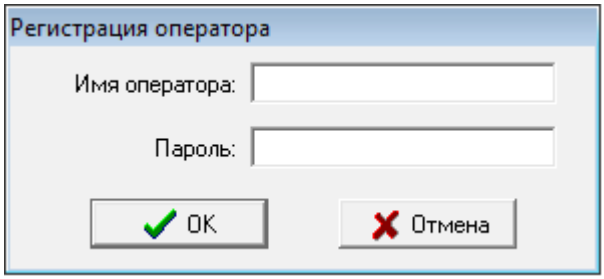



**Рисунок 5.6.2**

**ВНИМАНИЕ!** При вводе пароля необходимо учитывать язык и регистр символов.

В окне Регистрация оператора оператор должен заполнить поля ввода: Имя оператора: и Пароль:. Пароль (секретное слово) при вводе отображается звездочками. Имя и пароль каждому оператору назначается администратором Системы (см. п.5.6.2).

При инсталляции системы «КОДОС» предустановленным является только имя оператора PBADMIN. Предустановленный пароль – пустой (ни одного символа).

При инсталляции программы оператор с именем «PBADMIN» не имеет прав по работе с программой.

Для настройки программы предварительно необходимо настроить права операторов.

ПРИМЕЧАНИЕ – Если в Вашей организации эти параметры были изменены, то Вам следует обратиться за консультацией к своему системному администратору.

Нажатие кнопки «OK» завершает запуск программы Бюро пропусков. Кнопка Отмена служит для отказа от работы с программой. Признаком корректного входа в программу является доступность всех экранных кнопок панели инструментов.

Для завершения работы с программой служит экранная кнопка Выход и системная кнопка  , расположенная в правом верхнем углу главного окна.

### 5.6.2 Редактирование прав операторов

Работа оператора с программой осуществляется на основании разрешений, полученных при настройке. После установки программы существует единственный пользователь «PBADMIN», причем, по умолчанию, он не имеет прав доступа по работе с программой.

Вызов окна «Список операторов» (рисунок 5.6.3) осуществляется щелчком мыши по экранной кнопке  («Список операторов») на панели инструментов главного окна программы.

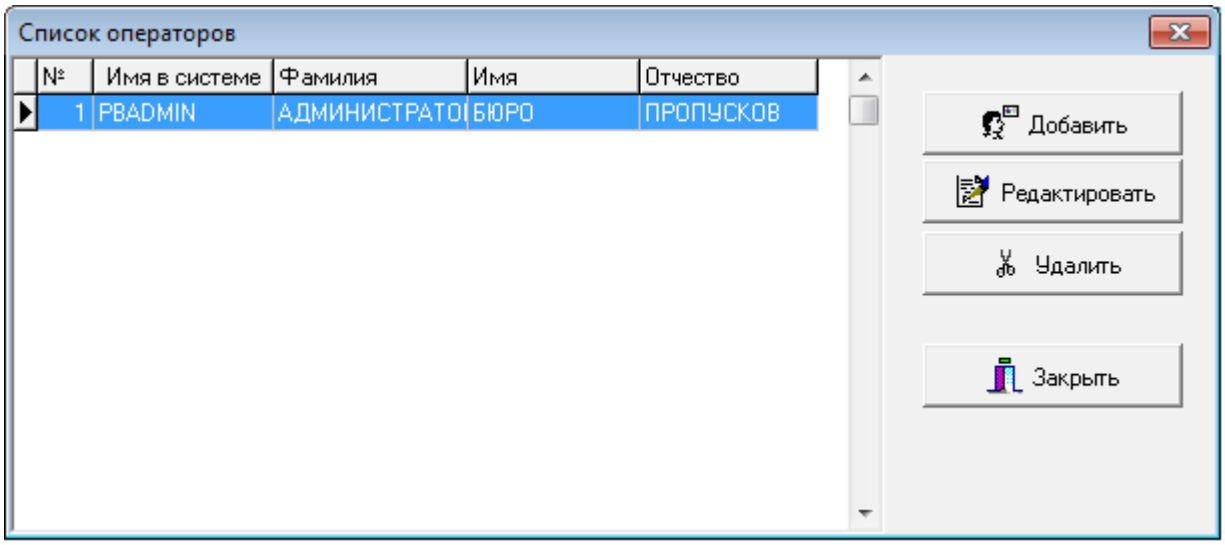



**Рисунок 5.6.3**

**ВНИМАНИЕ!** Доступ к работе со списком операторов имеет только администратор Системы.

В рабочей области окна располагается таблица с пятью полями, назначение которых следует из их названий. Содержимое полей может быть изменено. Исключение составляет порядковый номер записи, который присваивается Системой автоматически без участия администратора.

Текущая запись (строка) таблицы выделяется щелчком мыши, помечена маркером  и подсвечивается контрастным фоном.

Экранные кнопки, расположенные справа от таблицы, служат для завершения работы со списком операторов («Закрыть»), удаления текущей записи таблицы («Удалить»), добавления (в конец списка) новой записи («Добавить») и внесения изменений в текущую запись («Редактировать»).

При нажатии кнопок «Добавить» и «Редактировать» (или двойной щелчок по записи) открывается диалоговое окно, представленное на рисунке 5.6.4.

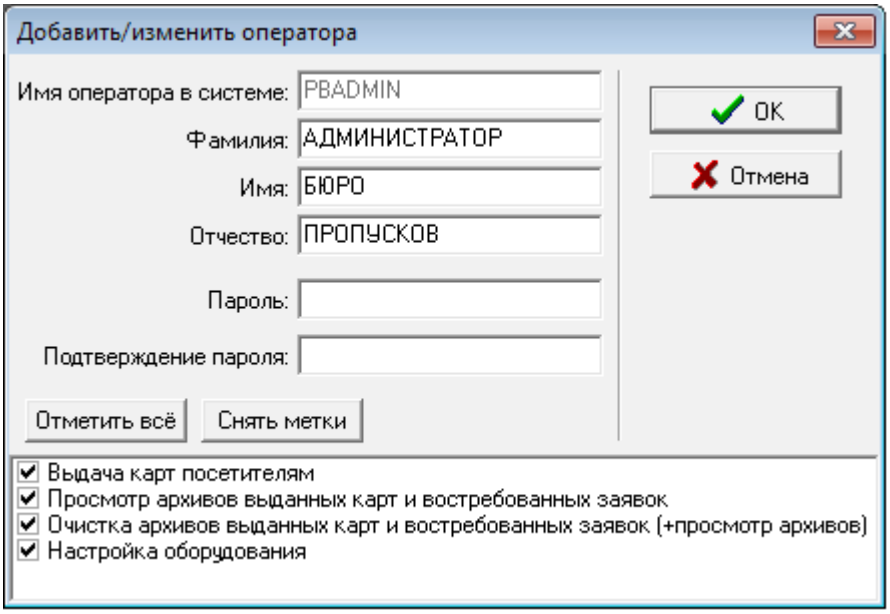



**Рисунок 5.6.4**

Назначение полей ввода совпадает с их названиями. Информация вводится с клавиатуры. Для перехода от поля к полю используется мышь и/или клавиша <Tab> на клавиатуре.

В поле «Имя оператора в системе:» можно задать до 15 символов (рекомендуются буквы и цифры).

В полях «Фамилия:», «Имя:» и «Отчество:» можно задать до 255 символов (рекомендуются буквы в количестве, ограниченном видимыми размерами поля).

ПРИМЕЧАНИЕ – При заполнении описанных выше полей программа для повышения надежности автоматически переводит все буквы в верхний регистр (в заглавные буквы).

В полях «Пароль:» и «Подтверждение пароля:» можно задать до 15 символов, которые будут использоваться оператором при входе в программу (см. п. 5.6.1 ). При вводе паролей учитываются язык и регистр символов. Из соображений безопасности вводимые символы отображаются звездочками. Содержимое обоих полей должно абсолютно совпадать.

Назначение флагов, располагаемых в нижней части окна, следует из их названий. Флаги («метки») устанавливаются/снимаются щелчками мыши. Экранная кнопка «Отметить все» позволяет одним нажатием установить сразу все метки. Экранная кнопка «Снять метки» позволяет одним нажатием снять сразу все флажки.

ПРИМЕЧАНИЕ – Для администратора Системы флаги, регламентирующие его права, всегда остаются установленными.

Нажатие кнопки «OK» закрывает окно, сохраняя в памяти новые значения свойств оператора. Кнопка «Отмена» (и системная кнопка ) закрывает окно, не сохраняя в памяти внесенные изменения.

**ВНИМАНИЕ!** При вводе Системы в эксплуатацию настоятельно рекомендуется изменить предустановленный изготовителем пароль Администратора.

### 5.6.3 Настройка оборудования

В строке меню окна «АРМ бюро пропусков» выбрать «Настройки». Откроется окно «Настройки» (рисунок 5.6.5).

В строке «Имя канала видеоввода» ввести имя видеоисточника, соответствующее полю «имя в системе» в конфигурации.

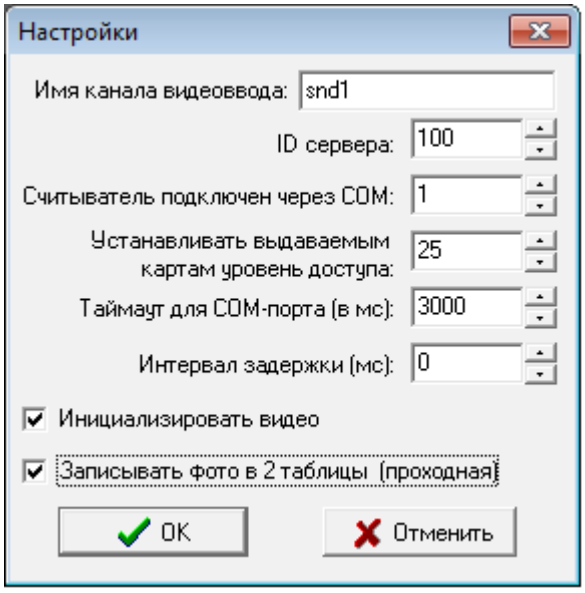



**Рисунок 5.6.5**

Значение "ID сервера:" соответствует значению, присваиваемому по умолчанию ПК- серверу в программе «Конфигуратор». Под сервером в данном случае понимается ПК, на котором установлена плата видеоввода, или подключена USB-камера. По умолчанию равно «100».

В поле «Считыватель подключен через COM:» следует задать номер последовательного порта, к которому подключен считыватель. Для этого в диспетчере устройств необходимо проверить номер COM-порта, который эмулирует USB считыватель.

Поле «Таймаут для COM-порта (в мс):» позволяет установить период (в миллисекундах) считывания кода выдаваемой карты. Например, значение 3000 означает, что через каждые 3 секунды Система будет повторно принимать код карты, размещенной на поверхности считывателя. Изначально рекомендуется принять значение, установленное по умолчанию.

В поле «Устанавливать выдаваемым картам уровень доступа:» указывается число (в диапазоне от 1 до 32), соответствующее уровню доступа гостевых карт, принятому в системе СКУД охраняемого объекта.

В поле "Интервал задержки, мс" устанавливается время задержки на выдачу следующей карты. По умолчанию равно «0». Рекомендуется увеличивать данное время при значительных нагрузках на сервер СУБД, а так же при загруженных или «плохих» линиях связи по протоколу TCP\IP.

Установка флага «Инициализировать видео» включает вывод видеоизображения для фотографирования документа, удостоверяющего личность посетителя. Если по каким-либо причинам фотографирование документа не предполагается, то этот флаг можно снять.

Если установить флаг "Записывать фото в 2 таблицы (проходная)", то фотографии посетителей будут отображаться в окне «Кто на входе?» на сервере и клиенте (программа удаленного администрирования), а так же в программе «Проходная». Отключение данной функции позволяет экономить значительное место в базе данных.

Кнопка «Отменить» служит для отказа от внесенных изменений. Нажатие кнопки «OK» завершает процесс настройки оборудования.

**ВНИМАНИЕ!** Установленные значения параметров настройки оборудования вступают в силу только после перезапуска программы «Бюро пропусков».

Изображение будет транслироваться с видеокамеры в панели с видеокамеры. Чтобы изображение зафиксировать в качестве фотографии, нажать кнопку Фото, появится фотография (рисунок 5.6.6).

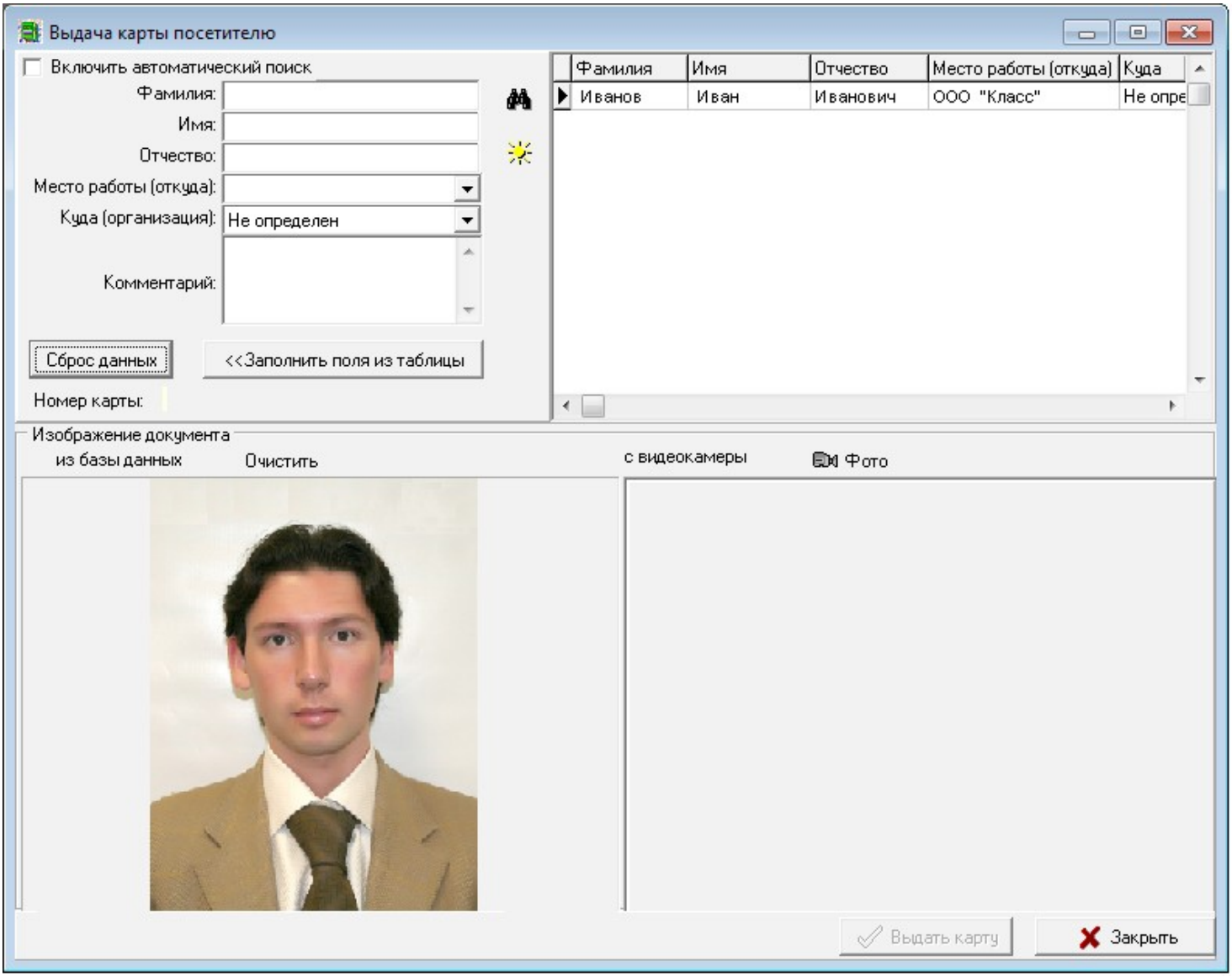



**Рисунок 5.6.6**

## 5.7 Дополнительные настройки

Для необходимости более тонкой настройки ИКБ КОДОС некоторые настройки осуществляются в файле codos.ini, находящегося в папке, где установлена программа. Структура файла стандартна для ОС Windows, редактирование файла осуществляется в любом текстовом редакторе, например в Блокноте (рисунок 5.7.1).

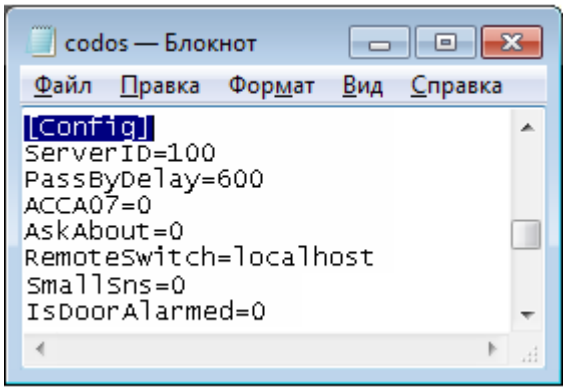



**Рисунок 5.7.1**

Ниже приведены основные параметры настройки с описанием порядка их установки.

ПРИМЕЧАНИЕ – Во избежание вывода программы из строя не рекомендуется менять остальные настройки, присутствующие в файле без предварительного согласования с отделом технической поддержки НПК «Союзспецавтоматики».

**Секция [Database]**

DBAlias - Этот параметр указывает Системе alias (псевдоним) базы данных. Тип базы (Interbase, Oracle, MS SQl), способ организации данных и другие характеристики БД задаются с помощью программы BDE Administrator.

Значением параметра является идентификатор псевдонима. Рекомендуется использовать набор латинских букв и арабских цифр в количестве не более 8. Например, DBAlias=codos_ib

**Секция [Config]**

AlwaysSwitchToPlanes – определяет режим переключения на план, в случае срабатывания датчиков. По умолчанию (0) – переключений не будет. (1) - переключать на планы при срабатывании датчиков только при нахождении на вкладке «Планы», (2) переключать на планы при срабатывании датчиков всегда (с любой вкладки).

ShowSnsText - показывать номера датчиков на планах (1) – по умолчанию, не показывать – (0).

AlwaysShowFloor - показывать все этажи (1) или только этажи на которых установлено оборудование (0) – по умолчанию.

IsDoorAlarmed – если дверь стоит на охране, то будет ли выдаваться тревога при проходе с разрешенной картой(1), тревоги не будет - (0) – по умолчанию.

ActionsVisible - показывать в мониторе текущих событий действия операторов (1) или нет - (0) - по умолчанию.

SectionsVisible – разрешает (1) или нет (0) выводить в мониторе текущих событий содержимое раздела при постановке (снятии).

MaxRecCount=N – «N» - максимальное число событий, выводимое в списке архива событий.

NotUseWav –включать уведомление о событиях через стандартный аудиовыход ПК (0), уведомление выключено (1)

**Секция [HardWare]**

Soundoff=0 - спикер ПК включен.(0) –по умолчанию, (1) - выключен.

ReaderPort - указатель номера COM –порта, к которому подключен USB-считыватель.

ReaderPortBaud –скорость работы через COM – порт при подключении USB-считывателя. Установлено 9600, менять не рекомендуется

**Секция [Video]**

CriticalFreeSpace - если объём свободного пространства на диске меньше этого параметра (в мегабайтах), начинается кольцевая запись, то есть новые видеоархивы будут записываться поверх самых старых

User – имя профиля пользователя в программе «GLOBOSS» («Кодос-Видеосеть»), от имени которого получается видеоизображение

Password – пароль пользователя в программе «GLOBOSS» («Кодос-Видеосеть»), от имени которого получается видеоизображение

**Секция [A-20]**

RstFirst – число минут до первого опроса конфигурации A-20 \. По умолчанию =15

RstReplay – число часов до повторного опроса конфигурации. По умолчанию = 6

## 5.8 Настройка программы для крупных объектов

Конфигурирование «ИКБ КОДОС» для крупных объектов, где число карт доступа превышает 2000, заключается в дополнительной настройке параметров периферийного оборудования и «ИКБ КОДОС». В этом случае рекомендуется производить перераспределение динамической памяти контроллеров доступа и параметров работы программы.

ПРИМЕЧАНИЕ – Не следует использовать эти настройки без необходимости для обычных объектов.

### 5.8.1 Настройка контроллеров доступа для крупных объектов

**Конфигурирование контроллеров с помощью утилиты ContrTools.**

1. Закрыть программу «ИКБ КОДОС». Запустить утилиту ContrTools.
2. В появившемся окне, во вкладке «Диагностика» выбрать тип подключения и настроить, при необходимости, хост и пароль, нажать кнопку «Старт COM» (рисунок 5.8.1).

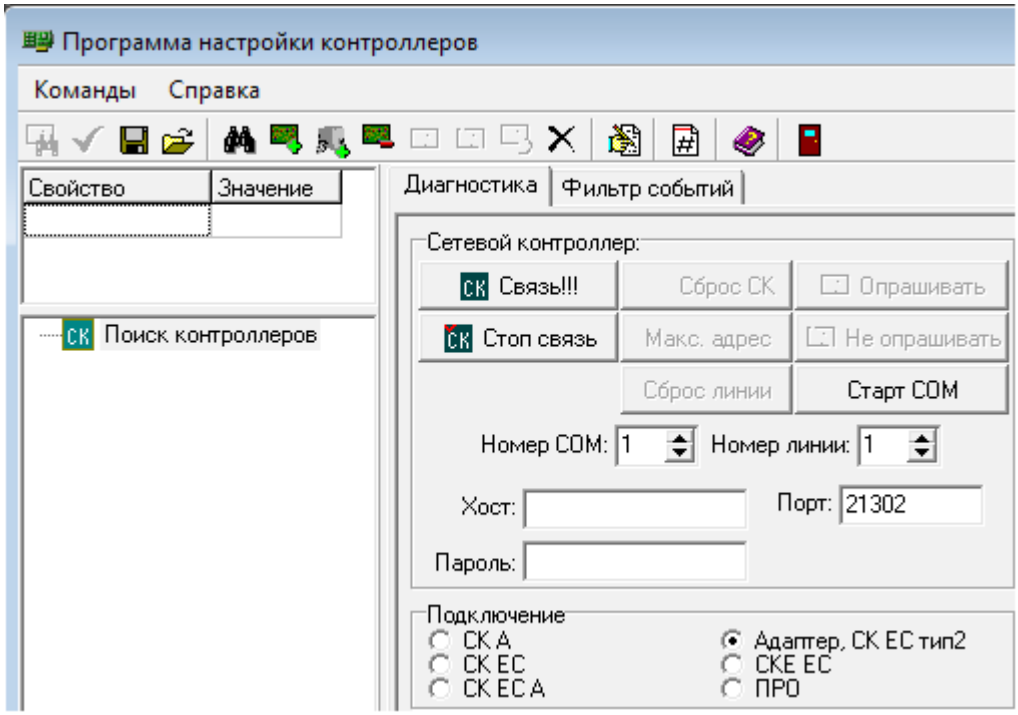



**Рисунок 5.8.1**

3. Установить максимальный адрес, нажав «Макс. адрес», далее нажать «Связь» (рисунок 5.8.2).

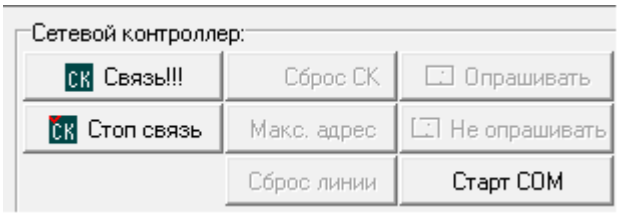



**Рисунок 5.8.2**

4. Нажать - «Добавить контроллер в список» (рисунок 5.8.3).

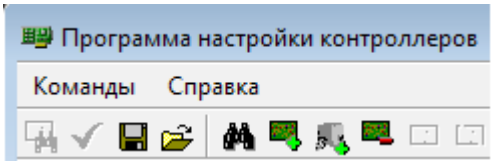



**Рисунок 5.8.3**

5. Ввести адрес контроллера (рисунок 5.8.4).

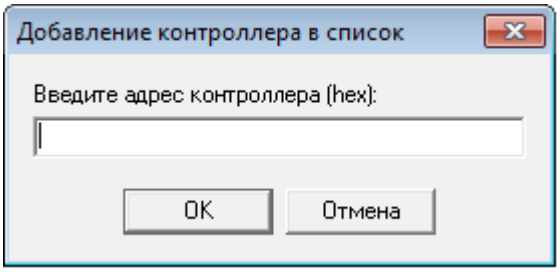



**Рисунок 5.8.4**

6. Выбрать добавленный контроллер и открыть вкладку «Свойства» (рисунок 5.8.5).

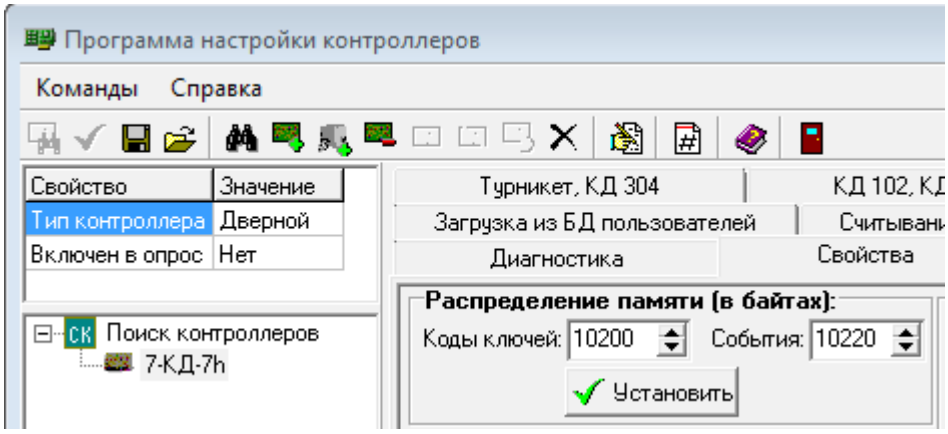



**Рисунок 5.8.5**

7. Увеличить значение «Коды ключей». Например, если необходимо увеличить число ключей, хранящихся в памяти контроллера, до 4000, то значение «Коды ключей» увеличить до 20400. Нажать «Установить» (рисунок 5.8.6).

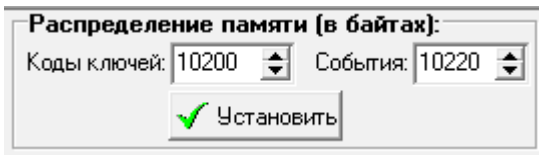



**Рисунок 5.8.6**

При увеличении места в памяти под ключи, уменьшается место в памяти контроллера под события.

**Конфигурирование файла codos.ini.**

1. В корневой папке «ИКБ КОДОС», расположенной, в зависимости от диска установки, находится файл, где настраиваются параметры программы. Открыть: «Диск установки»□«SSA»□«SKD» (рисунок 5.8.7). Файл codos.ini открыть в редакторе «Блокнот».

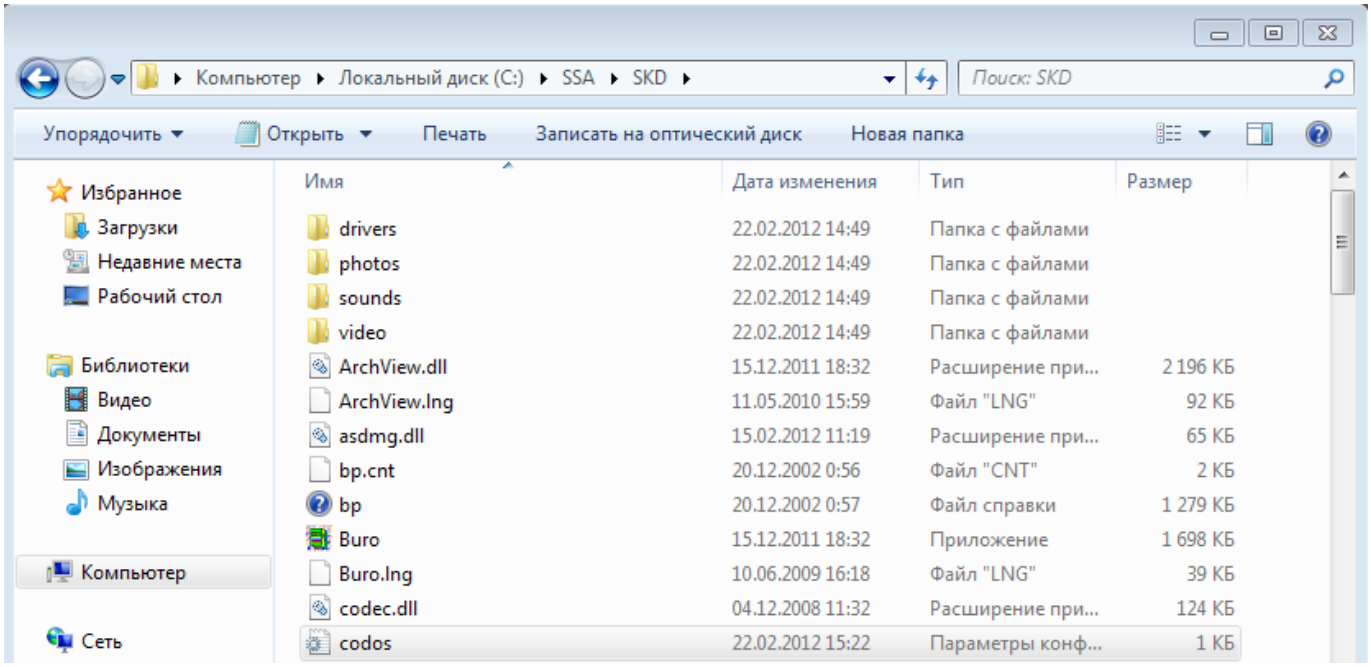



**Рисунок 5.8.7**

2. «CriticalKeyIndex= » - задаёт максимальный индекс ключа, хранящегося в контроллере, по умолчанию 2000. Задать новый индекс в соответствии с требованиями предприятия и сохранить изменения (рисунок 5.8.8). Максимальное значение индекса – 10000. Рекомендуется «CriticalKeyIndex= » задавать несколько большим, чем планируемое число карт в базе. Необходимо учитывать, что при увеличении объема памяти, отводимой под ключи, уменьшается количество памяти под события.

Следует обратить особое внимание на регистр букв, а также на отсутствие пробелов при написании добавляемых строк. При ошибочном вводе изменения учитываться не будут.

3. После того, как изменения были добавлены, файл codos.ini следует сохранить и закрыть. Если сервер ИКБ был запущен, перезапустить его, чтобы изменения в файле codos.ini вступили в силу.

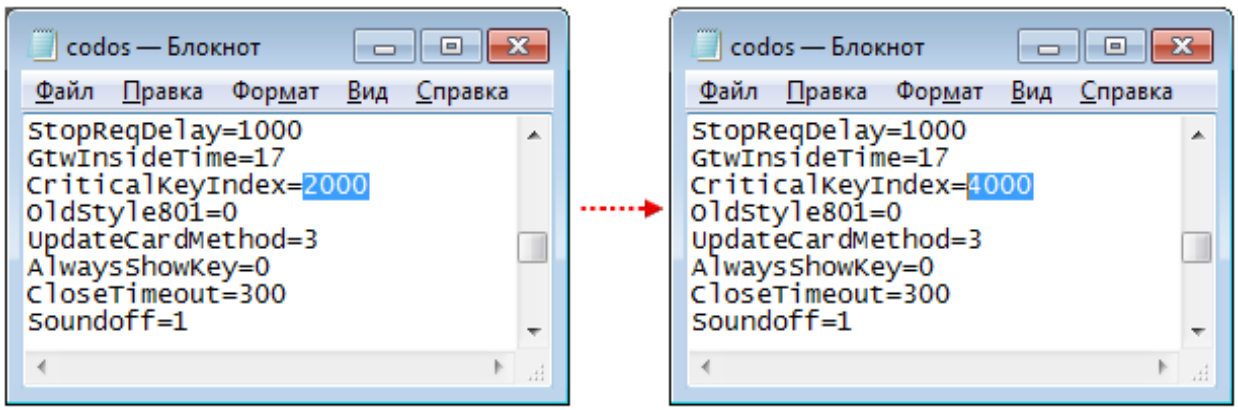



**Рисунок 5.8.8**

### 5.8.2 Использование локальных баз данных

Данную функцию программы рекомендуется использовать, если количество пользователей, хранящихся в базе данных, превышает количество пользователей, которые могут быть записаны в память контролера.

Это может происходить как на крупных объектах, так и в территориально-распределенных системах, состоящих из большого числа сравнительно небольших объектов, объединенных одной базой данных.

Предполагается, что через конкретную точку доступа (дверь, турникет) одновременно не должен быть назначен доступ сразу всем пользователям из базы данных. При этом, в память контроллера записываются коды карт только тех пользователей, которым разрешен доступ через точку или точки доступа, которыми управляет данный контроллер.

Программа хранит данные о картах, которые в данный момент находятся в контроллере. Когда через точку доступа впервые проходит новый пользователь, имеющий право на проход через неё, информация о его карте записывается на свободное место, а при его отсутствии перезаписывает одну из существующих карт, которая, таким образом, удаляется из контроллера, но будет храниться в базе данных. Критерием выбора карты для замещения является наиболее старое время прохода, т.е. при добавлении новой карты в случае отсутствия памяти в контроллере из него будет удалена карта с наиболее старым временем прохода.

При проходе пользователя через контроллер с картой, кода которой нет в памяти контроллера, происходит запрос о наличии этого кода в базе данных. В случае положительного ответа его карта прописывается в память контроллера. С точки зрения пользователя, поведение контроллера при первом поднесении карты идентично поведению при поднесении неизвестной карты - считыватель будет мигать красным цветом. При повторном и любом последующем поднесении карты проход будет разрешён или запрещён согласно заданным владельцу карты в системе правам доступа.

Часть пользователей может быть всегда прописана в контроллеры. Такие карты никогда не перезаписываются новыми и всегда находятся в памяти контроллера. Чаще всего в этот список заносятся карты руководящего состава организации и сотрудников, отвечающих за поддержание систем жизнеобеспечения.

Для настройки локальных баз данных в файле codos.ini в разделе LocalIndexes существуют следующие параметры:

Enabled – включение (параметр равен 1) или отключение (параметр равен 0) локальных баз данных;

MinLocalIndex – определяет количество карт доступа, заблокированных от удаления из памяти контроллера;

MaxLocalIndex – значение, обозначающее верхнюю границу памяти контроллера, т.е. это верхний предел массива данных карт в контроллере.

Перед включением функции локальных баз данных необходимо произвести перераспределение памяти контроллеров (см.п.5.8.1) с учетом максимального ее использования. Все контроллеры доступа в системе должны иметь одинаковые настройки распределения памяти. При включении функции локальных баз данных параметр CriticalKeyIndex не используется.

Изменения в файле codos.ini необходимо произвести на всех рабочих местах, где установлено ПО «ИКБ КОДОС» (программа «Сервер ИКБ», «Администратор ИКБ»).

Пример настройки:

Например, существует организация (всего 15 000 сотрудников), имеющая головной офис в Москве (26 точек доступа) и 84 филиала по территории страны (по 2 точки доступа в каждом). В качестве контроллеров доступа используются контроллеры EC-202. В головном офисе находится сервер ИКБ «КОДОС», в каждом филиале установлено удаленное рабочее место (ПО «Администратор ИКБ»).

Порядок настройки:

Через программу ContrTools производим перераспределение памяти всех (110 шт.) контроллеров доступа EC-202. Под коды ключей отводим максимально-возможное значение (51000 байт (10200 ключей)), под события назначаем 7154 байт памяти (1022 события). Нужно помнить, что у контроллеров серии RC в 2 раза меньше памяти, поэтому при их использовании необходимо назначить следующие значения: 25500 байт под коды ключей, 3066 байт под события, что даст возможность хранить 5100 ключей и 432 события.

В файле codos.ini всех рабочих мест (в нашем случае 85 рабочих мест) устанавливаем следующие значения для параметров:

[LocalIndexes]

Enabled=1

MinLocalIndex=300

MaxLocalIndex=10000

Значение MinLocalIndex выбирается исходя из конкретной ситуации.

При запуске программы на вкладке «Пользователи» появится новая колонка «Позиция карты». У всех пользователей, карты которых заблокированы от удаления из памяти контроллера, значение в столбце «позиция карты» выделено цветом.

При необходимости можно вручную регулировать привилегированные карты. Для исключения карты пользователя из списка привилегированных необходимо в карточке пользователя снять галочку в параметре «поместить в начало списка». А для пользователя, чью карту необходимо заблокировать от удаления галочку нужно установить.

ПРИМЕЧАНИЕ

1. Функция локальных баз данных работает только с СУБД Firebird.

2. Действия по блокировке\разблокировке карточки от удаления расцениваются программой как вновь выданные карты. Все события по этим пользователям, которые произошли ранее, будут недоступны.

## 5.9 Настройка модуля «владельцы»

Модуль «Владельцы» предназначен для регулирования доступа к ресурсам ИКБ «КОДОС» при использовании несколькими фирмами (владельцами), либо разных подразделений одной организации, единого сервера.

Например, в офисном здании установлен единый интегрированный комплекс безопасности «Кодос». Помещения в здании арендуют несколько фирм, которые могут периодически меняться, а так же может изменяться площадь помещений, арендуемых данными фирмами. В этом случае в каждой фирме будет установлен свой АРМ, на котором будут отображаться только «свои» сотрудники и «своё» оборудование. В то же время владелец здания (администратор системы, служба безопасности) имеет возможность просматривать и управлять всем оборудованием Системы.

Создание списка фирм-владельцев производится в программе «Конфигуратор». Для этого необходимо нажать кнопку Редактировать список фирм-владельцев (рисунок 5.9.1).

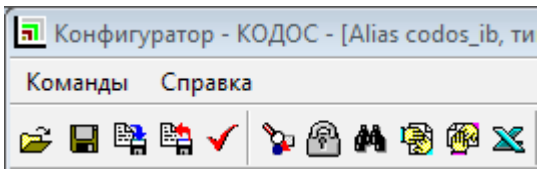



**Рисунок 5.9.1**

В открывшемся окне Редактирование списка владельцев (рисунок 5.9.2) возможно добавить, переименовать или удалить имеющиеся фирмы-владельцы.

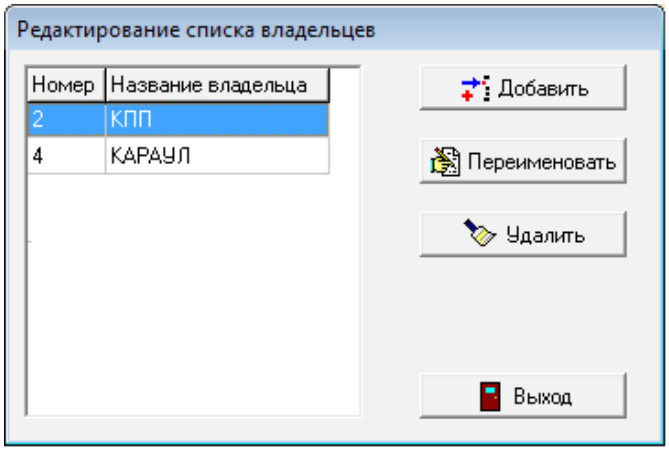



**Рисунок 5.9.2**

В свойствах оборудования (двери, датчики, видеоисточники) необходимо указать, кто является его «владельцем». Для каждой двери/датчика/устройства владелец устанавливается индивидуально.

ПРИМЕЧАНИЕ — В программе существует владелец «не определен». Его нельзя удалить. Наличие данного владельца позволяет «скрывать» оборудование и пользователей от всех операторов. Оператору admin этот владелец доступен по умолчанию.

Если в Конфигураторе у какого-либо элемента шлюза установить владельца, то такое же имя будет установлено и у всех других элементов шлюза - кнопок и дверей. Таким образом, для шлюза достаточно при конфигурировании установить владельца только на одном элементе.

Не рекомендуется устанавливать разных владельцев для дверей контроллера, сконфигурированного для работы в двухдверном режиме.

Для настройки прав операторов, предварительно необходимо создать список операторов, как указано в п.4.1.

Администратор системы (пользователь – admin) по умолчанию имеет права доступа на все элементы системы (двери, датчики, устройства, пользователей), независимо от их принадлежности к тому или иному владельцу.

Для настройки прав операторов по отношению к фирмам-владельцам нажать кнопку Настройка прав в окне Список операторов системы (рисунок 5.9.3).

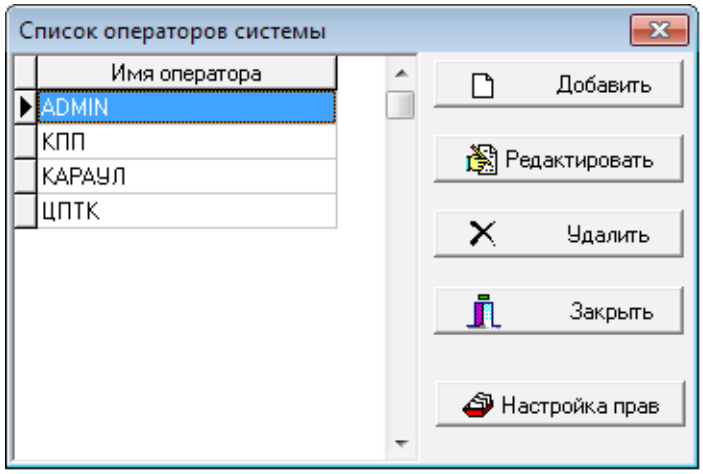



**Рисунок 5.9.3**

Окно настройки прав доступа в модуле «Владельцы» состоит из двух основных областей: области списка владельцев и области списка операторов (рисунок 5.9.4).

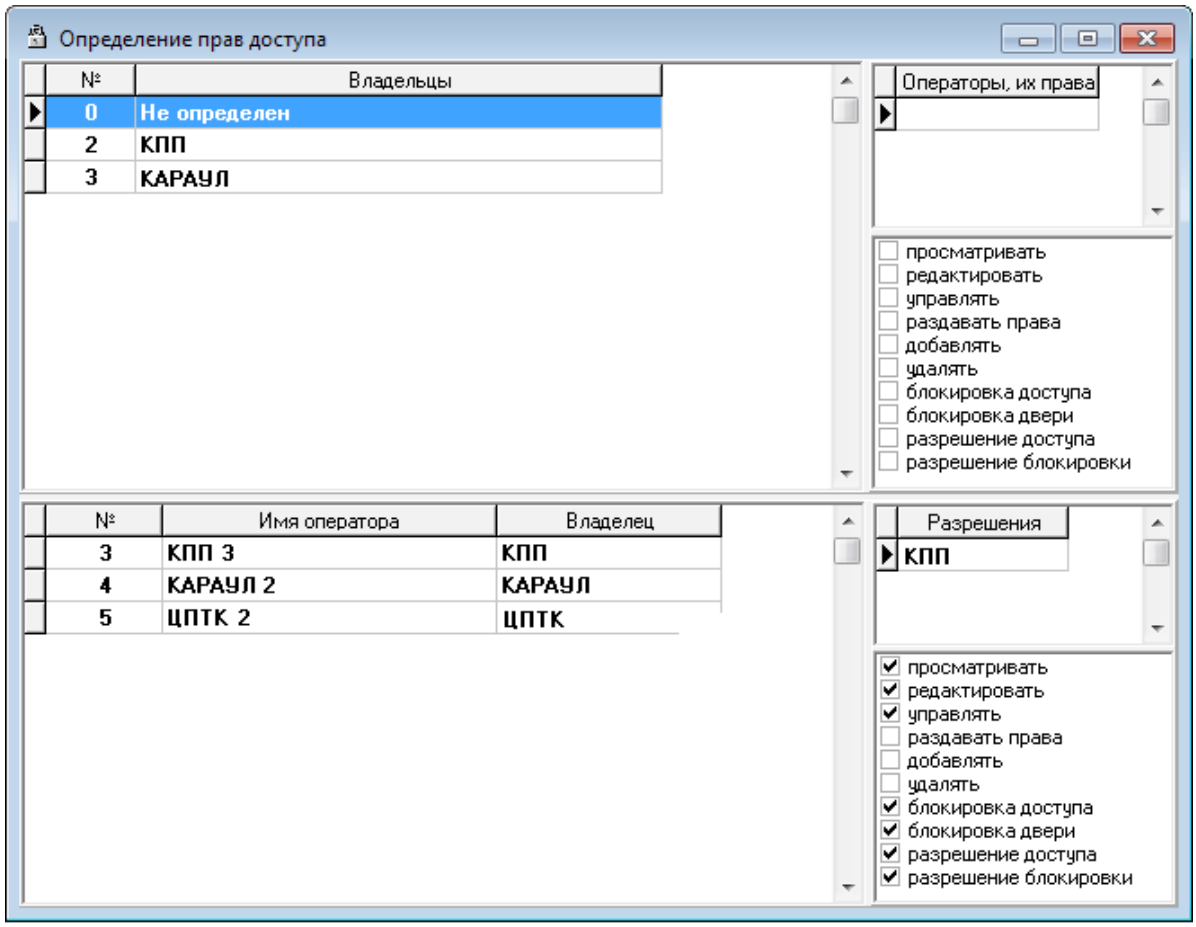



**Рисунок 5.9.4**

Область списка владельцев позволяет устанавливать права операторам для работы с разрешенными «владельцами».

Область списка владельцев делится на две части: непосредственно список владельцев (левая часть) и список операторов для текущего (выделенного) владельца (правая часть). Двойной щелчок по строке с названием владельца (фирмы), приводит к открытию окна Назначения прав для операторов на владельца (рисунок 5.9.5). Для текущего владельца можно добавить любого оператора и установить ему индивидуальные права. Можно так же удалить любого оператора из списка.

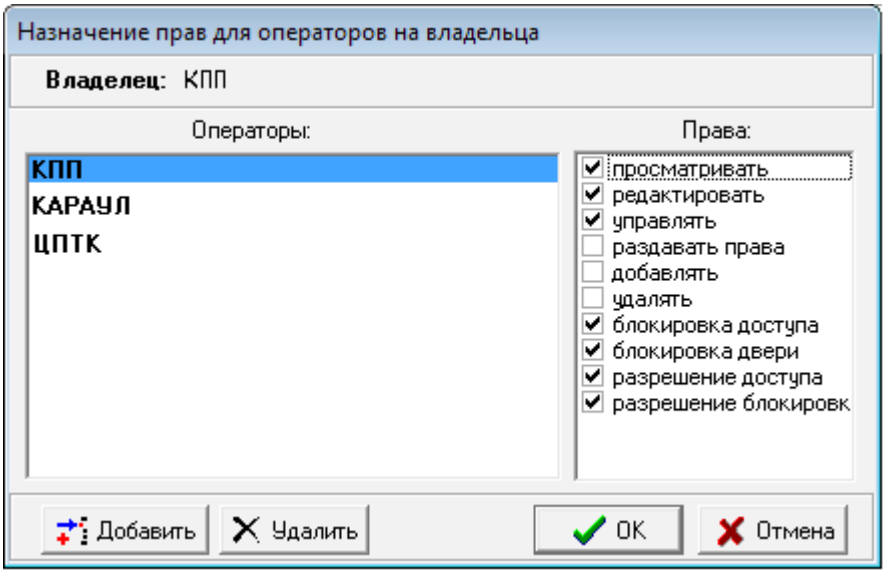



**Рисунок 5.9.5**

Права просматривать, редактировать, добавлять, удалять распространяются на действия с картами пользователей. Если при работе с ИКБ используется модуль «Владельцы», то права, настроенные в этом модуле являются приоритетными перед правами операторов сервера ИКБ в случае их совпадения. При этом некоторые права модуля «Владельцы» являются своего рода «масками» прав, допускающими оператору совершить то или иное действие в рамках прав его операторской записи. Т.е., если, например, у текущего оператора по правам модуля «Владельцы» есть право «редактировать», то дальше вступают в силу права записи оператора сервера: если есть право редактировать карту, то он сможет им воспользоваться, если есть право редактировать гостевую карту, то оператор так же может им воспользоваться. Однако, если по модулю «Владельцы» у текущего оператора нет права на редактирование, то он не сможет редактировать тот или иной вид карт, даже если такое право предоставлено ему в правах операторской учётной записи.

Право управлять разрешает производить операции с оборудованием системы. Например, ставить и снимать датчики с охраны, открывать двери и .т.д.

Область списка операторов (рисунок 5.9.5) показывает права операторов для работы с определенным владельцем.

Оператору можно назначать права для работы с несколькими владельцем. Список всех разрешенных «владельцев» для текущего оператора показывается в графе «разрешения» правой части области списка операторов (рисунок 5.9.5).

В процессе работы, при добавлении нового пользователя, последний будет добавляться в базу данных по умолчанию с признаком того владельца, значение которого указано для данного оператора в столбце Владелец области списка операторов (рисунок 5.9.5). Для изменения владельца необходимо произвести двойной щелчок на нужной записи в строке списка операторов окна определения прав доступа, и в раскрывшемся окне Изменение владельца (рисунок 5.9.6) задать нового владельца оператору.

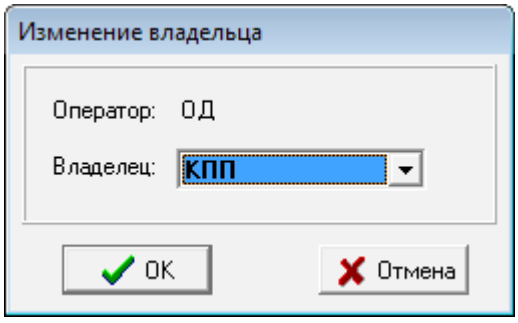



**Рисунок 5.9.6**

При входе в программу, под каким либо оператором, отображается только та информация, на которую у данного владельца есть права (в свойствах оборудования или пользователя установлен тот же самый владелец), а также прав самого оператора для работы с данным владельцем.

При создании групп дверей или групп датчиков, она создается с признаком того владельца, что и текущий оператор. Это поле не редактируется операторами, кроме администратора системы (admin).

При добавлении в группу дверей (датчиков) оператору доступен только список тех дверей (датчиков), на которые у него есть разрешения. Если датчик уже включен в группу, то при добавлении датчиков в группу, в списке выбора он не отображается.

# 6 РАБОТА И ОБСЛУЖИВАНИЕ ПРОГРАММЫ

## 6.1 Логика обработки прохода пользователя

Пользователи идентифицируются по их кодоносителям при помощи считывателей. От считывателя в контроллер поступает код поднесенного кодоносителя. Номер считывателя (1 или 2) позволяет контроллеру определить, поднесен кодоноситель со стороны входа или выхода – в однодверном режиме работы, или же на входе какой из дверей (первой или второй) – в двухдверном режиме.

После приема кода от считывателя контроллер определяет соответствующие пользователю права и принимает решение о доступе. Если пользователю с этим кодом в данный момент времени доступ разрешен, то контроллер открывает замок двери, соответствующей считывателю, от которого принят код. Разрешение или запрет доступа индицируется светодиодом считывателя.

Права доступа в системе «КОДОС» настраиваются чрезвычайно гибко. Это достигается использованием следующих понятий и параметров:

- таблица пользователей;
- уровень доступа;
- таблица уровней доступа;
- временные зоны;
- режим запрета повторного прохода;
- режим запрета выхода.

Контроллер доступа при принятии решения о разрешении прохода проверяет несколько условий:

Первое условие, необходимое для разрешения доступа, – это наличие кода кодоносителя в памяти контроллера. Если код контроллеру неизвестен (кодоноситель не прописан в памяти), то контроллер отказывает в доступе обладателю этого кодоносителя (сообщение – «на входе неизвестный код»).

Если код присутствует в памяти контроллера (кодоноситель прописан в памяти), то проверяется второе условие – присутствие уровня доступа этого кодоносителя в таблице разрешенных уровней, действующих для данной двери в данный момент времени. Кодоносителю с уровнем доступа, отсутствующим в таблице разрешенных, контроллер в доступе отказывает (сообщение- «запрет входа»).

Уровень доступа – это число в диапазоне от 1 до 32, которое ставится в соответствие каждому коду кодоносителя, хранящемуся в памяти контроллера. В отличие от кода, уровень доступа не является собственной характеристикой кодоносителя, а задается при занесении кода в память контроллера и в дальнейшем может быть изменен. Коды кодоносителей вместе с соответствующими уровнями доступа заносятся в таблицу пользователей контроллера.

Третье условие, необходимое для разрешения доступа, – отсутствие ограничений по режиму запрета повторного прохода. Контроллер отказывает в доступе, если для считанного кодоносителя действует режим запрета повторного прохода и в предыдущий раз проход с ним осуществлялся в том же направлении (событие– «попытка повторного входа»).

Режим запрета повторного прохода в одном направлении может быть включен или выключен. Когда режим запрета повторного прохода для какой-либо двери включен, через эту дверь запрещается с одним кодоносителем два раза подряд входить или два раза подряд выходить. Таким образом, пользователь сможет войти в дверь, только если ранее он из нее выходил, а выйти – только если ранее входил.

Когда режим AntiPassBack включен, ограничения действуют не для всех пользователей, а лишь для тех, чьи уровни доступа присутствуют в таблице запрета повторного прохода. Это позволяет выделить привилегированных пользователей (гостей, руководство) или тех сотрудников, у кого работа связана с частыми входами-выходами, чтобы избавить данных пользователей от неудобств, вызванных необходимостью обязательно подносить кодоноситель к считывателю при каждом входе и выходе (даже если дверь уже открыта другим пользователем).

Когда кодоноситель подносится к считывателю ВЫХОД, то проверяется еще одно, четвертое условие – отсутствие запрета на выход для считанного кодоносителя. Режим запрета выхода может быть включен или выключен. Если он включен, то запрещается выход тем пользователям, уровни доступа которых находятся в таблице запрета выхода (сообщение-«запрос на выход» ).

ПРИМЕЧАНИЕ – В программном обеспечении интегрированного комплекса безопасности «ИКБ КОДОС» событие «Запрет выхода» трактуется как «Запрос на выход». Предполагается, что оператор (охранник), увидев сообщение о запросе на выход, может разблокировать дверь с компьютера – и тогда в системе будет зафиксировано событие "Выход с ключом" пользователя, подносившего кодоноситель

Выполнения всех четырех описанных условий достаточно для разрешения доступа. Однако гибкость системы этим не исчерпывается: выполнение второго из условий зависит от момента времени, в который осуществляется попытка доступа.

Контроллер оперирует восемью временными зонами. Каждая временная зона состоит из восьми временных интервалов. Интервал считается активным, если выполнены два условия:

- текущий день недели отмечен флагом для данного интервала.
- текущее время («часы : минуты») попадает между началом и окончанием этого интервала;

Рассмотрим, например, интервал с 9:00 до 12:00, для которого установлены флаги Пн, Ср, Пт. Если сейчас 10:30 и сегодня среда, то данный интервал активен, если же сегодня вторник, то – нет.

Если в данный момент времени хотя бы один интервал временной зоны активен, то эта временная зона также считается активной.

С каждой временной зоной сопоставляется таблица уровней доступа. Если временная зона активна, то разрешены все уровни доступа, входящие в ее таблицу. Если в какой то текущий момент времени активны несколько временных зон, то текущая таблица доступа содержит все уровни доступа, разрешенные для активных временных зон в рассматриваемый момент времени.

Некоторое исключение из этого правила составляет доступ в праздничные дни. Флаг, соответствующий праздничным дням, перекрывает действие флагов, соответствующих дням недели.

Таким образом, если некоторый интервал активен, например, по средам, но не активен по праздникам, то он не активен в среду, являющуюся праздничным днем. Соответственно, уровни доступа, которые должны быть разрешены по средам, но не должны быть разрешены по праздникам, контроллер не считает разрешенными.

Если ни одна из временных зон в настоящий момент не активна, то права доступа контроллер определяет по таблице доступа «по умолчанию». Та же таблица применяется, если режим использования временных зон для доступа отключен.

ПРИМЕЧАНИЕ – В двухдверном режиме работы контроллера уровень доступа пользователя одинаков для обеих дверей. Таблицы разрешенных уровней доступа для первой и второй дверей могут быть различными. Режимы запрета повторного прохода и запрета на выход при таком подключении кон-троллера должны быть отключены.

Нормальной считается нижеприведенная последовательность событий:

- Пользователь подносит разрешенный кодоноситель к считывателю при закрытой двери.
- Контроллер фиксирует событие «Считывание ключа на входе (выходе)» и разблокирует замок (подает напряжение на клеммы, если замок прямого типа или снимает, если инверсного) на время, заданное параметром «Длительность открытия замка».
- Пользователь открывает дверь в течение вышеуказанного интервала времени и проходит через нее. Обнаружив открытие двери (размыкание дверного датчика), контроллер фиксирует событие «Вход (выход) с ключом» пользователя с тем кодоносителем, который перед этим был считан.
- Пользователь закрывает дверь за время, не превышающее длительности открытия замка. Контроллер при этом фиксирует событие «Дверь закрыта».

Если время длительности открытия замка истекло, а дверь до этого момента не была закрыта, то контроллер фиксирует событие «Дверь оставлена открытой».

Если открытия двери за период, равный времени длительности открытия замка, так и не произошло, то событие «Вход (выход) с ключом» не фиксируется, а замок остается разблокированным в течение данного интервала времени.

**Настройка прохода пользователя**

Для выполнения прохода пользователю через дверь в программе «ИКБ КОДОС» необходимо, чтобы выполнялись следующие условия:

- наличие флажка рядом с описанием этой двери в поле «Разрешен доступ», в окне редактирования личных данных о пользователе. Пока это условие не будет выполнено, сотрудник не сможет пройти через данную дверь, несмотря на другие настройки, дающие ему туда доступ.
- уровень доступа, назначенный пользователю, должен быть прописан как разрешенный в таблице доступа по временным зонам этой двери. Для настройки прохода пользователей по временным зонам следует нажать название временных зон и установить для каждой из них флажки для тех уровней доступа пользователей, которые должны иметь доступ через данную дверь в течение этой временной зоны.
- должна быть активна хотя бы одна временная зона, в которой разрешен уровень доступа, назначенный этому пользователю.

- срок действия карты пользователя на данный момент не истек.

**Организация проходов посетителей (гостей)**

- определить специальный уровень доступа для гостевых карт. Например, если сотрудники имеют уровень доступа «1», то для гостевых карт установить уровень доступа «2». Этот уровень доступа должен быть уникальным и не использоваться другими сотрудниками.
- для дверей, через которые можно проходить с гостевыми картами, установить разрешенный уровень доступа (например, «2») – поставить флажок у номера уровня доступа. Для других уровней доступа флажки менять не требуется (рисунок 6.1.1).

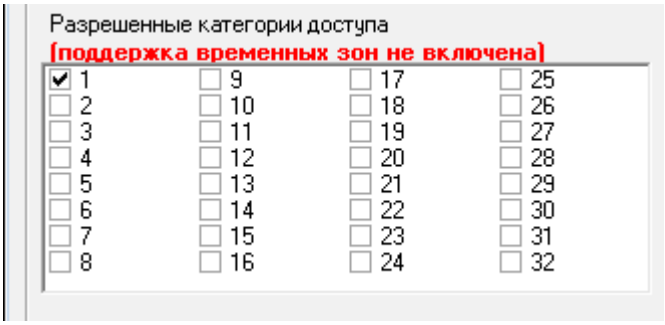



**Рисунок 6.1.1 –**

- если требуется, чтобы выход по гостевым картам происходил через одну дверь, необходимо задать ограничения, нажав кнопку «По уровням доступа» в окне «Настройка двери». После чего появится окно «Дополнительные ограничения доступа». В этом окне для уровня доступа гостей (например, «2») установить флажок – запретить выход через эту дверь. Кроме того, необходимо установить контроль за ограничением выхода – установить флажок «Ограничение выхода» в окне «Настройка двери». Ограничение выхода необходимо применять, в основном, для сохранности кодоносителей. При использовании картоприемника возвращение кодоносителей пользователями происходит автоматически.
- действия п. 2 – 4 выполнить для всех временных зон выбранной двери.

## 6.2 Обслуживание базы данных

Для поддержания высокой надежности и оперативности работы используемой СУБД необходимо проводить периодическое обслуживание базы данных. Рекомендуется, с периодичностью, определяемой пользователем, производить выгрузку событий из базы данных, проверку и резервное копирование БД. При обнаружение ошибок производится восстановление БД из резервной копии:

Периодичность проведения данных действий выбирается исходя:

- из размера системы на объекте
- количества пользователей (карт доступа), зарегистрированных в системе
- интенсивности использования системы

### 6.2.1 Выгрузка событий из БД

В ИКБ КОДОС существует возможность производить:

- выгрузку  событий из базы данных и сохранение выборки в виде отдельного файла
- удалять из архива текущие события
- удалять из архива выбранные события

Для того, чтобы выгрузить события из БД необходимо:

1. Во вкладке «События в системе» нажать кнопку «Архив событий». В появившемся окне «Архив событий» нажать кнопку «Архив». В списке выбрать «Выгрузить архив» (рисунок 6.2.1).

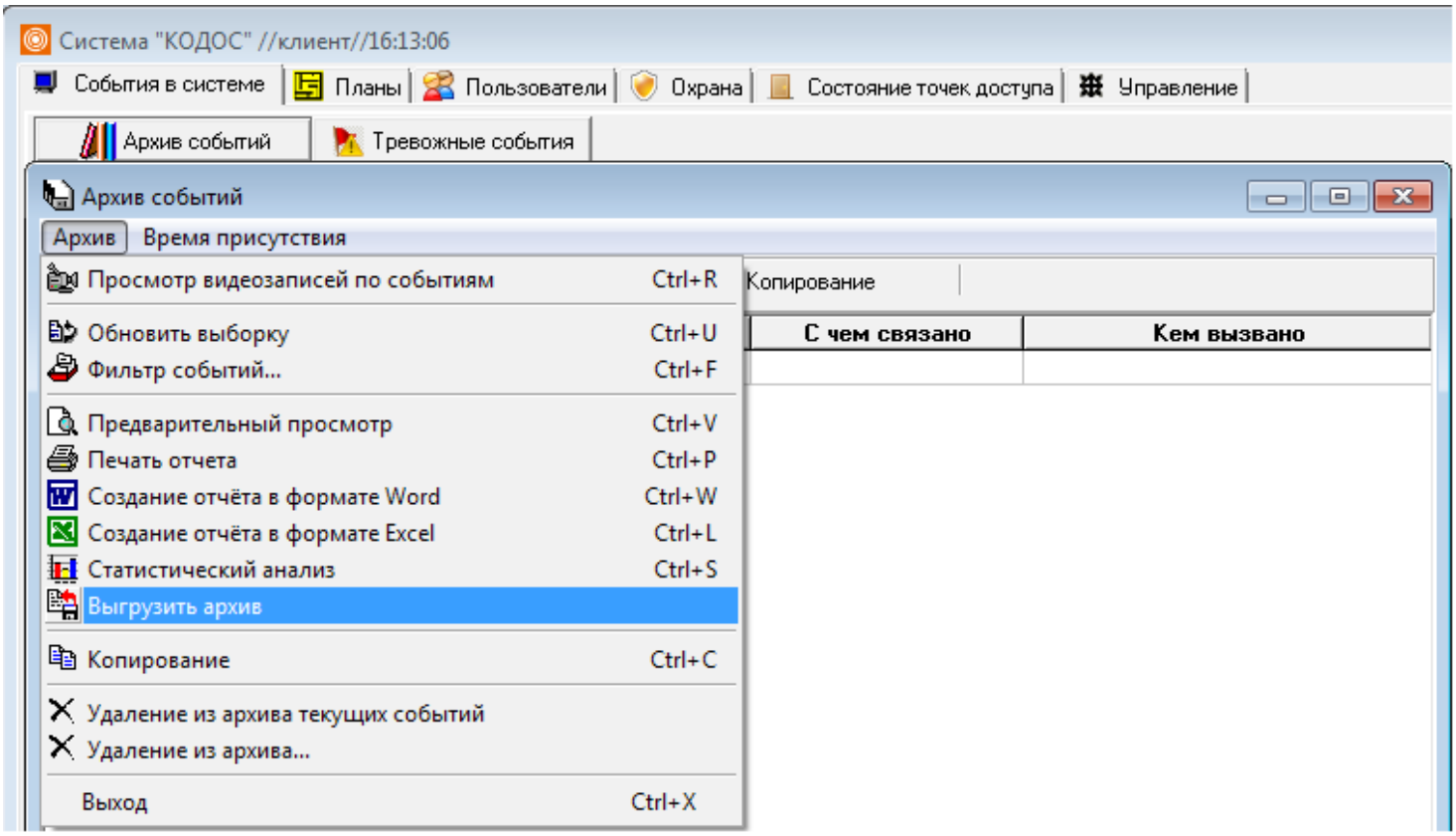



**Рисунок 6.2.1 –**

2. В окне «Выгрузка архива» (рисунок 6.2.2) в панели «Период» задать период выгружаемого архива. В панели «Действия над таблицами» выбрать «Создать и перенести». В строке «Описание» задать имя выгружаемого файла. В строке «Расположение» указать, куда сохранить указанный файл. Для этого нажать кнопку «Обзор» и в появившемся окне «Обзор папок», (рисунок 6.2.2) выбрать место сохранения файла. После указания места сохранения нажать кнопки «ОК». Начнется процесс выгрузки архива (рисунок 6.2.3).

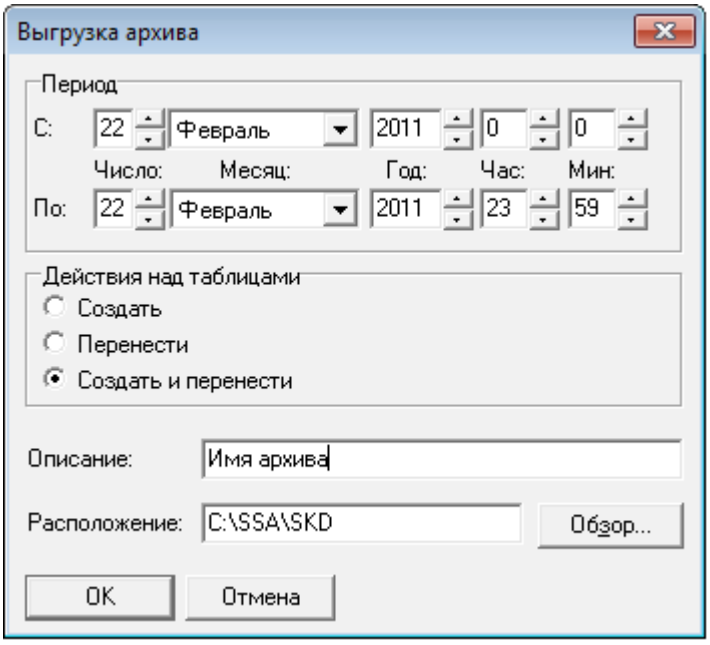



**Рисунок 6.2.2 –**

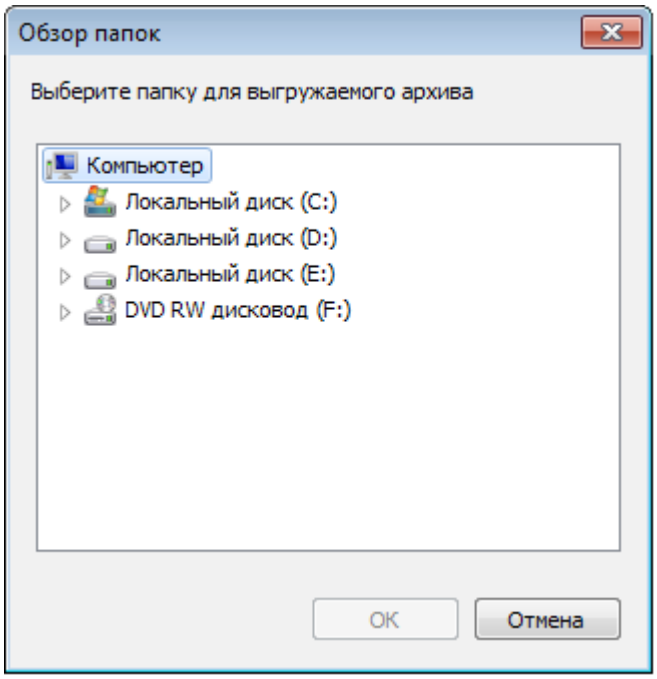



**Рисунок 6.2.3 –**

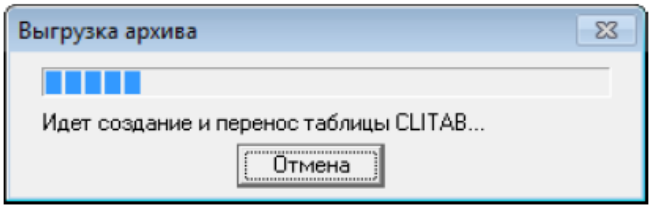



**Рисунок 6.2.4**

3. Выгруженный архив можно просмотреть в программе MS Access или аналогичной. После окончания процесса выгрузки архива будет предложено удалить выгруженный архив из СУБД. Нажать кнопку «Да» (рисунок 6.2.6).

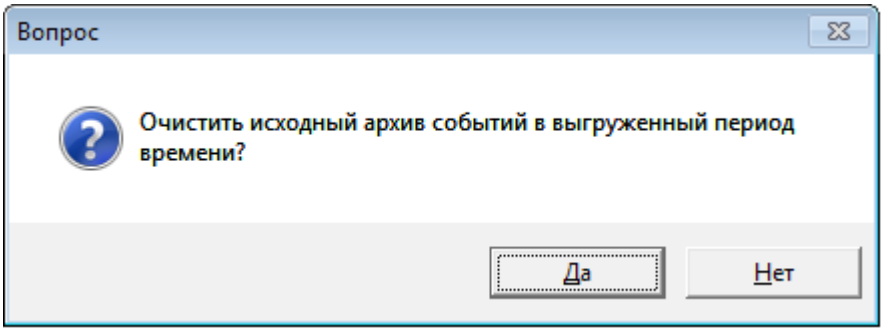



**Рисунок 6.2.5 –**

4. Архив будет удален из СУБД, появится уведомление (рисунок 6.2.6). Нажать «ОК».

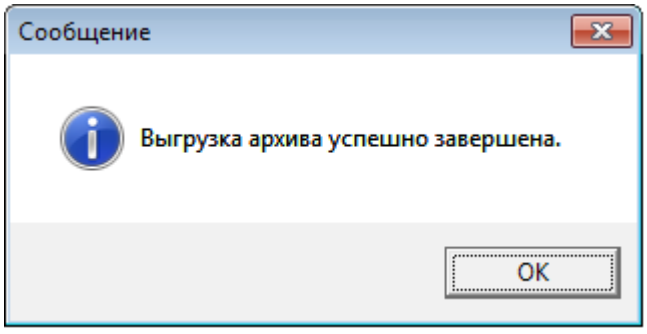



**Рисунок 6.2.6 –**

После проведения выгрузки событий рекомендуется провести процедуры резервного копирования и восстановления БД

### 6.2.2 Проверка, копирование и восстановление бд

Проведение работ по проверке, резервному копированию и восстановлению базы данных должно осуществляться сотрудниками, имеющими представление о работе СУБД, используемой в данной системе.

ВНИМАНИЕ! Перед проведением копирования необходимо обязательно отключать все Автоматизированные рабочие места (АРМ) системы, работающих с базой данной и отключить ПО Кодос Сервер ИКБ, чтобы к рабочей базе данных не было обращений, иначе при копировании может быть получен испорченный файл базы.

ИКБ КОДОС поддерживает работу следующих СУБД: Firebird, Oracle и MS SQL

В Приложении Г приведена последовательность действий при проведении резервного копирования базы данных средствами FireBird.

В Приложении Д приведена последовательность действий при проведении восстановления базы данных средствами FireBird.

В Приложении Е приведена последовательность действий при проведении восстановления базы данных сразу после резервного копирования.

В Приложении Ж приведена последовательность действий при проведении проверки базы данных средствами FireBird.

## ПРИЛОЖЕНИЕ А Глоссарий

Администратор системы – специалист, осуществляющий установку, настройку и техническое обслуживание системы. Имеет наивысший приоритет доступа в системе.

Активный элемент экранной формы – текущий, выделенный элемент.

Артефакты – искажения изображения, звука.

Архив видеоканала – файлы с записанной видео- и аудиоинформацией, элемент дерева конфигурации видеоканалов.

Видеоархив – запись видеоизображений хранящихся в памяти компьютера.

Видеоканал – оборудование (плата видеоввода, мультиплексор, сеть), являющееся источником видеосигнала, а также элемент древовидной структуры, служащий для настройки соответствующего оборудования.

Видеоокно – окно, в котором отображается видеоинформация.

Деинсталляция – удаление программного обеспечения.

Детектор движения – программный модуль, включающий видеозапись при обнаружении движения.

Дочерний элемент – подчиненный элемент в дереве каталога.

Инсталляция – установка программного обеспечения.

Клиент – компьютер и ПО, принимающее информацию по локальной сети от сервера.

Ключ аппаратной защиты – устройство, предназначенное для защиты программы на аппаратном уровне от несанкционированного копирования и эксплуатации.

Кодек – кодировщик/декодировщик данных.

Кольцевая запись – способ записи, когда новая запись замещает старую.

Коммутация аудиоканала – включение звукового сопровождения изображения, поступающего с видеоканала.

Контекстное меню – меню, вызываемое щелком правой клавиши мыши.

Контекстная справка – раздел справочной системы программы.

Конфигурация архивов – настройка видеоархивов. Для каждой конфигурации каналов ПК может быть сформирована только одна конфигурация архивов.

Конфигурация видеоокон – элемент конфигурации видеоокон (каналов и архивов). Для каждой конфигурации каналов ПК может быть сформировано несколько различных конфигураций видеоокон. В каждый момент времени только две из них являются текущими: одна для основного окна программы, другая – для окна «Видеоархивы».

Конфигурирование каналов ПК – выполненные на компьютере системы настройки видеоканалов, конфигурации видеоокон, конфигурация архивов, настройки панелей инструментов и др. Для каждого ПК может быть сформировано несколько различных конфигураций каналов. В каждый момент времени только одна является текущей.

Конфигурация системы – оборудование, интерфейс и настройки устройств, входящих в состав системы.

Корневой элемент – первый элемент в дереве элементов, все остальные элементы для него являются дочерними.

ЛВС – локальная вычислительная сеть.

Лицензия – право на использование компонентов системы.

Менеджер лицензий – программа, предназначенная для активизации модулей ПО в соответствии с лицензией.

Мультиплексор – электронное устройство, переключающее видеоканалы; тип видеоканала.

Название видеоканала – идентификатор (имя) видеоканала.

Оператор – Пользователь системы.

Главное (верхнее) меню – меню (обычно располагается сразу под заголовком окна программы), где собраны все основные команды, выполняемые программой.

Панель видеоокна – образ, служащий для задания положения и размеров видеоокон при конфигурировании.

Панель инструментов – экранная форма, служащая для размещения кнопок, полей ввода и т.п., предназначенных для выполнения определенных функций программы.

Пароль пользователя – запись, служащая для идентификации пользователя.

Период обновления видеоканала – промежуток времени, по прошествии которого система обновляет связь с источником видеосигнала.

ПК – персональный компьютер.

Пиксель – минимальная единица изображения на экране монитора. В записи «384x288» первое число означает число точек по горизонтали, второе – по вертикали.

Планировщик – программный модуль для управления автоматическим включением/выключением записи по расписанию.

Плата видеоввода – устройство видеозахвата; тип видеоканала.

Пользователь – оператор, осуществляющий работу с программным обеспечением. Идентифицируется при помощи ввода имени и пароля.

Предтревожная запись – режим, позволяющий включать в видеозапись некоторое число кадров, предшествующих тревоге.

Рабочая директория программы – место размещения загрузочного модуля программы и других вспомогательных файлов.

Рабочая область окна – часть окна программы, внутри которой располагаются вторичные окна.

Разрядность – параметр, характеризующий число различаемых уровней.

Регистрация пользователя – вход в систему путем ввода имени и пароля пользователя.

Сеть – несколько компьютеров и средства их связи; тип видеоканала.

Сетевая камера – сетевое устройство видеоввода, тип видеоканала.

Сервер – компьютер, к которому подключено оборудование системы, и соответствующее ПО, управляющее работой этого оборудования.

Система – совокупность оборудования и программного обеспечения «ИКБ КОДОС».

СКУД – система контроля и управления доступом.

Тип видеоканала – либо плата видеоввода, либо мультиплексор, либо сеть.

Текущий объект (окно, конфигурация и др.) – активный объект, с которым работает оператор. В списке аналогичных ему элементов обычно выделяется цветом, фоном.

Текущий пользователь – пользователь, зарегистрированный по определенному имени и паролю, и управляющий работой компьютера.

Устройство аудиозахвата – устройство ввода звуковой информации.

Устройство аудиовоспроизведения – устройство вывода звуковой информации.

Частота дискретизации – количество минимальных единиц (дискрет) в единицу времени, при преобразовании аналогового сигнала в цифровой.

Шум – неинформативная часть сигнала, отделяемая от информативной части с помощью фильтров.

## ПРИЛОЖЕНИЕ Б Пример создания правила

Допустим, на объекте имеются два помещения, которые следует ставить на охрану по окончании рабочего дня. Окончание работы – в 18.00. Выход из помещения 1 осуществляется через дверь 1, а из помещения 2 – через дверь 2. Руководство считает необходимым настроить систему доступа таким образом, чтобы, как только все сотрудники покинут помещения 1 и 2, они автоматически ставились бы на охрану.

Администратор Системы для решения поставленной задачи должен настроить временную зону (например, номер 6) так, чтобы ее действие охватывало период, когда в охраняемых помещениях никто не должен находиться (например, с 17:45 до 7:45). Настройка временных зон описана в п.4.2. «Настройка временных зон". В базе данных Системы должен храниться список всех сотрудников (и их кодоносителей) с указанием дверей, доступных для их прохода.

Ниже приводится описание дальнейших действий администратора Системы по формированию правил, решающих поставленную задачу.

1. Нажмите экранную кнопку "Правила", расположенную во вкладке "Управление".

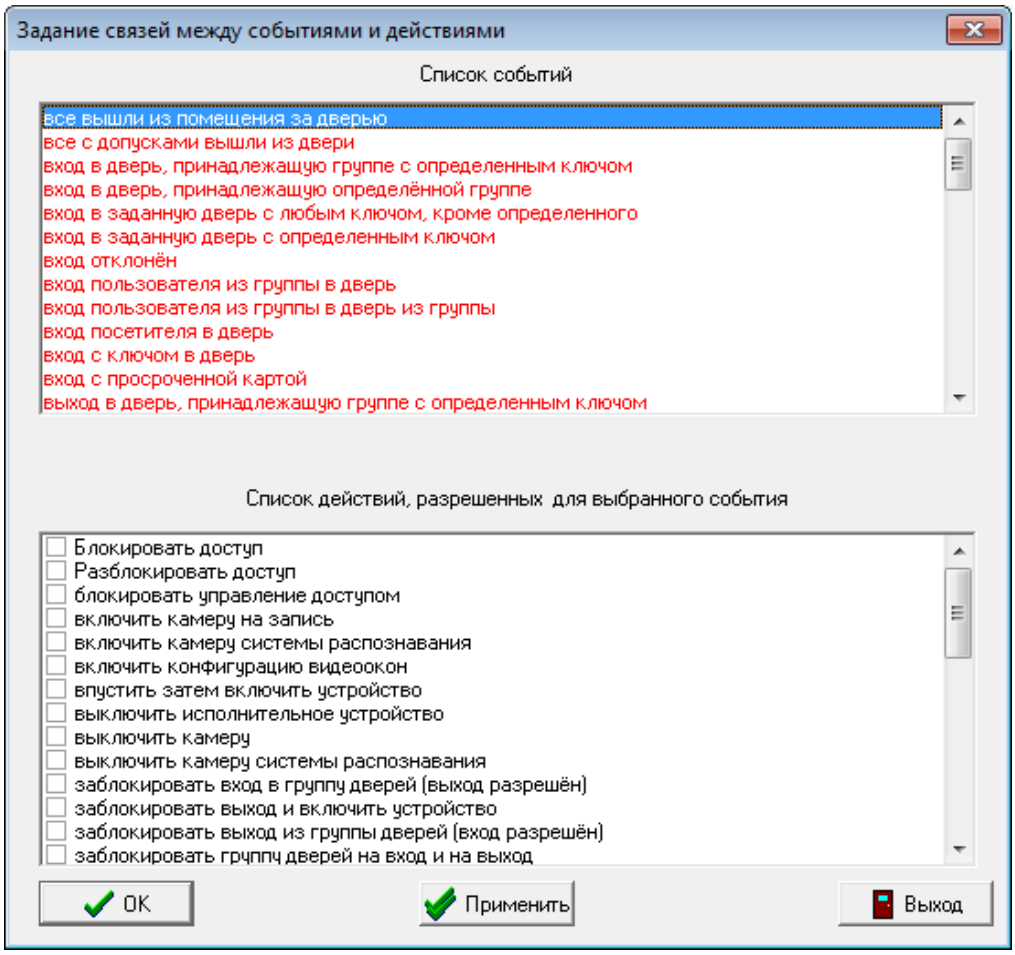



**Рисунок Б-1**

2. В появившемся окне "Правила" нажмите экранную кнопку "Редактировать связи" для того, чтобы определить связи между событиями в Системе и разрешенными для них действиями.

3. В появившемся окне "Задание связей между событиями и действиями" (см. рисунок Б.1) выберите щелчком мыши событие "все вышли из помещения за дверью". Назначьте этому событию действие "поставить эту дверь на охрану".

4. Нажмите экранную кнопку "Применить" для того, чтобы сохранить все текущие изменения.

5. Нажмите экранную кнопку "ОК" для закрытия окна редактирования связей.

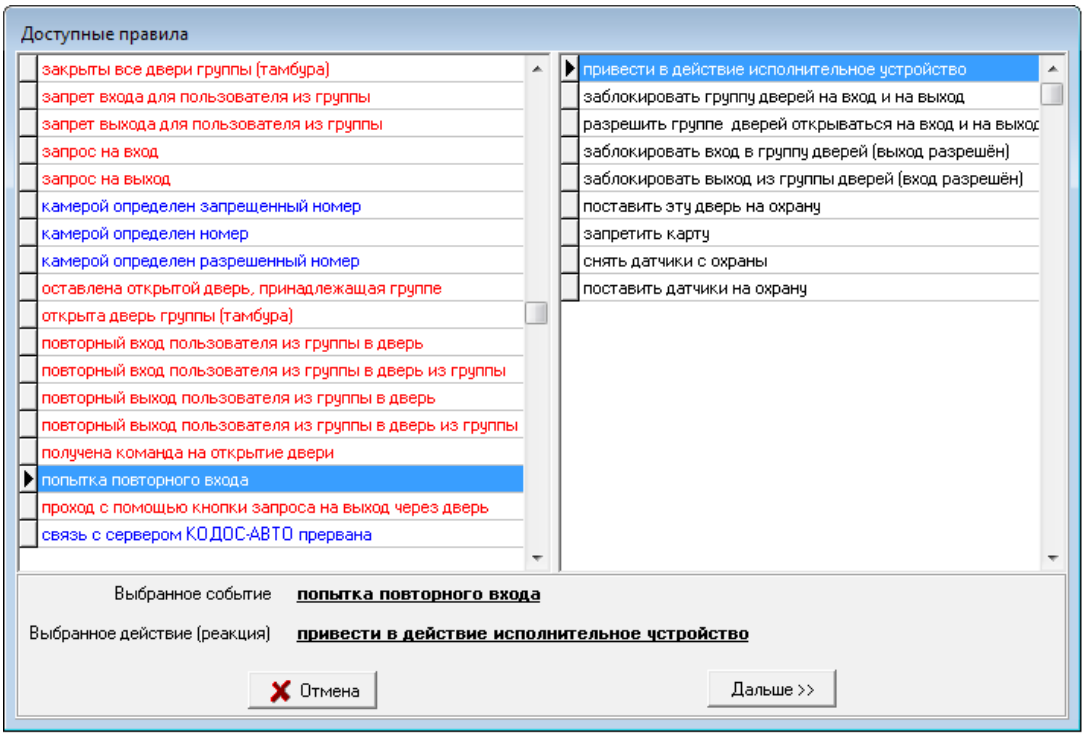



**Рисунок Б-2**

6. В окне "Правила" нажмите экранную кнопку "Новое правило".

7. В появившемся диалоговом окне (см. рисунок Б2) в поле ввода "События, предусмотренные правилами" путем установки мышью маркера в строку с выбираемым событием укажите тип события, на которое необходимо настроить автоматическую реакцию Системы: "все вышли из помещения за дверью". В поле ввода "Доступные действия (реакции на событие)" будут перечислены все действия, назначенные данному событию при редактировании связей.

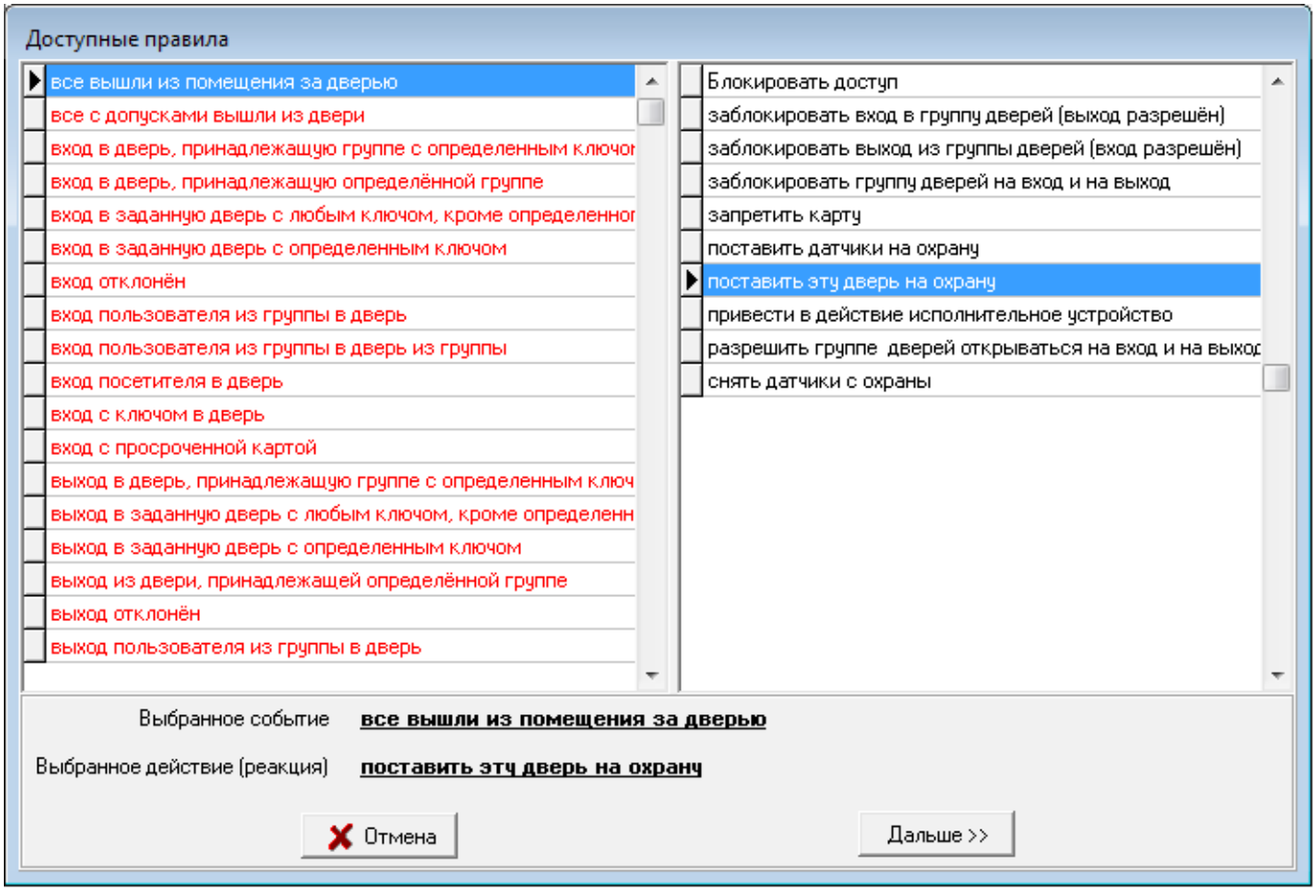



**Рисунок Б-3**

8. Из списка "Доступные действия (реакции на событие)" путем установки мышью маркера в строку с выбираемым действием выберите то действие, которое должно выполняться Системой при наступлении события ("поставить эту дверь на охрану").

9. Нажмите экранную кнопку "Дальше >>".

10. В появившемся окне "Настройка параметров событий и действий" (см. рисунок Б.3) запрашиваются дополнительные параметры для выполнения правила. В нем (одинарным щелчком мыши на нужном объекте) следует указать дверь 1, которую необходимо поставить на охрану.

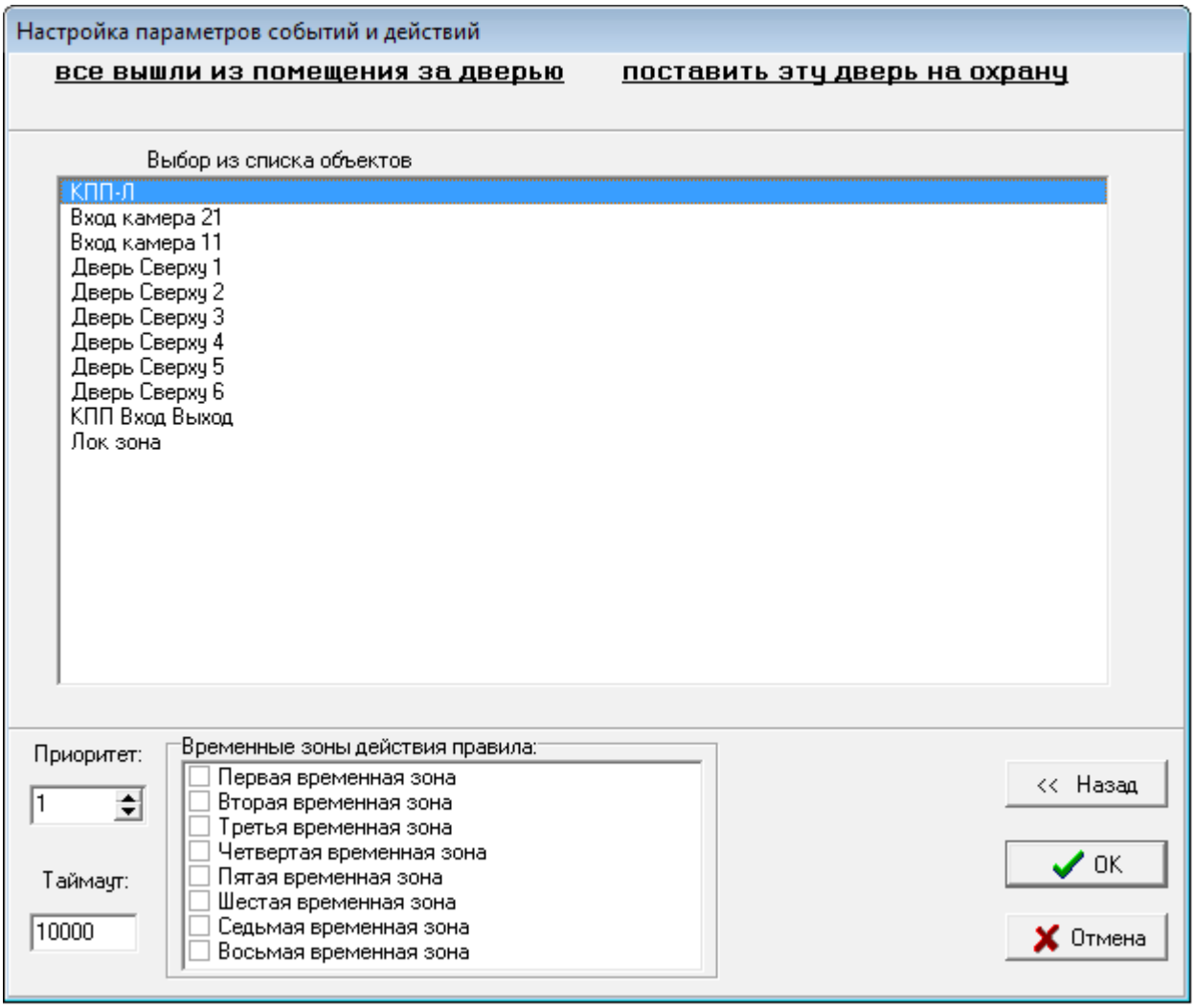



**Рисунок Б-4**

11. Укажите временную зону, в которую будет действовать правило, путем установки флажка напротив названия этой зоны (в нашем примере это шестая временная зона).

12. С помощью поля с пошаговым изменением значений "Приоритет" установите приоритет выполнения Правила (по умолчанию - 1).

13. В поле "Таймаут" установите в миллисекундах (тысячные доли секунды) продолжительность задержки перед выполнением правила. Действие, заданное Правилом, будет выполняться спустя указанное время от момента возникновения события. Если задержка не нужна, установите в этом поле значение 0.

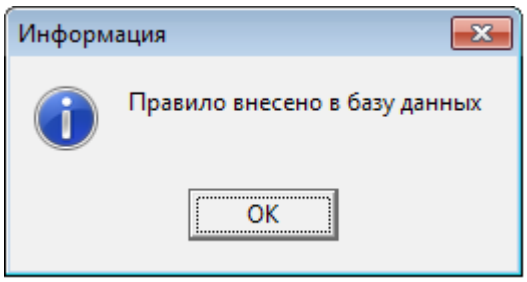



**Рисунок Б-5**

14. Нажмите экранную кнопку "ОК".

Если все действия были выполнены правильно, то Системой будет выдано подтверждение (см. рисунок 3.5), а в поле окна "Правила" должен появиться текст нового правила (см. рисунок 3.6).

Обратите внимание на то, что задание связей между событиями и действиями (см. действие 3) позволяет создать лишь заготовку для правил, которую в дальнейшем можно использовать несколько раз. В нашем случае, произведя аналогичные действия и для двери 2, из той же заготовки получим новое правило.

Список правил (см. рисунок 3.6) содержит все действия, которые будет автоматически производить Система при наступлении соответствующих событий. Этот список администратором Системы в случае необходимости может быть откорректирован в плане назначения текущему (выделенному) правилу приоритета и изменения соответствующей ему временной зоны. Чтобы указанные изменения вступили в силу, нажмите экранную кнопку "Применить".

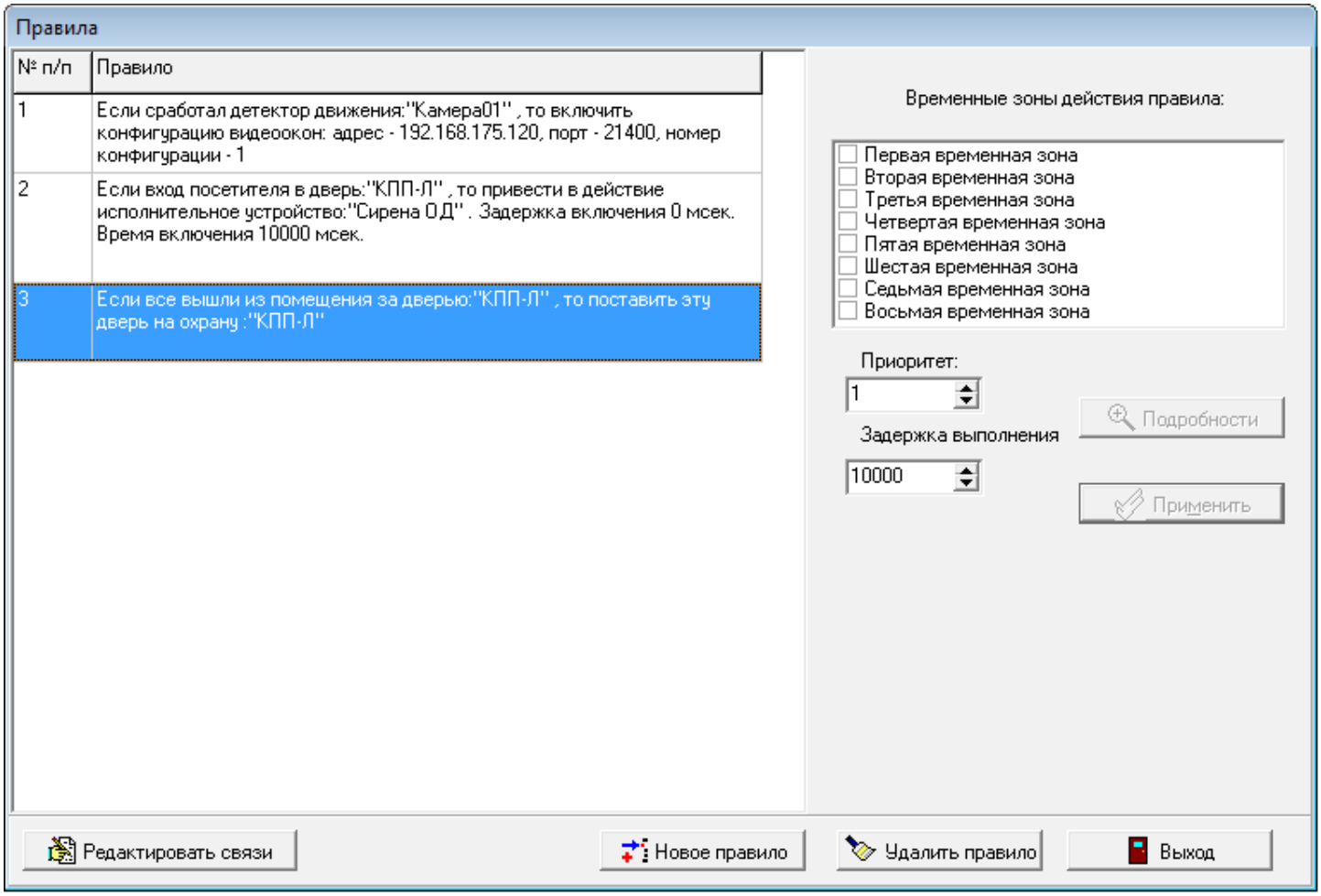



**Рисунок Б-6**

## ПРИЛОЖЕНИЕ В Пример создания пропуска

Ниже приводится краткое описание действий для создания пропуска.

1. Запустите на выполнение программу Дизайна пропусков (следует помнить, что при этом будет загружена база данных, Alias (псевдоним) которой указан в файле codos.ini).

2. Нажмите сочетание клавиш <Ctrl+N>.

3. В появившемся диалоговом окне вам будет предложено выбрать размеры нового пропуска. Если вас устраивают предложенные по умолчанию размеры, то нажмите экранную кнопку "ОК".

ПРИМЕЧАНИЕ — Названия экранных кнопок можно увидеть во всплывающих подсказках появляющихся при наведении указателя мыши на кнопку.

Перед началом редактирования, а в процессе работы периодически рекомендуется сохранять схему пропуска при помощи комбинации клавиш <Ctrl+S>. При сохранении схемы в первый раз программа запросит имя схемы нового пропуска.

4. Нажмите на панели инструментов экранную кнопку "Добавить заголовок". С помощью команды основного меню "Формат" → "Изменить шрифт", выберите Times New Roman, полужирный, размер 28 и нажмите экранную кнопку "ОК" Затем в окне "Редактор объектов" установите настройки заголовка пропуска. Например:

- Верхний отступ – 20
- Левый отступ – 20
- Ширина – 360
- Высота – 40
- Подпись – ПРОПУСК
- Выравнивание – по центру

5. Нажмите на панели инструментов экранную кнопку "Добавить поле таблицы из БД". Нажмите сочетание клавиш <Ctrl + F> и установите: Шрифт: Times New Roman, Начертание: полужирный, Размер: 22. Затем нажмите кнопку "ОК" и в окне Редактора объектов установите следующие параметры:

- Верхний отступ – 80
- Левый отступ – 40
- Ширина – 300
- Высота – 40
- Поле в БД – Фамилия
- Выравнивание – по левому краю

6. Нажмите на панели инструментов экранную кнопку "Добавить поле таблицы из БД". Нажмите сочетание клавиш <Ctrl + F> и установите: Шрифт: Times New Roman, Начертание: обычный, Размер: 20. Затем установите следующие параметры в окне Редактора объектов:

- Верхний отступ – 130
- Левый отступ – 40
- Ширина – 300
- Высота – 35
- Поле в БД – Имя
- Выравнивание – по левому краю

7. Нажмите на панели инструментов экранную кнопку "Добавить поле таблицы из БД". Нажмите сочетание клавиш <Ctrl + F> и установите: Шрифт: Times New Roman, Начертание: обычный, Размер: 20. Затем установите следующие параметры в окне Редактора объектов:

- Верхний отступ – 165
- Левый отступ – 40
- Ширина – 300
- Высота – 35
- Поле в БД – Отчество
- Выравнивание – по левому краю

8. Нажмите на панели инструментов экранную кнопку "Добавить фотографию". Затем установите следующие параметры в окне Редактора объектов:

- Верхний отступ – 52
- Левый отступ – 400
- Ширина – 151
- Высота – 168

9. Нажмите экранную кнопку "Добавить рамку". Затем установите следующие параметры в окне Редактора объектов:

- Верхний отступ – 70
- Левый отступ – 30
- Ширина – 340
- Высота – 150

10. Нажмите экранную кнопку "Добавить заголовок". С помощью команды основного меню "Формат" → "Изменить шрифт", выберите шрифт: Times New Roman, жирный, размер 14, нажмите экранную кнопку "ОК" Затем установите настройки в Редакторе объектов такими, как они указаны ниже.

- Верхний отступ – 240
- Левый отступ – 30
- Ширина – 100
- Высота – 20
- Подпись – Должность:
- Выравнивание – по левому краю

11. Нажмите на панели инструментов экранную кнопку "Добавить поле таблицы из БД". Нажмите сочетание клавиш <Ctrl + F> и установите следующее: Шрифт – Times New Roman, Начертание – обычный, Размер – 14. Затем установите следующие параметры в окне Редактора объектов:

- Верхний отступ – 240
- Левый отступ – 140
- Ширина – 230
- Высота – 20
- Поле в БД – Должность
- Выравнивание – по левому краю

12. Нажмите на панели инструментов экранную кнопку "Добавить заголовок". С помощью команды основного меню "Формат" → "Изменить шрифт", выберите Times New Roman, полужирный, размер 14, нажмите экранную кнопку "ОК" Затем установите настройки в Редакторе объектов такими, как они указаны ниже.

- Верхний отступ – 250
- Левый отступ – 400
- Ширина – 151
- Высота – 20
- Подпись – Код карты
- Выравнивание – по центру

13. Нажмите на панели инструментов экранную кнопку "Добавить поле таблицы из БД". Нажмите сочетание клавиш <Ctrl + F> и установите следующее: Шрифт – Times New Roman, Начертание – обычный, Размер – 14. Затем установите следующие параметры в окне Редактора объектов:

- Верхний отступ – 270
- Левый отступ – 400
- Ширина – 151
- Высота – 20
- Поле в БД – Код карты
- Выравнивание – по центру

14. Нажмите на панели инструментов экранную кнопку "Добавить заголовок". В меню "Формат"  "Изменить шрифт", выберите Times New Roman, полужирный, размер 14, нажмите экранную кнопку "ОК" Затем установите настройки в Редакторе объектов такими, как они указаны ниже.

- Верхний отступ – 280
- Левый отступ – 30
- Ширина – 160
- Высота – 20
- Подпись – Уровень доступа:
- Выравнивание – по левому краю

15. Нажмите на панели инструментов экранную кнопку "Добавить поле таблицы из БД". Нажмите сочетание клавиш <Ctrl + F> и установите следующее: Шрифт – Times New Roman, Начертание – обычный, Размер – 14. Затем установите следующие параметры в окне Редактора объектов:

- Верхний отступ – 280
- Левый отступ – 190
- Ширина – 30
- Высота – 20
- Поле в БД – Уровень доступа
- Выравнивание – по центру

16. Нажмите на панели инструментов экранную кнопку "Добавить заголовок". С помощью. команды основного меню "Формат"  "Изменить шрифт", выберите Times New Roman, полужирный, размер 14, нажмите экранную кнопку "ОК" Затем установите настройки в Редакторе объектов такими, как они указаны ниже.

- Верхний отступ – 320
- Левый отступ – 30
- Ширина – 150
- Высота – 20
- Подпись – Пропуск выдан
- Выравнивание – по левому краю

17. Нажмите на панели инструментов экранную кнопку "Добавить поле таблицы из БД". Нажмите сочетание клавиш <Ctrl + F> и установите следующее: Шрифт – Times New Roman, Начертание – обычный, Размер –14. Затем установите следующие параметры в окне Редактора объектов:

- Верхний отступ – 320
- Левый отступ – 180
- Ширина – 110
- Высота – 20
- Поле в БД – Дата выдачи карты
- Выравнивание – по центру

18. С помощью команды меню "Фон"  "Выбрать цвет" выберите фиолетовый цвет.

Если все действия были выполнены правильно, то должен получится пропуск показанный на рисунке В.1

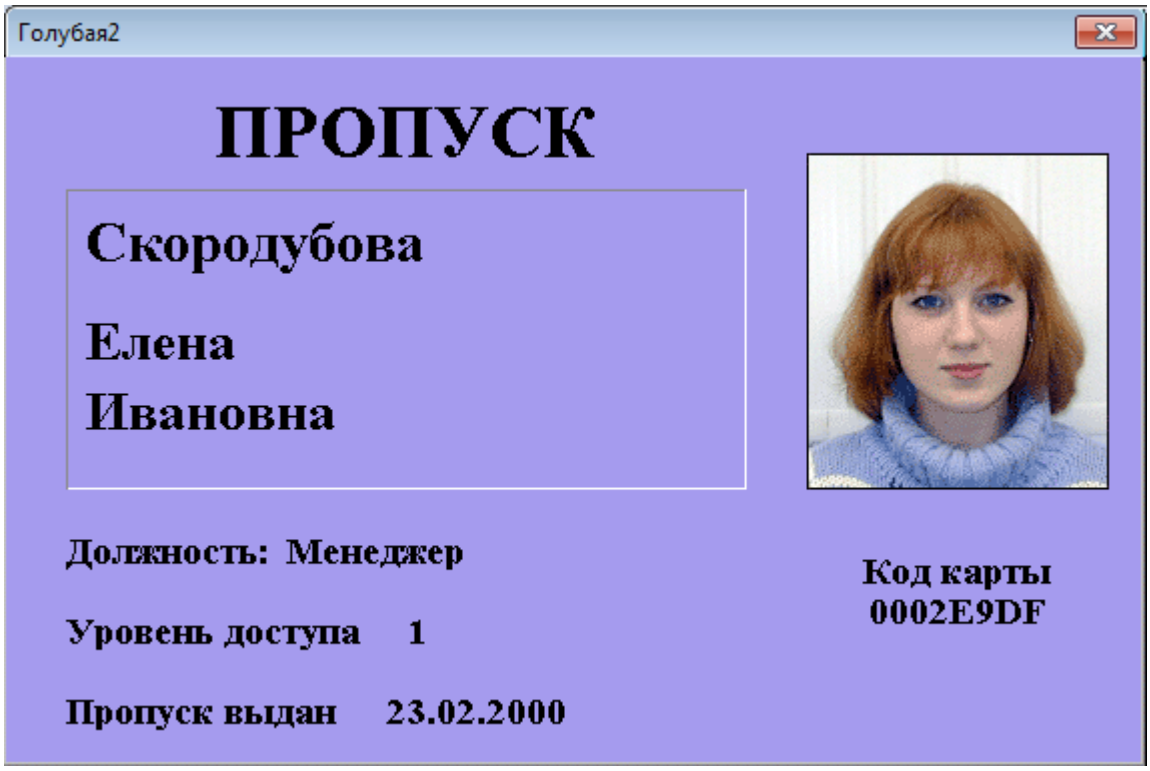



**Рисунок В-1**

ПРИМЕЧАНИЕ — Содержание полей имя, фамилия, фотография и т.д. будет автоматически взято из БД, на работу с которой настроена программа дизайна пропусков.

## ПРИЛОЖЕНИЕ Г Резервное копирование БД СУБД FireBird.

1. Вначале необходимо найти местоположение БД в компьютере и файл БД. По умолчанию файл БД расположен: C:\ssa\skd\codos_db\codos.gdb.

Чтобы узнать, где находится БД, с которой работает «КОДОС-ИКБ» - открыть файл codos.ini и посмотреть имя «alias» в «[Database] DBAlias=codos_ib», где «codos_ib» – это «alias» БД (рисунок Г.1).

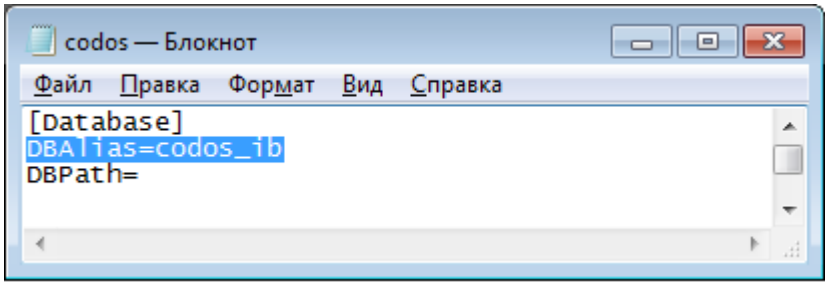



**Рисунок Г-1**

2. Запустить «BDE администратор» - «Пуск»□«Настройки»□«Панель управления». Откроется окно «BDE Administrator …» (рисунок Г.2).

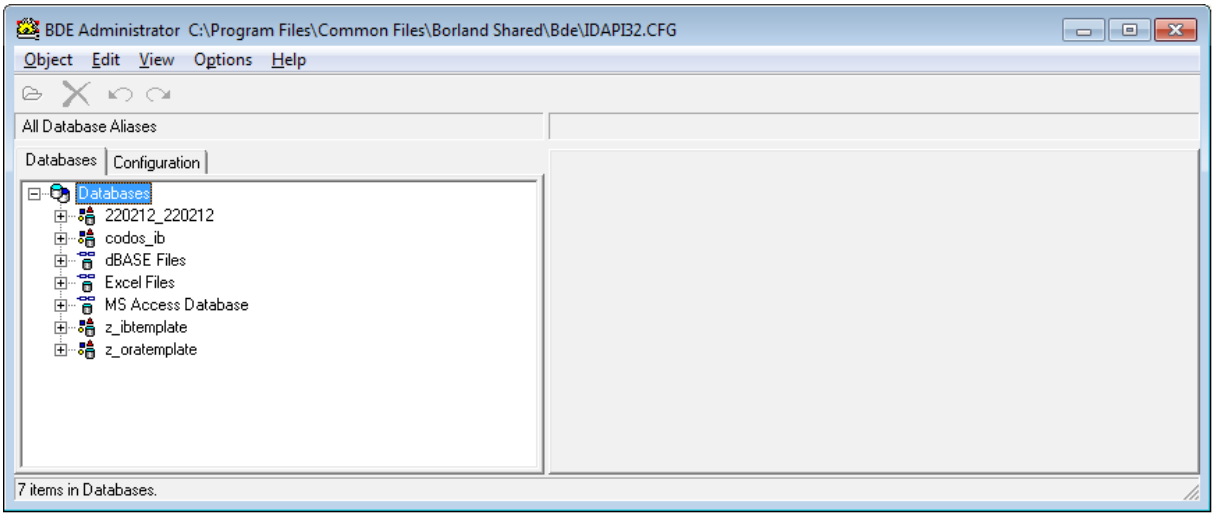



**Рисунок Г-2**

3. В появившемся окне выбрать имя рабочего «alias» БД. Путь, указанный в поле SERVER NAME рабочего «alias», указывает месторасположение файла БД на жёстком диске компьютера. Файл, находящийся по этому пути и есть искомый файл БД (рисунок Г.3).

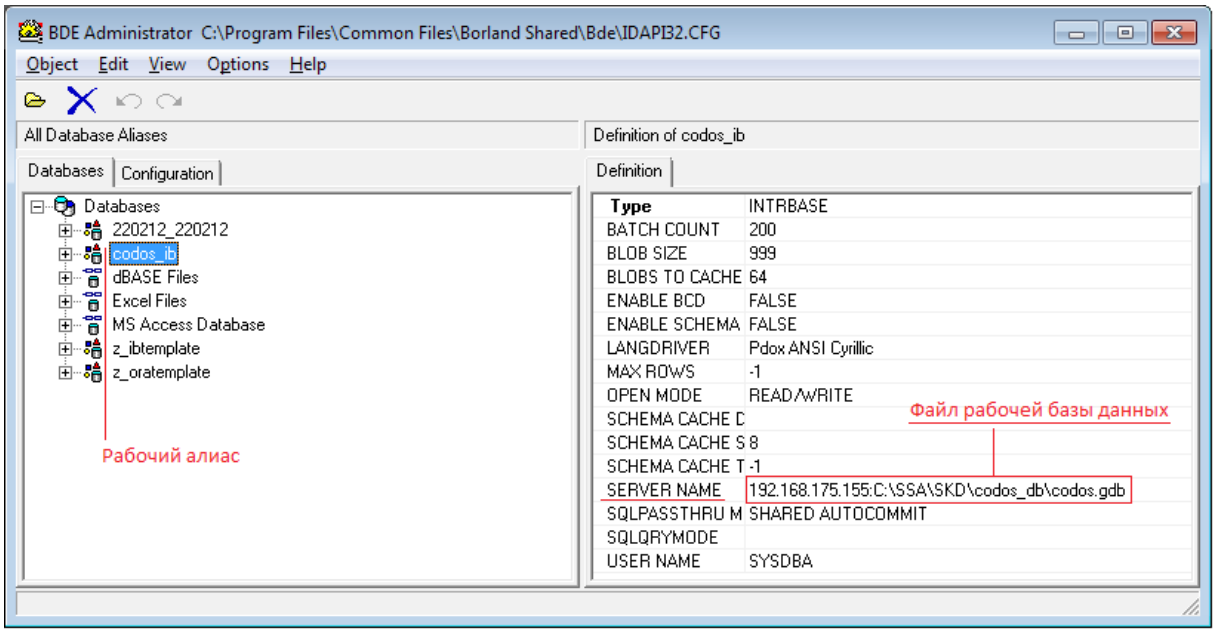



**Рисунок Г-3**

4. Отключить «Кодос ИКБ» и АРМ, связанные с «КОДОС-ИКБ». Скопировать файл рабочей БД на жёсткий диск компьютера или в директорию другого компьютера, где будет выполняться резервное копирование с последующим восстановлением базы данных СУБД FireBird. Например: БД из папки C:\ssa\skd\codos_db\ скопировать в директорию C:\bases\. Произвести процедуру резервного копирования с последующим восстановлением базы данных СУБД FireBird копии БД из C:\bases\.

Скопировать рабочую БД из папки C:\ssa\skd\codos_db\ в директорию C:\xxxxxx\, где xxxxxx - дата проведения процедуры (рекомендуемое сохранение на случай «отката»).

5. Далее, «Пуск» → «Программы» → «Firebird» → «IBConsole» (рисунок Г.4). Щелкнуть в строке «Local Server» правой клавишей мыши.

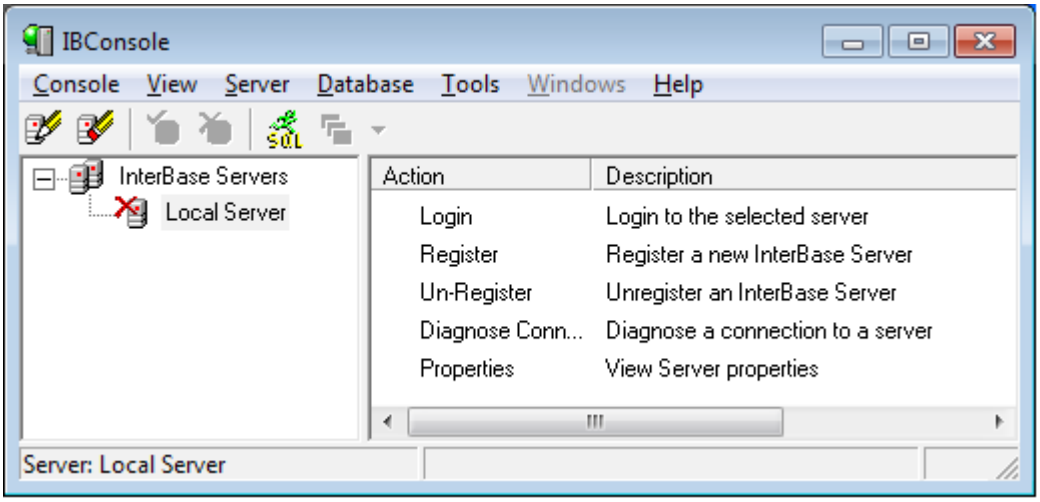



**Рисунок Г-4**

6. Выбрать «Un-Register» (рисунок Г.5).

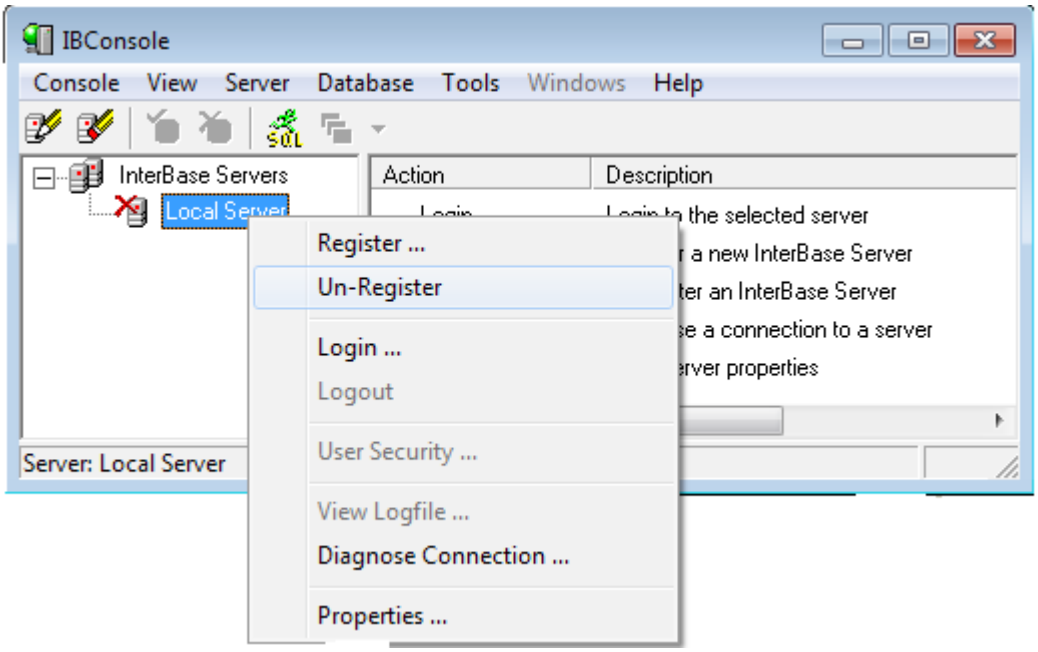



**Рисунок Г-5**

7. В окне «Confirm» нажать кнопку «Yes» (рисунок Г.6).

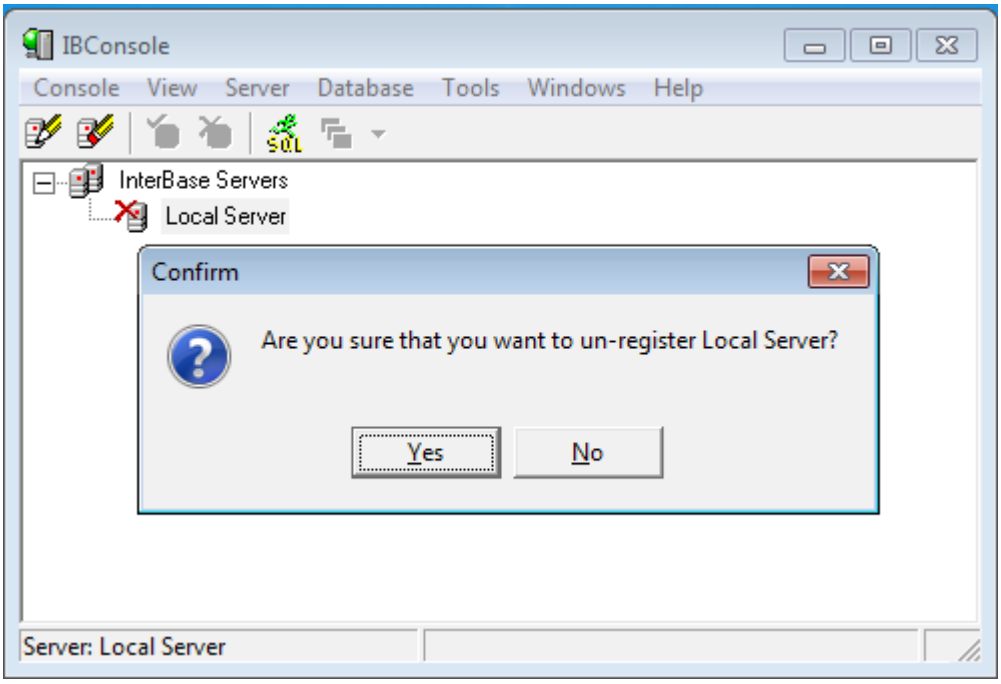



**Рисунок Г-6**

8. Щелкнуть правой клавишей мыши в строке «InterBase Servers». Выбрать «Register…» (рисунок Г.7).

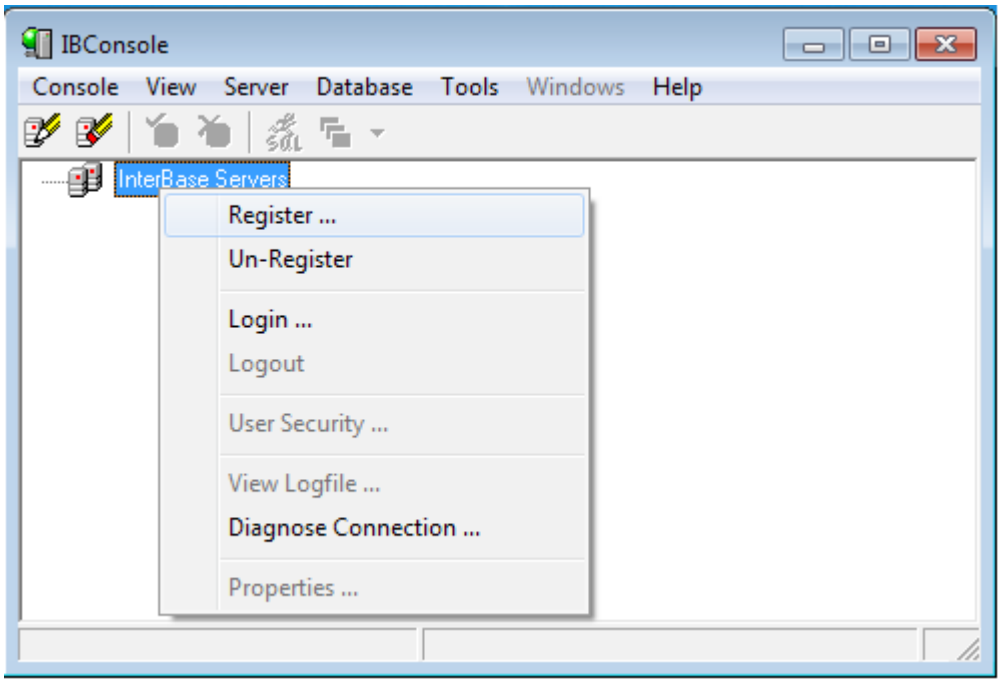



**Рисунок Г-7**

9. В окне «Register Server and Connect» (рисунок Г.8) выбрать тип подключения «Local Server». В поле «Login Information» ввести «User Name:» - «sysdba», «Password:» - «masterkey». Имя и пароль, указанные в данной инструкции, указаны по умолчанию. Вводить следует установленные «Имя пользователя» и «Пароль» базы данных. Затем нажать кнопку «ОК».

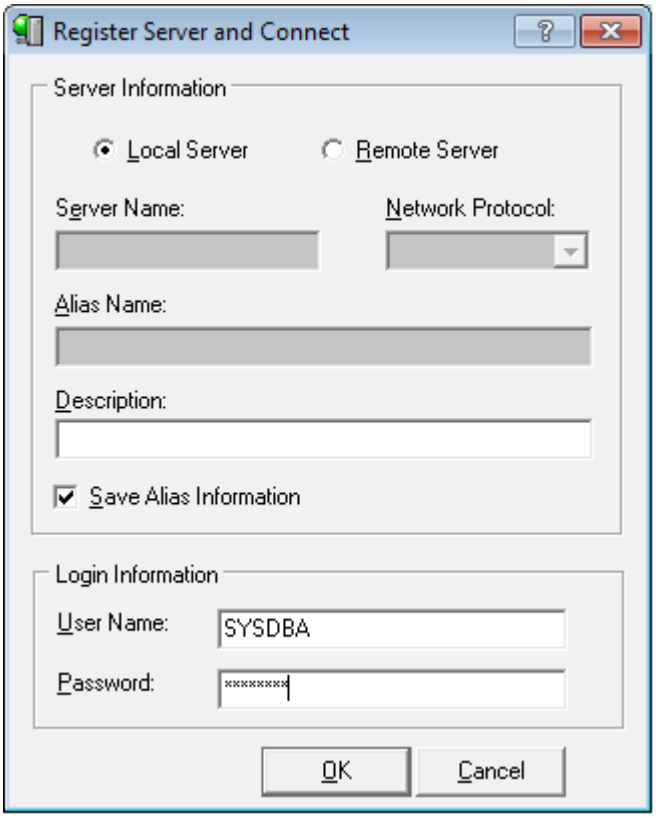



**Рисунок Г-8**

10. Нажать ⊞ «Local Server» (рисунок Г.9), раскроется список. Нажать «Databases» правой клавишей мыши, в появившемся списке выбрать «Register».

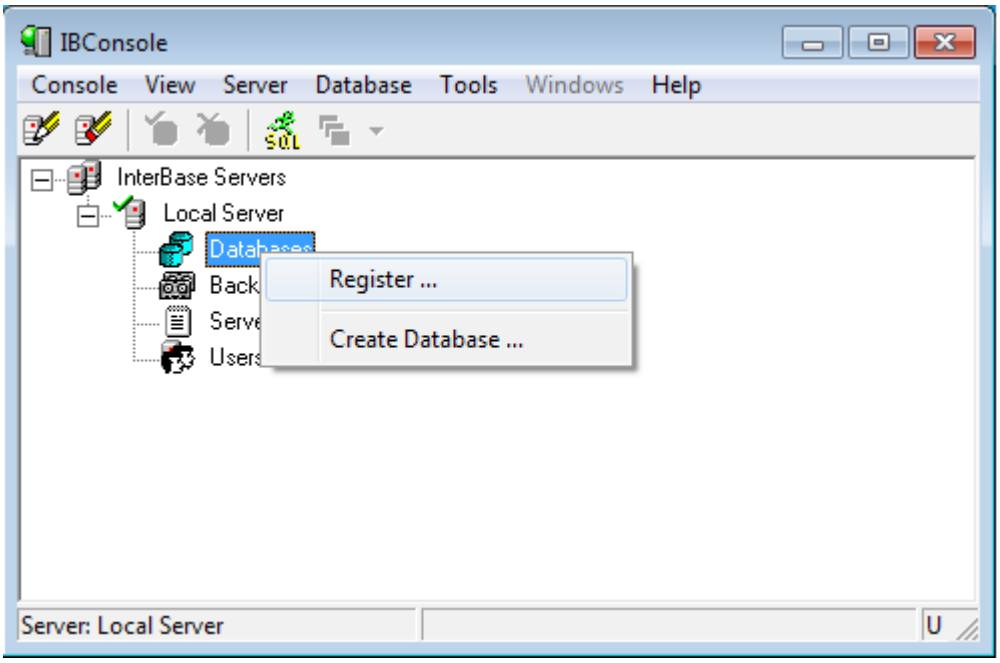



**Рисунок Г-9**

11. В панели «Database» нажать ... (рисунок Г.10), указать файл копии рабочей базы данных из папки c:\bases\. В панели «Login Information» ввести «sysdba» (по умолчанию). В поле «User Name» ввести пароль «masterkey» (по умолчанию). Затем нажать кнопку «OK».

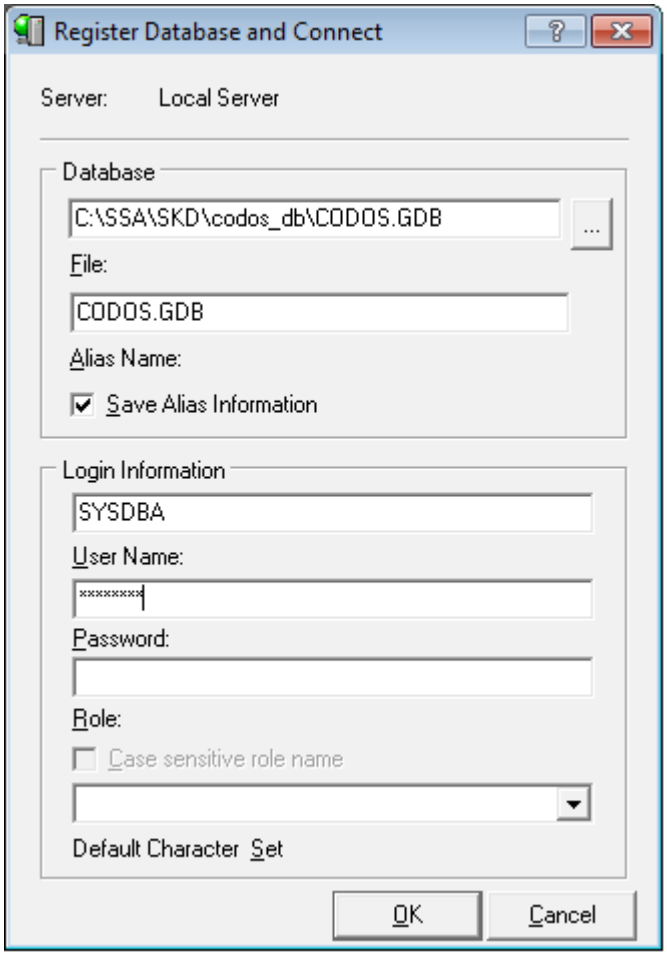



**Рисунок Г-10**

12. Нажать «Backup» правой клавишей мыши. В появившемся меню выбрать «Backup» (рисунок Г.11).

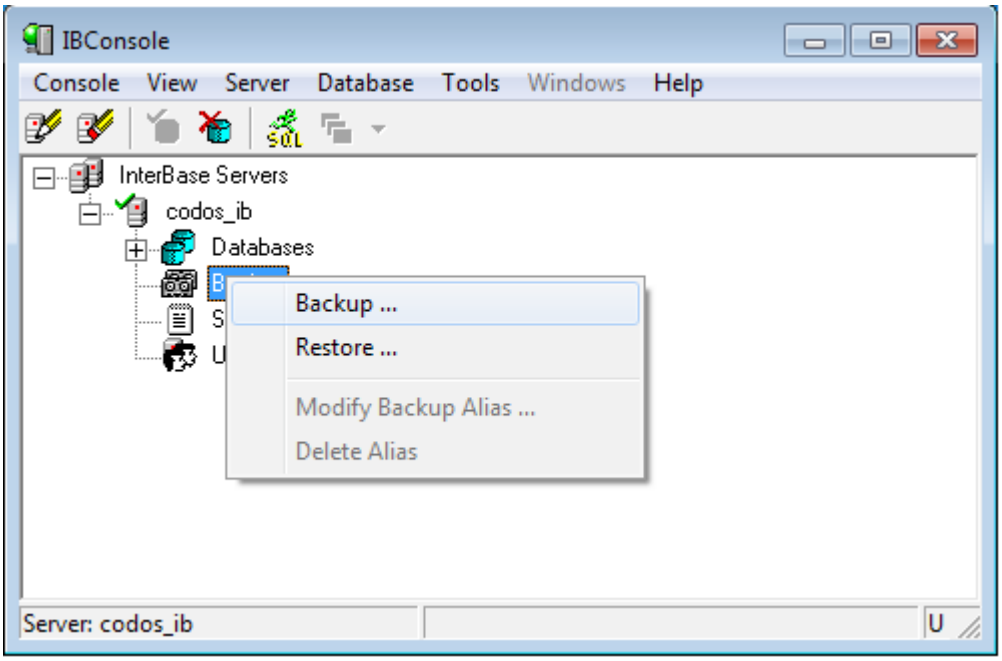



**Рисунок Г-11**

13. Появится окно «Database Backup» (рисунок Г.12).

В строке «Alias» панели «Database» выбрать рабочий «alias»./

В строке «Server» панели «Backup File(s)» выбрать «Local Server».

В строке «Alias» панели «Backup File(s)» написать имя латинскими символами, например, «codosbackup».

В поле «Filename(s)» указать место и имя файла Backup базы данных, например, «c:\190706.bak». Нажать кнопку «ОК».

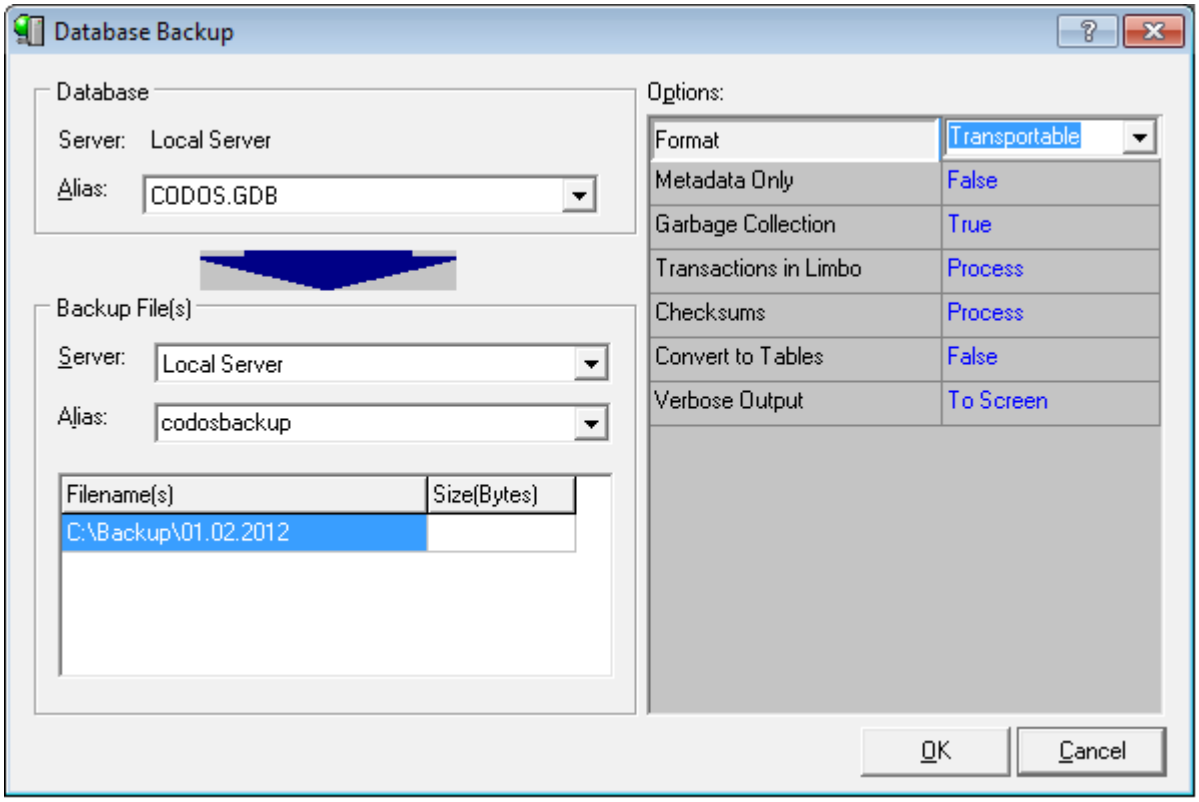



**Рисунок Г-12**

14. Начнется процедура «Backup» (рисунок Г.13).

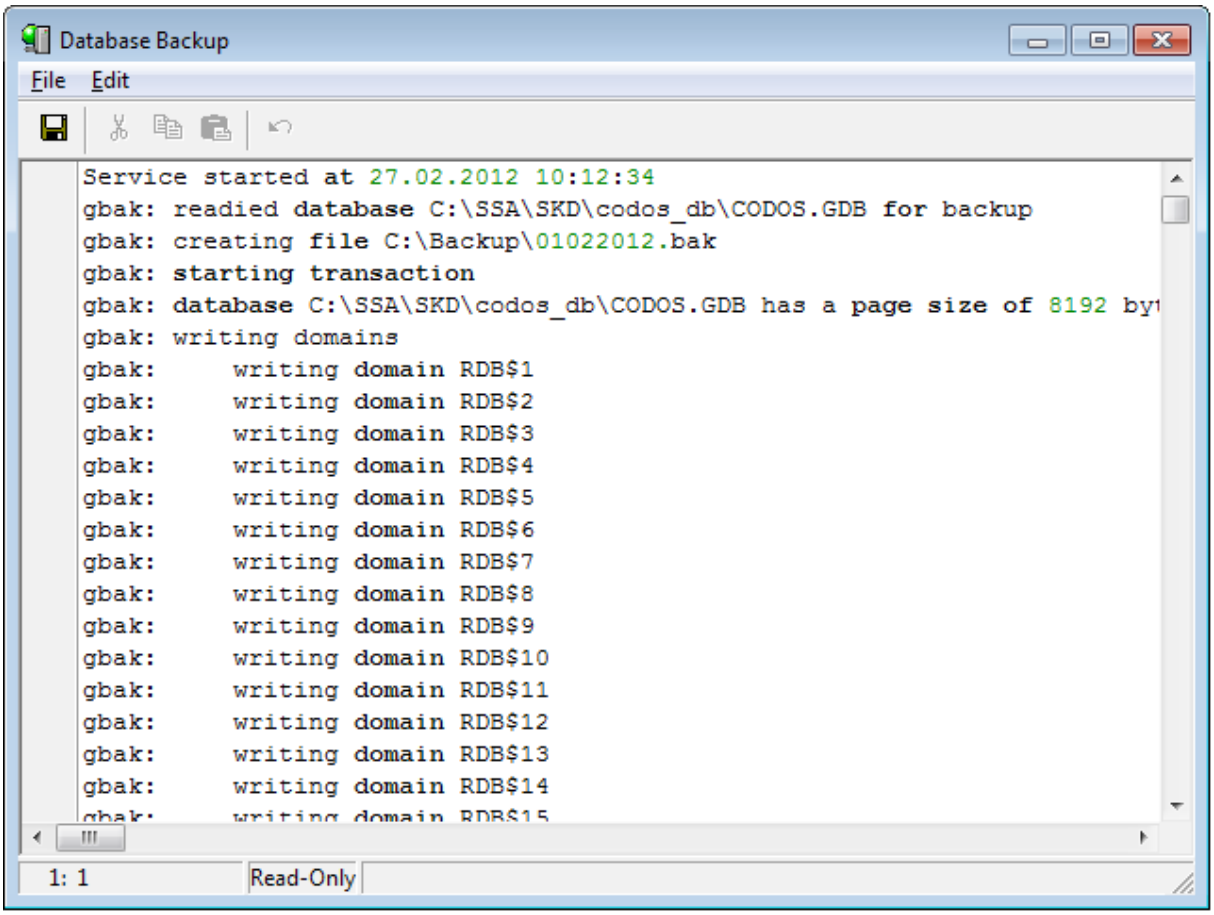



**Рисунок Г-13**

15. По завершении процедуры «Backup» появится информационное окно (рисунок Г.14), нажать «OK».

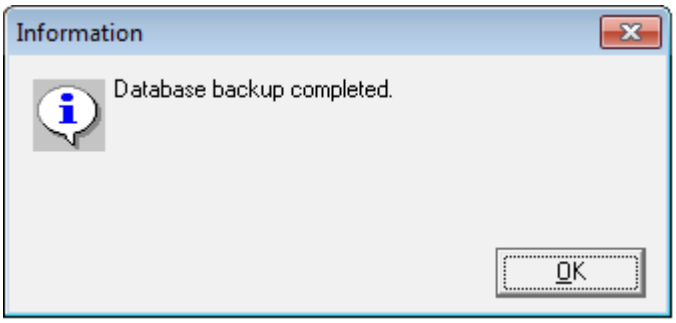



**Рисунок Г-14**

Если восстановление БД «Restore» не будет производиться сразу, закрыть окно «Database Backup» и окно «IBConsole».

## ПРИЛОЖЕНИЕ Д Восстановление БД СУБД FireBird.

1. Запустить «IBConsole» - «Пуск» → «Программы» →«Firebird» →«IBConsole» (рисунок Д.1). Щелкнуть в строке «Local Server» правой клавишей мыши.

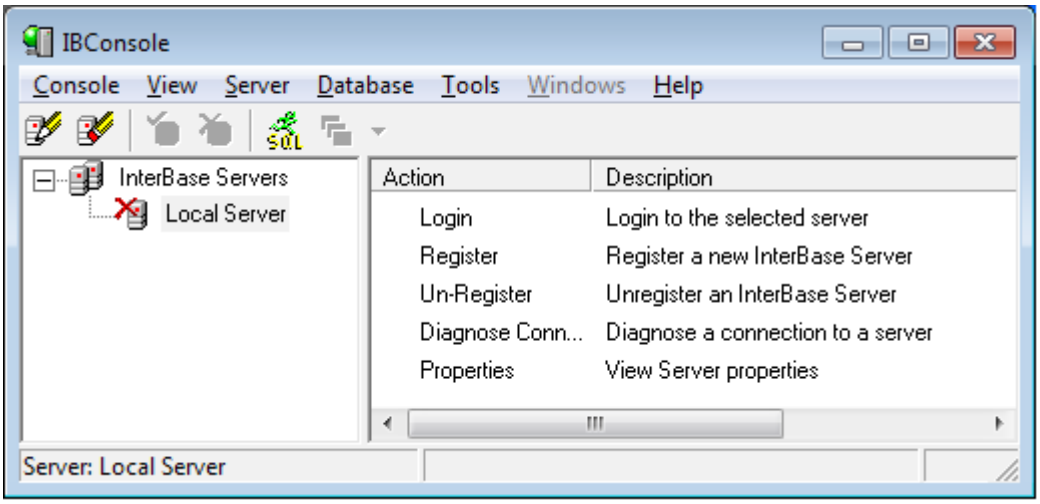



**Рисунок Д-1**

2. Выбрать «Un-Register» (рисунок Д.2).

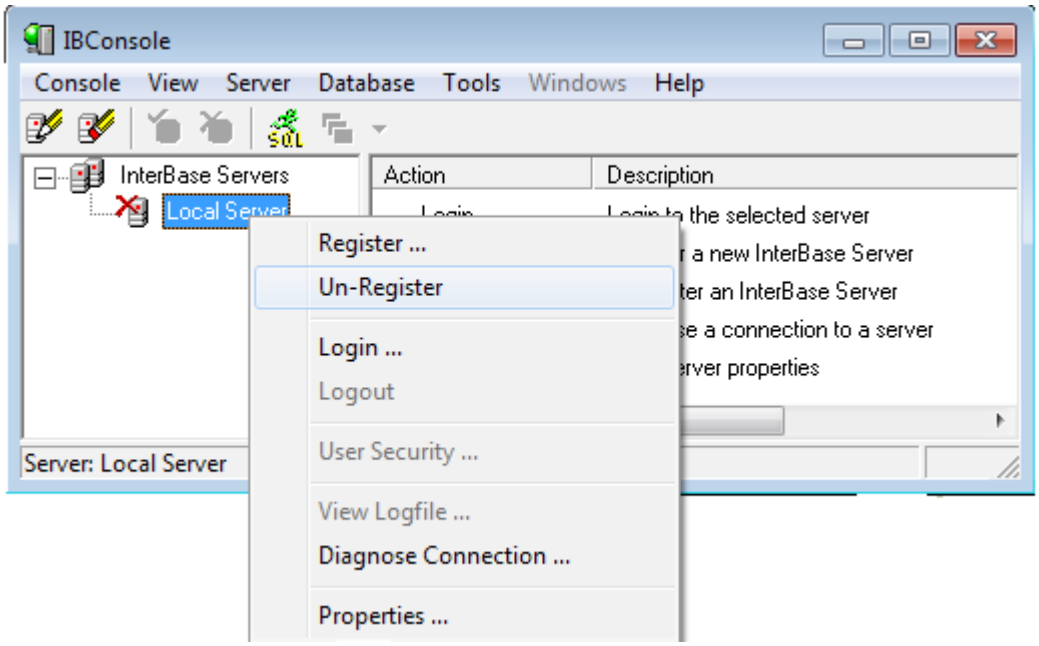



**Рисунок Д-2**

3. В диалоговом окне «Confirm» нажать кнопку «Yes» (рисунок Д.3).

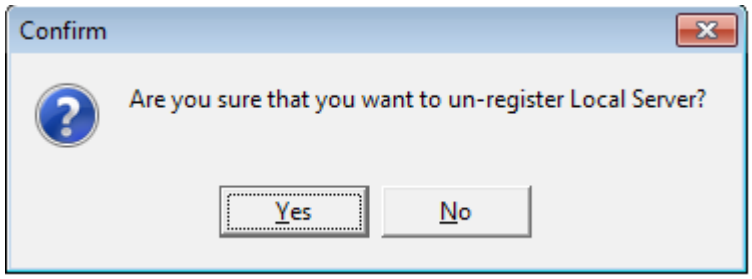



**Рисунок Д-3**

4. Нажать «InterBase Servers» правой клавишей мыши (рисунок Д.4).
5. Выбрать «Register…» (рисунок Д.5).

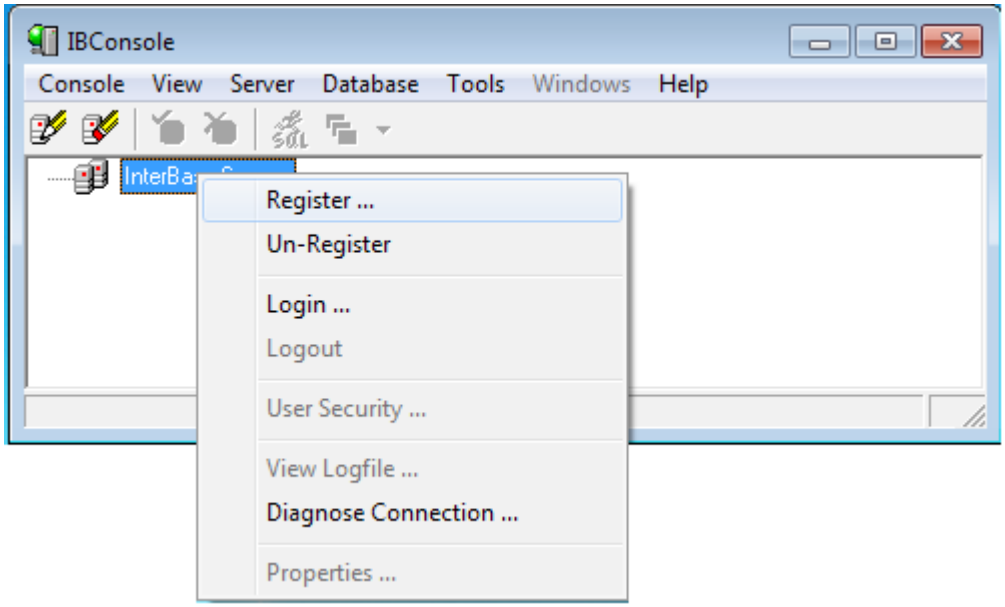



**Рисунок Д-4**

6. В окне «Register Server and Connect» (рисунок Д.6) выбрать тип подключения «Local Server». В панели «Login Information» в строке «User Name:» ввести «sysdba», в строке «Password:» ввести «masterkey». Имя и пароль указаны по умолчанию. Вводить необходимо реальные имя и пароль. После ввода информации нажать кнопку «ОК».

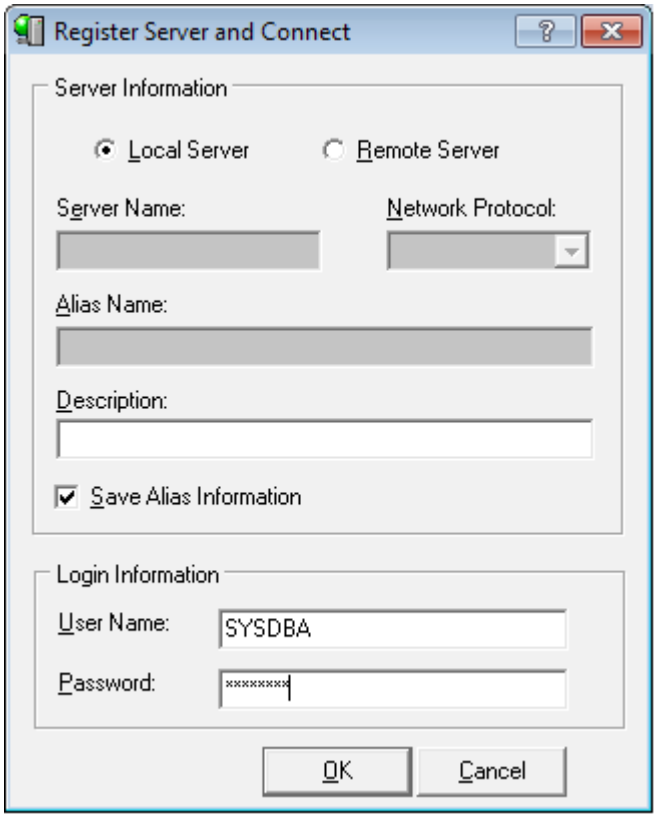



**Рисунок Д-5**

7. Нажать ⊞ «Local Server». В раскрывшемся списке нажать «Backup» правой кнопкой мыши. В появившемся меню выбрать «Restore» (рисунок Д.7).

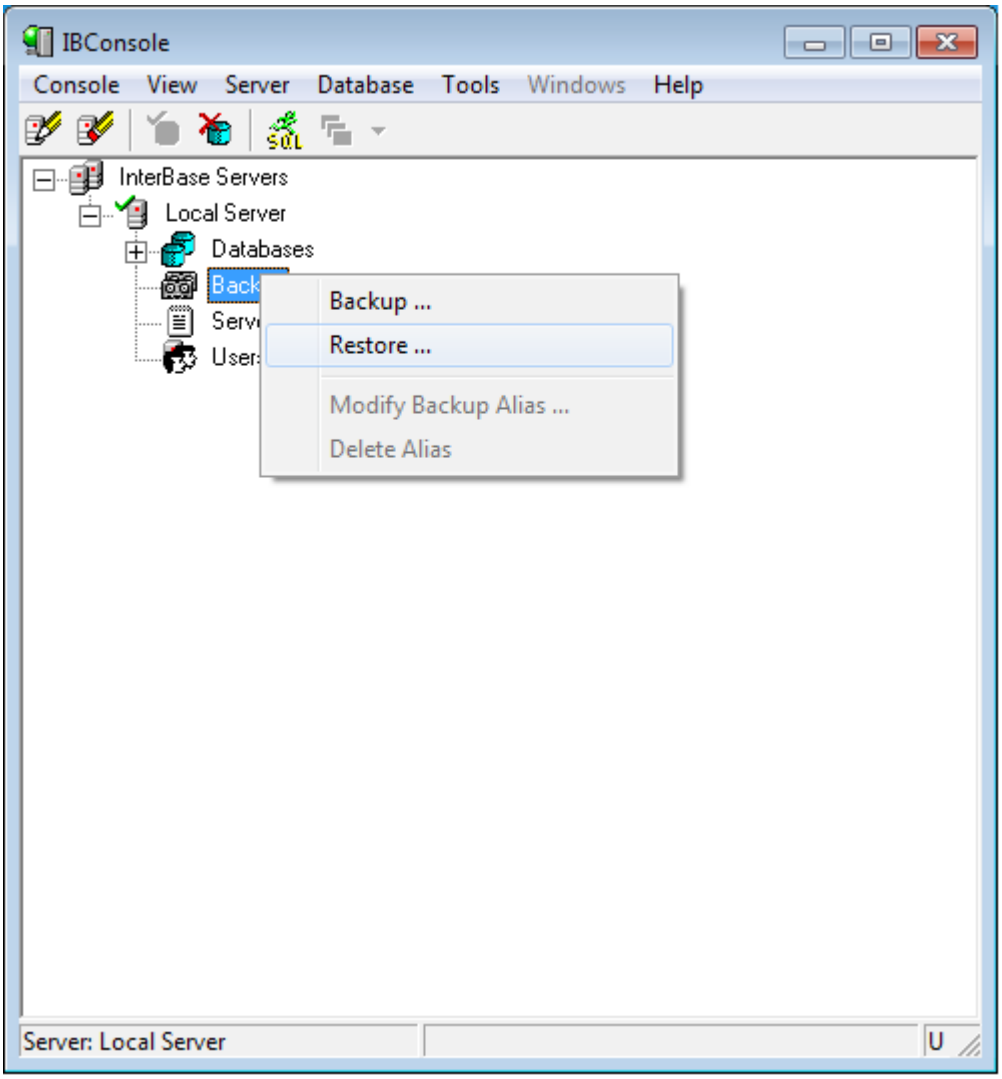



**Рисунок Д-6**

8. В строке «Alias:» нажать  и выбрать «File…» (рисунок Д.8).

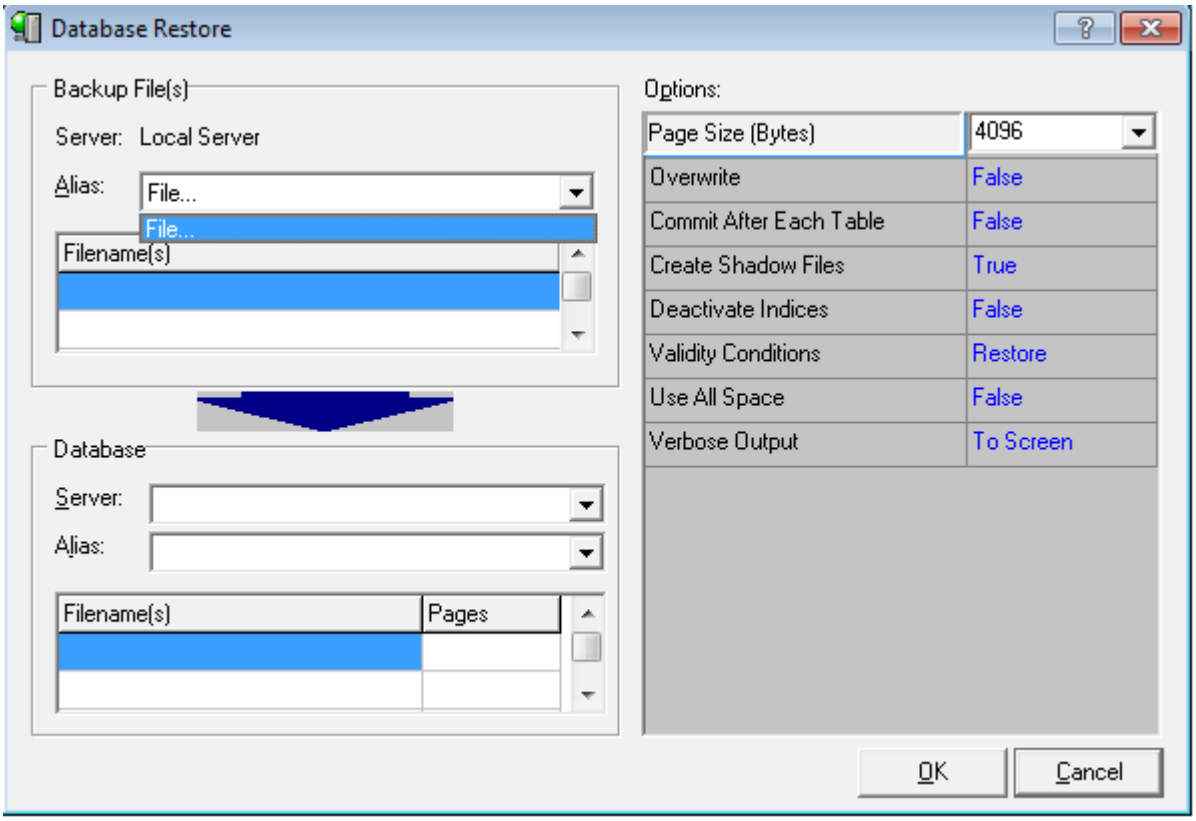



**Рисунок Д-7**

9. В окне «Открыть» установить тип файлов: «All files (*.*)».Выбрать файл архива базы данных. Нажать кнопку «Открыть» (рисунок Д.9).

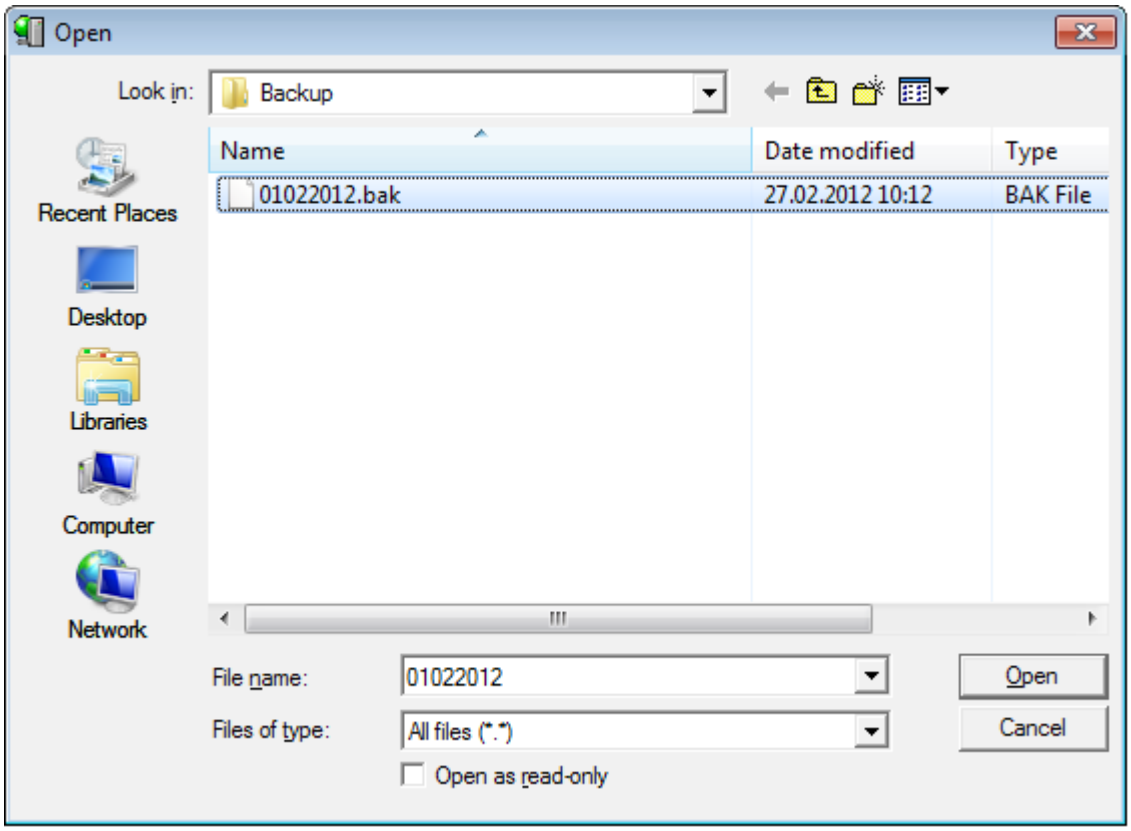



**Рисунок Д-8**

10. В панели «Backup File (s)» в строке «Alias» выбрать «codosbackup». В панели «Database» в строке «Server» выбрать «Local Server». В строке «Alias:» написать: «codos.gdb». В поле «Filename(s)» написать: «c:\restore\codos.gdb». В панели «Options» установить «Page Size (Bytes)» - «8192». Нажать кнопку «ОК» (рисунок Д.10).

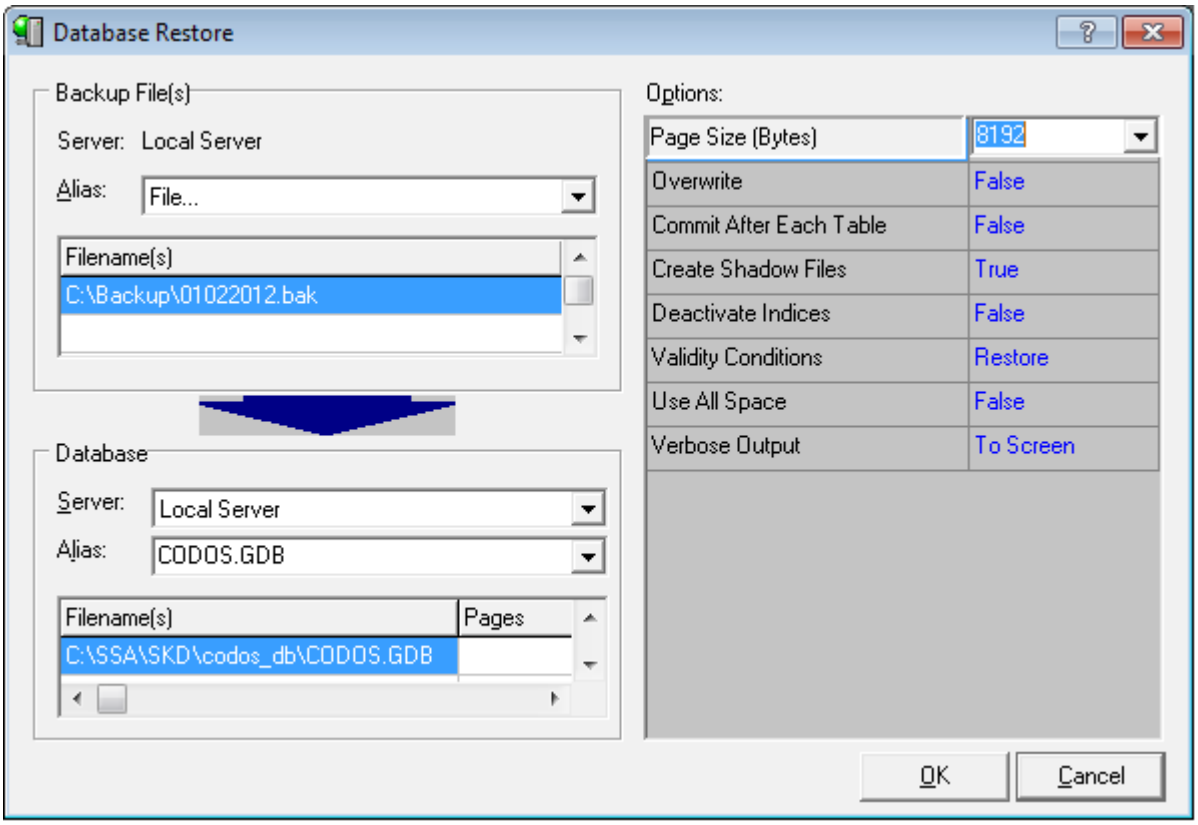



**Рисунок Д-9**

11. Начнется процедура «Restore». Она закончится после появления записи: «Service ended at …» (рисунок Д.11). После завершения процедуры «Restore» закрыть окно «Database Restore» и закрыть окно «IBConsole».

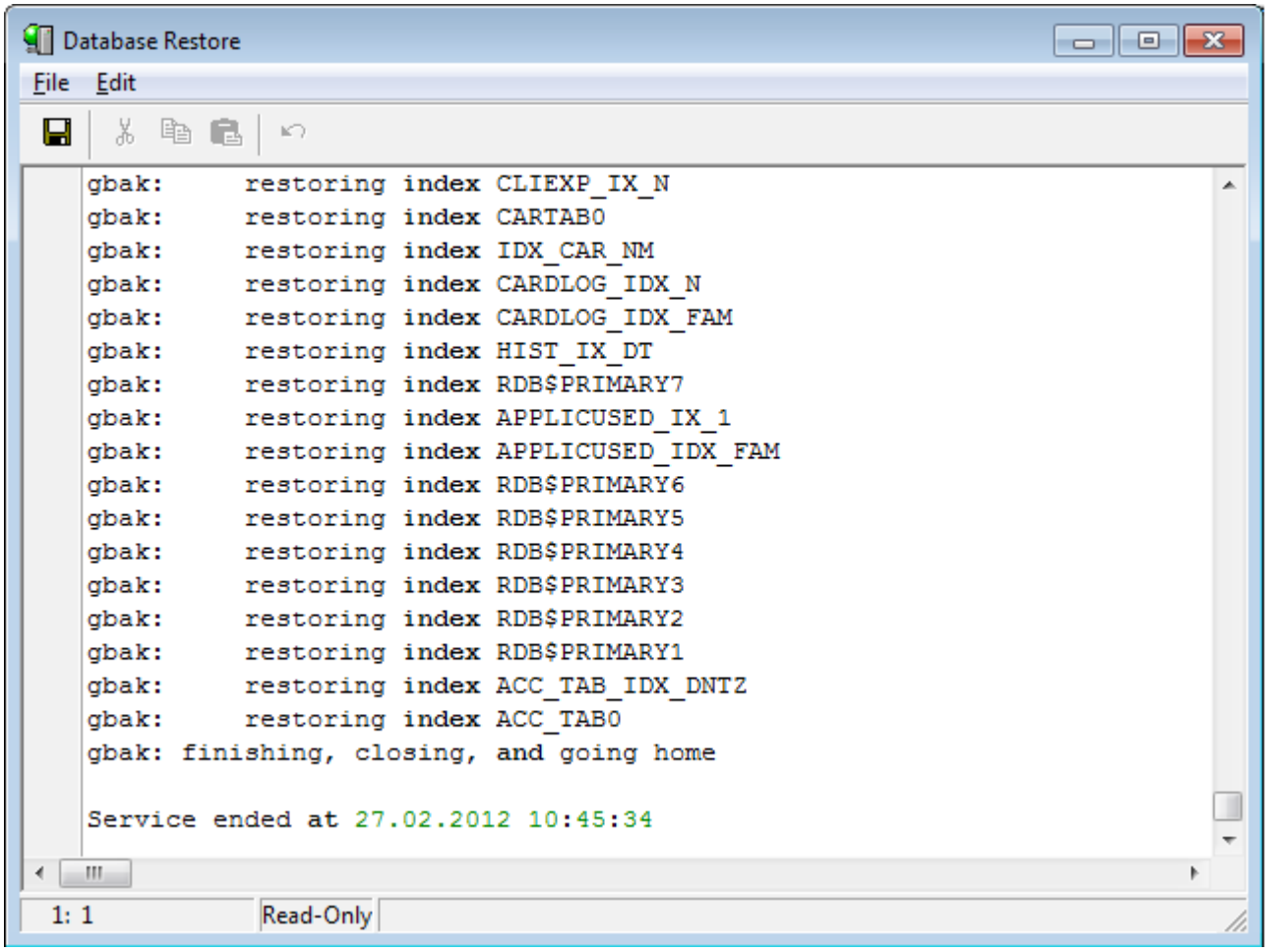



**Рисунок Д-10**

## ПРИЛОЖЕНИЕ Е Восстановление базы данных сразу после резервного копирования

1. Нажать название файла архивного копирования правой кнопкой мыши. В выпавшем меню выбрать «Restore» (рисунок Е.1).

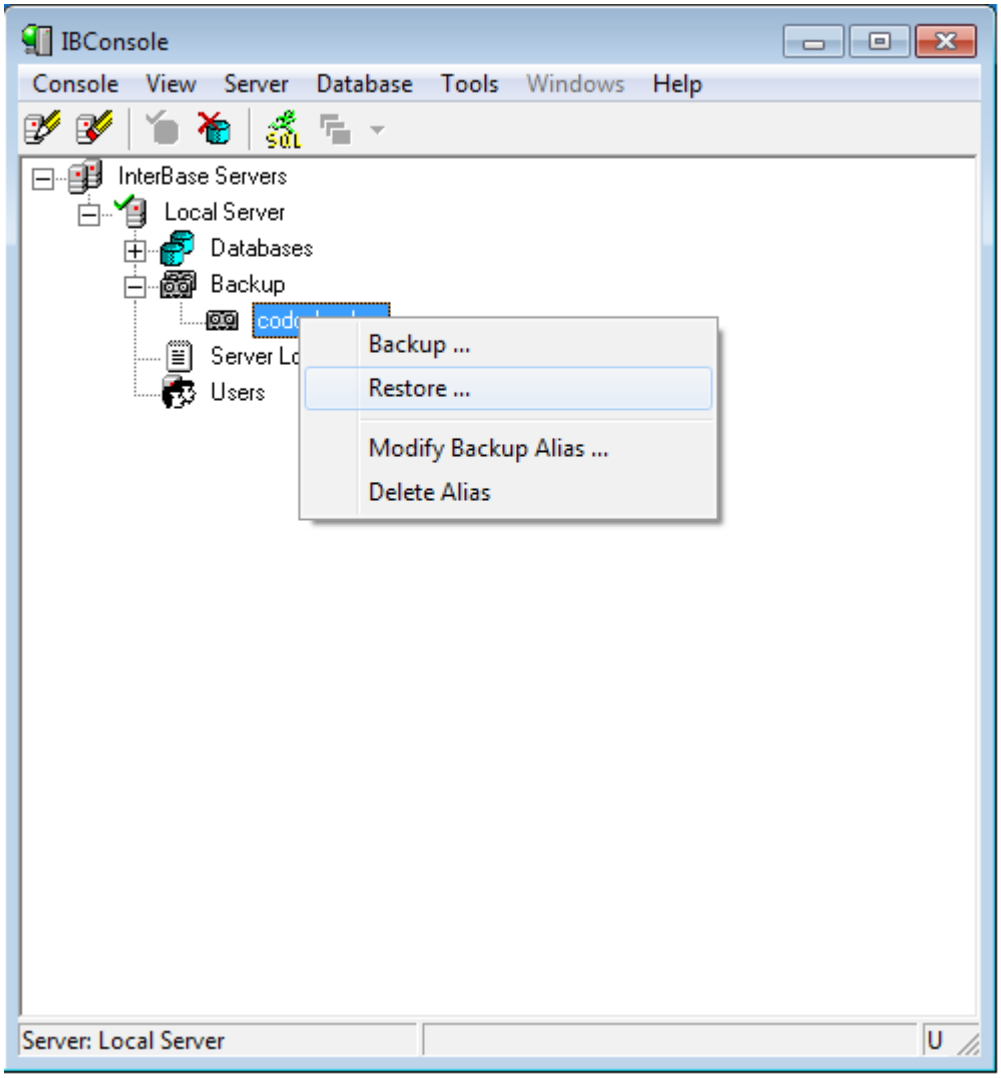



**Рисунок Е-1**

2. В панели «Backup File(s)» в строке «Alias» выбрать название файла архивного копирования.

3. В панели «Database» в строке «Server» выбрать «Local Server». В строке «Alias:» написать: «codos.gdb». В поле «Filename(s)» написать: «c:\restore\codos.gdb».
В панели «Options» установить «Page Size (Bytes)» - «8192». Нажать кнопку «ОК» (рисунок Е.2).

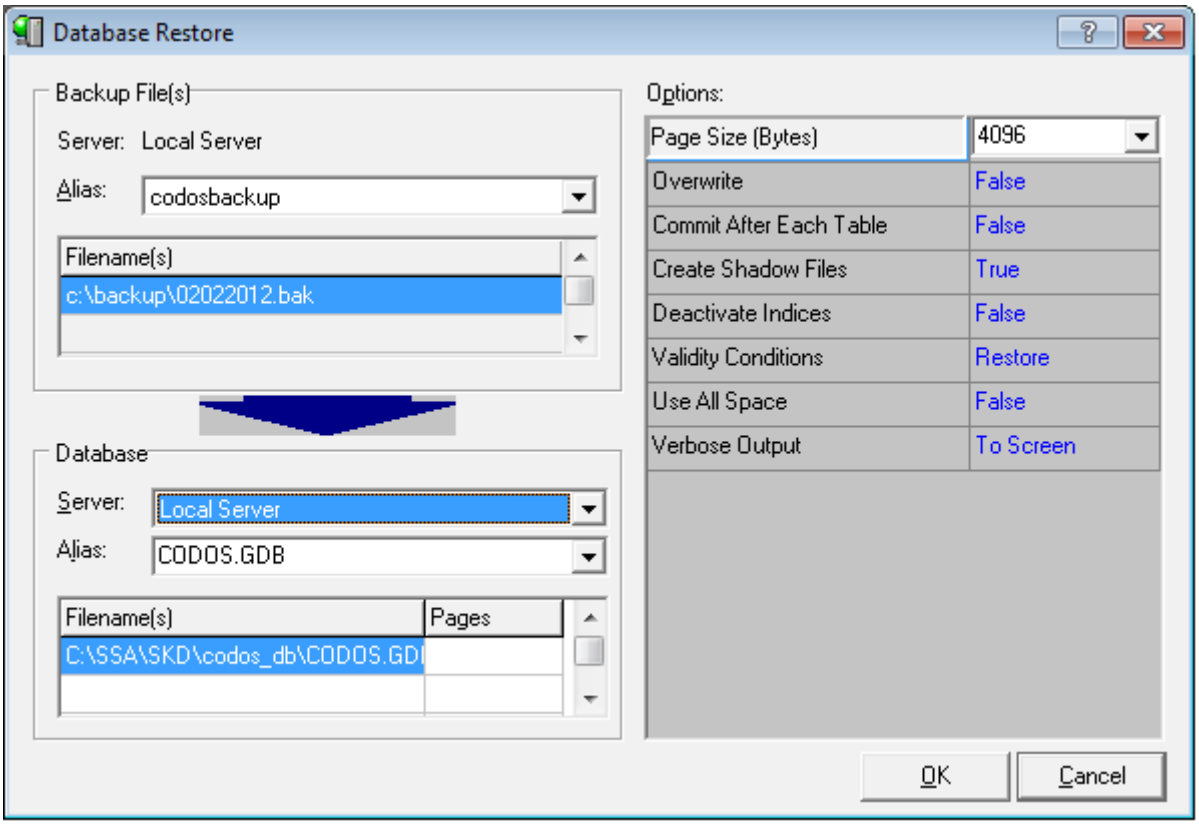



**Рисунок Е-2**

4. Начнется процедура «Restore». Она закончится после появления записи: «Service ended at …» (рисунок Е.3). После завершения процедуры «Restore» закрыть окно «Database Restore» и закрыть окно «IBConsole».

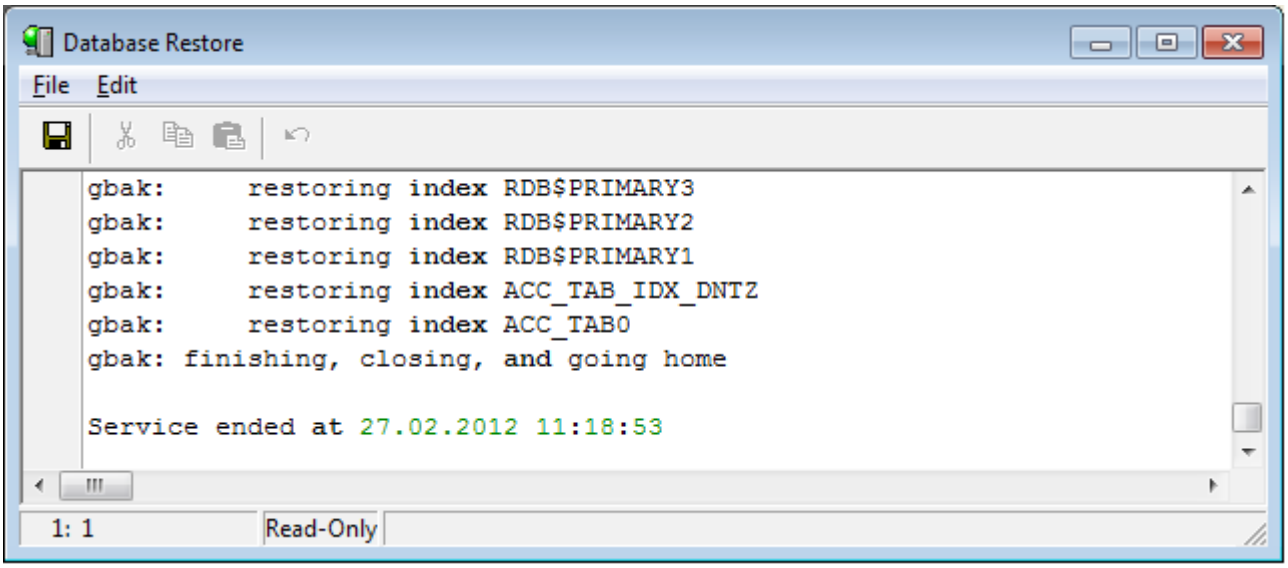



**Рисунок Е-3**

5. Файл базы данных из папки «c:\restore\» скопировать с заменой в папку: «c:\ssa\skd\codos_db\». Запустить «Сервер ИКБ».

## ПРИЛОЖЕНИЕ Ж Проверка базы данных средствами FireBird

Периодически рекомендуется проводить проверку БД на ошибки стандартными средствами Firebird.

1. Запустить «BDE администратор» - «Пуск»□«Настройки»□«Панель управления». Откроется окно «BDE Administrator …» (рисунок Ж.1)

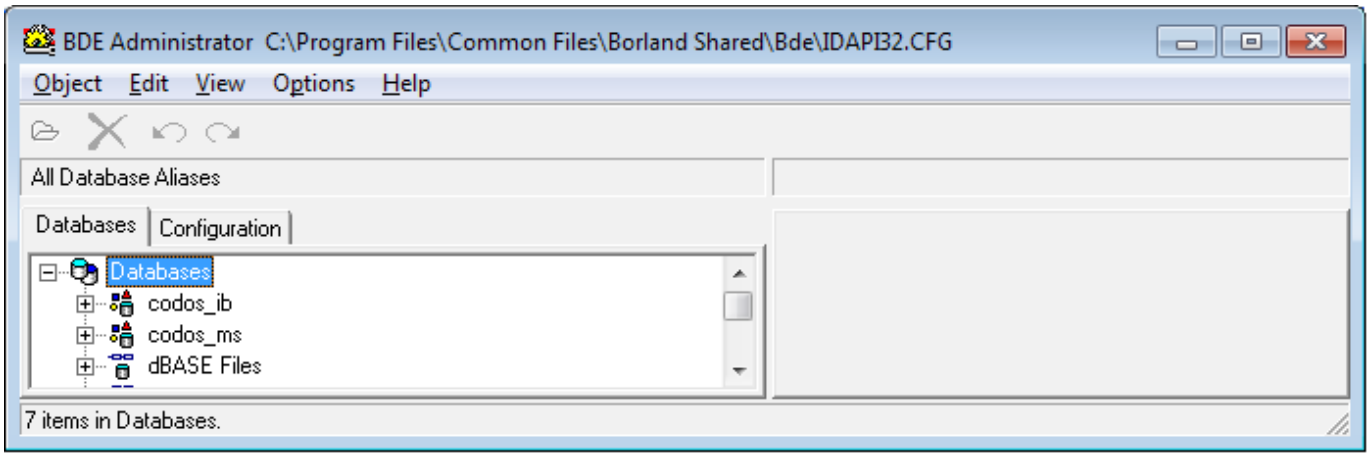



**Рисунок Ж-1**

2. Нажать имя рабочего «alias'а» базы данных (рисунок Ж.2). Путь, указанный в поле «SERVER NAME» указывает расположение файла базы данных на жёстком диске. Это и есть искомый файл базы данных.

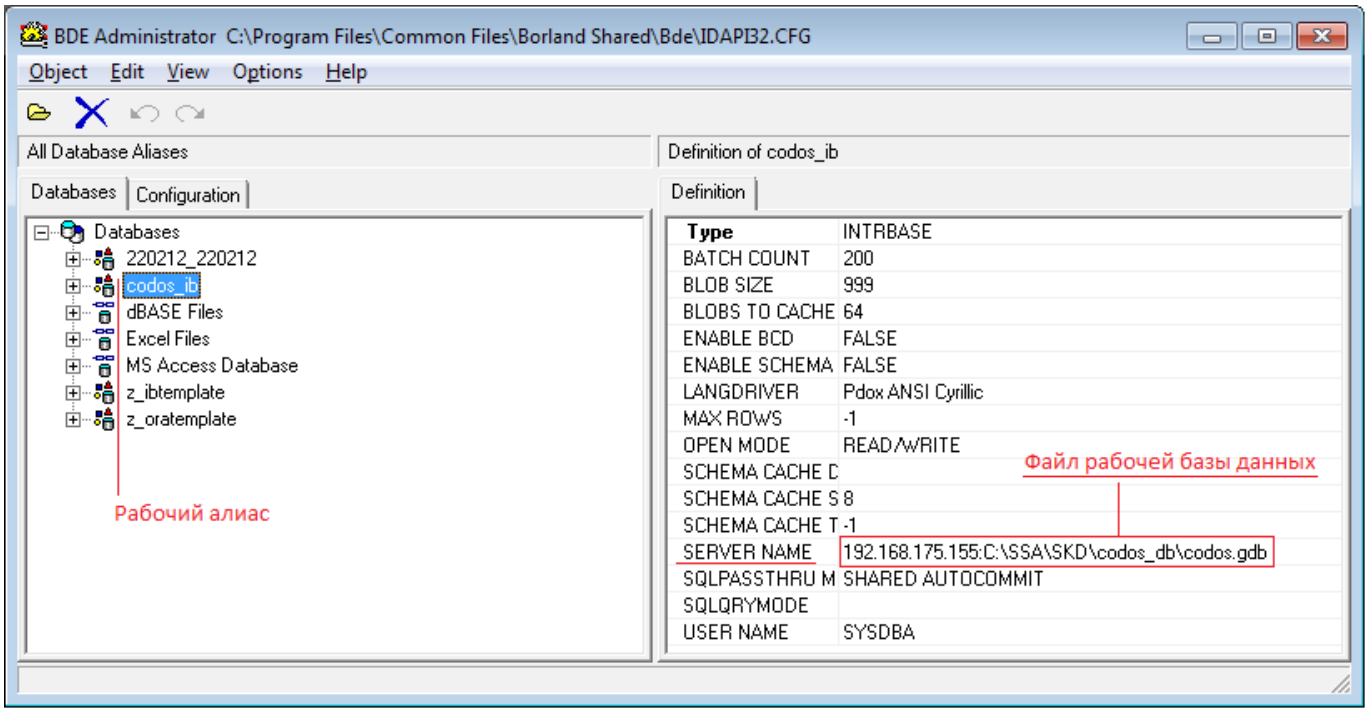



**Рисунок Ж-2**

3. Отключить «Сервер ИКБ» и «АРМ» связанные с «Сервером ИКБ».

4. Файл рабочей базы данных скопировать в директорию, созданную для проверки базы данных на жёстком диске компьютера или в директорию другого компьютера, где будет производиться проверка на ошибки БД СУБД Firebird. Например, БД из папки «c:\ssa\skd\codos_db\» скопировать в директорию «c:\bases\».

5. Скопировать, на случай отката, рабочую базу данных из папки «c:\ssa\skd\codos_db\» в директорию «c:\ xxxxxx \», где «xxxxxx» - дата проведения процедуры проверки.

6. Далее, «Пуск» → «Программы» → «Firebird» → «IBConsole» (рисунок Ж.3). Щелкнуть в строке «Local Server» правой клавишей мыши

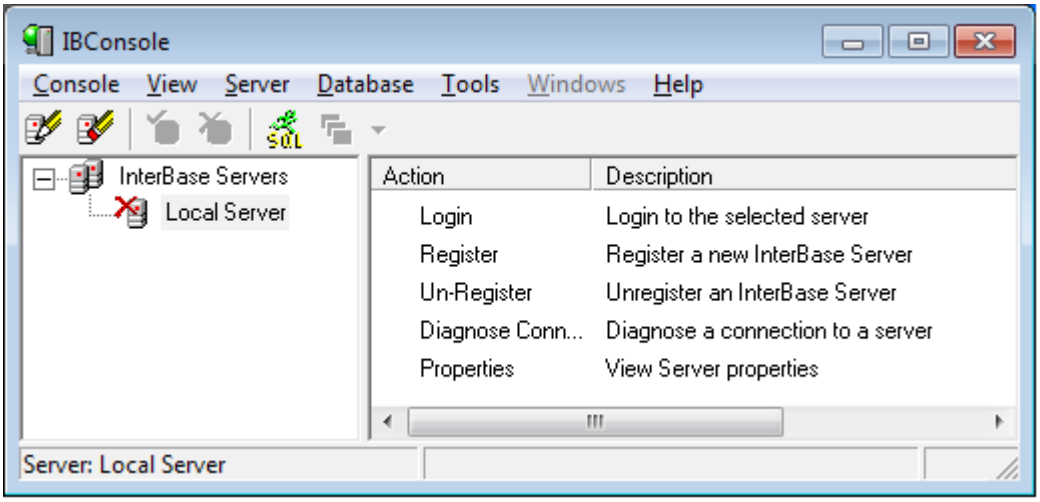



**Рисунок Ж-3**

7. Выбрать «Un-Register» (рисунок Ж.4)

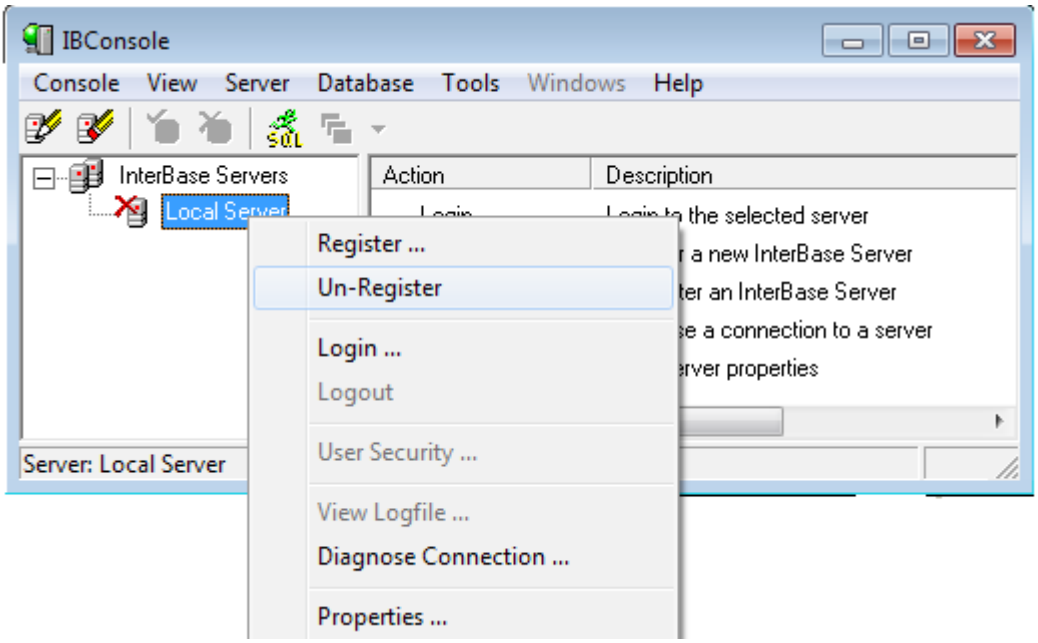



**Рисунок П7-4**

8. В окне «Confirm» нажать кнопку «Yes» (рисунок Ж.5).

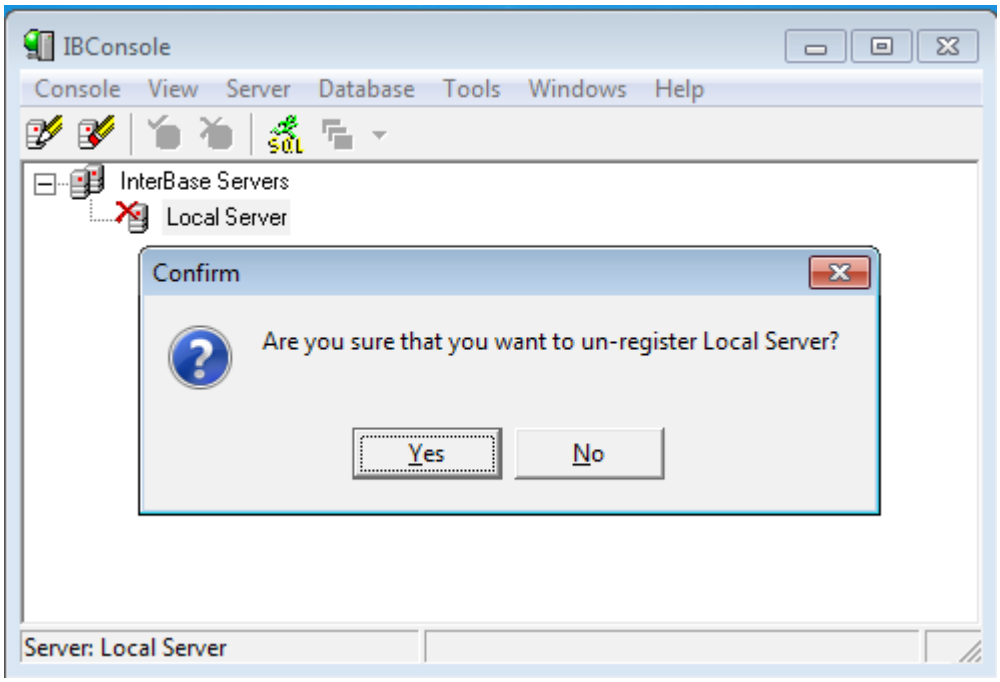



**Рисунок Ж-5**

9. Нажать «InterBase Servers» правой клавишей мыши. Выбрать «Register…» в выпавшем меню (рисунок Ж.6).

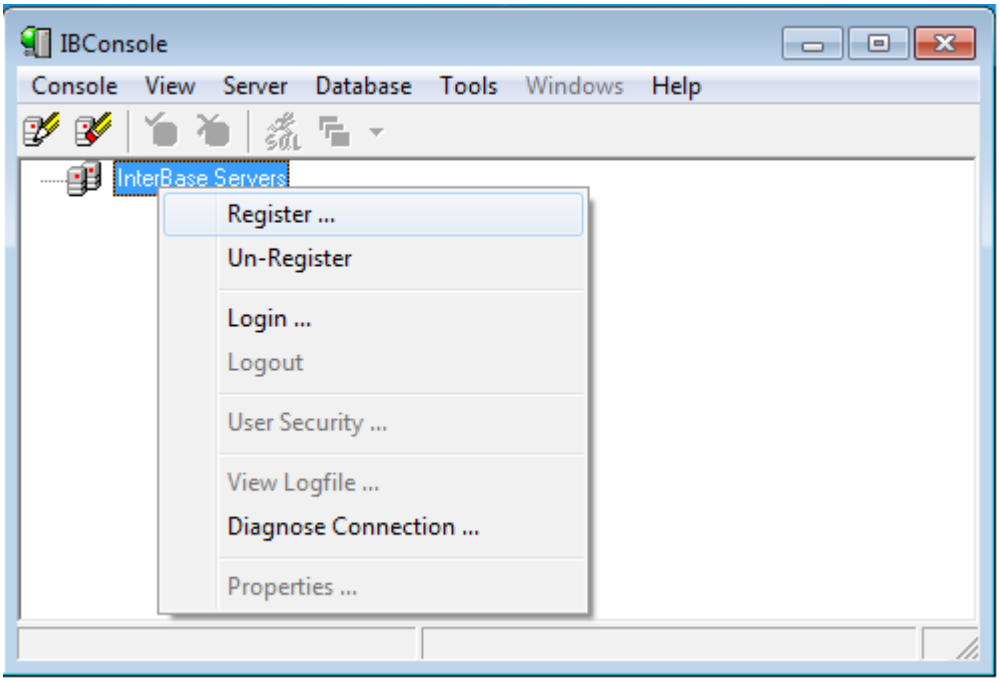



**Рисунок Ж-6**

10. В окне «Register Server and Connect» выбрать тип подключения «Local Server». В панели «Login Information», в строке «User Name:» ввести «sysdba». В строке «Password:» ввести «masterkey». После ввода информации нажать «ОК» (рисунок Ж.7). Имя и пароль указаны по умолчанию. Вводить необходимо действующие имя и пароль базы данных.

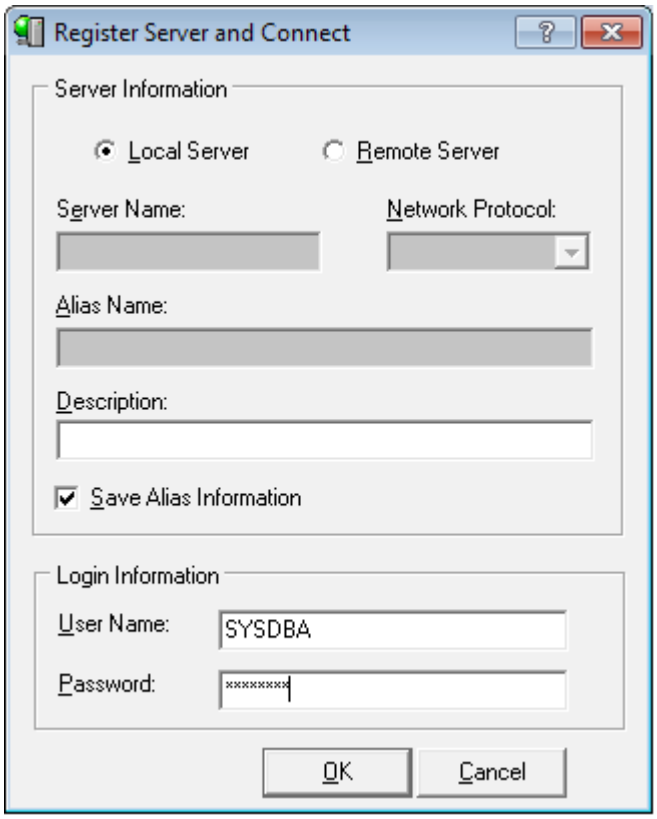



**Рисунок Ж-7**

11. Нажать ⊞ «Local Server». В появившемся списке нажать «Databases» правой кнопкой мыши. В выпавшем меню выбрать «Register» (рисунок Ж.8).

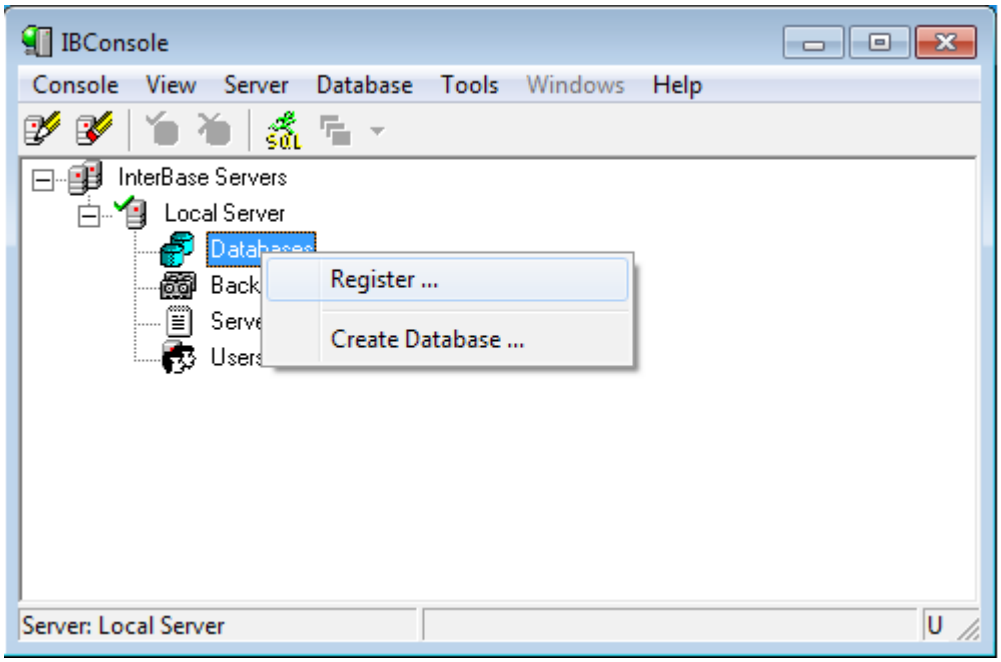



**Рисунок Ж-8**

12. В окне «Register Database and Connect» в панели «Database» нажать кнопку ..., указать файл копии рабочей базы данных из папки «c:\bases\». В строке «Login Information» ввести «sysdba» (по умолчанию). В строке «User Name» ввести пароль на базу данных «masterkey» (по умолчанию). Затем нажать кнопку «OK» (рисунок Ж.9).

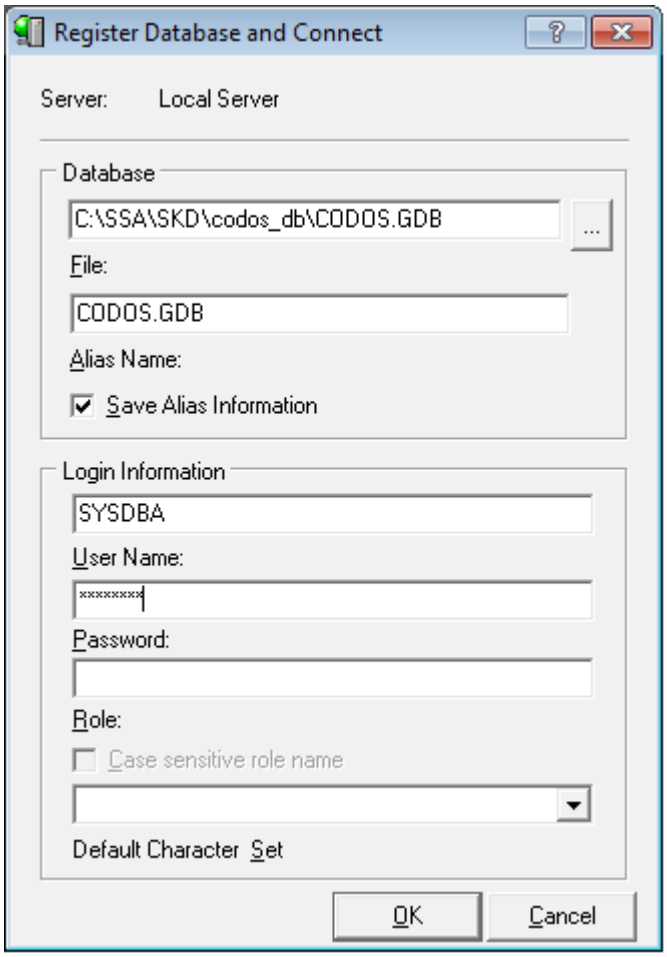



**Рисунок Ж-9**

13. Нажать ⊞ «Databases», в открывшемся списке нажать «CODOS.GDB» правой кнопкой мыши и в появившемся меню выбрать «Disconnect» (рисунок Ж.10).

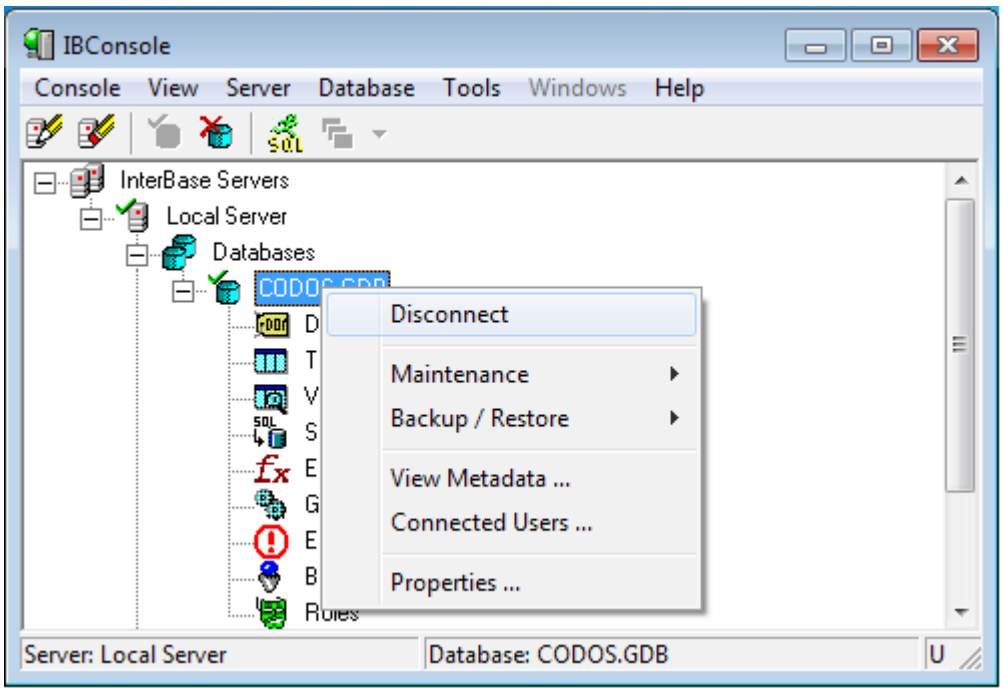



**Рисунок Ж-10**

14. В окне «Confirm» нажать кнопку «Yes» (рисунок Ж.11).

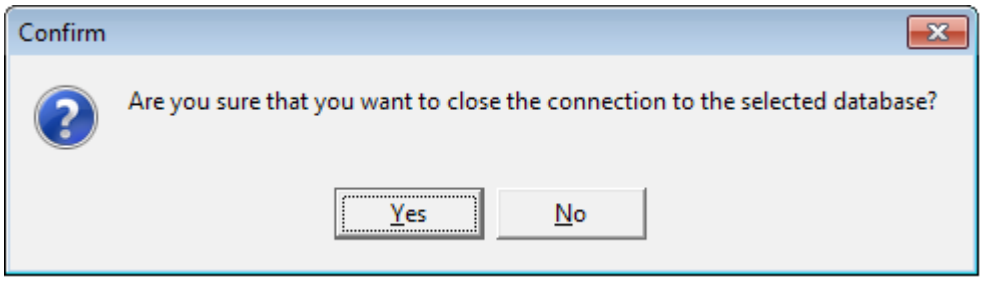



**Рисунок Ж-11**

15. Нажать «CODOS.GDB» правой клавишей мыши. В появившемся меню выбрать «Validation…» (рисунок Ж.12).

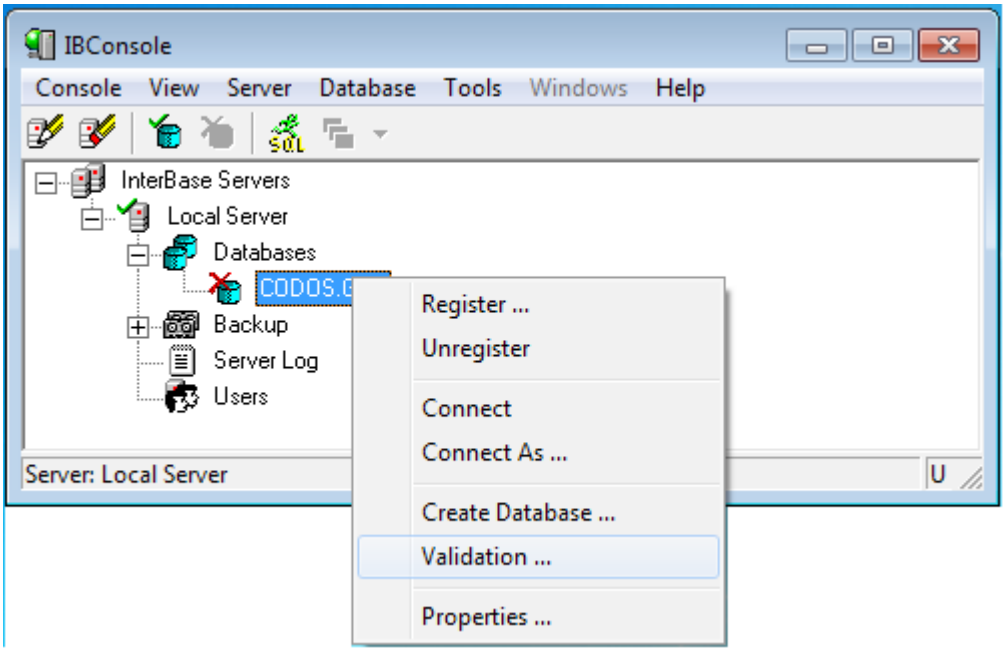



**Рисунок Ж-12**

16. В окне «Database Validation», в строке «Validate Record Fragments» нажать  и установить значение «True» (рисунок Ж.13). Нажать кнопку «OK».

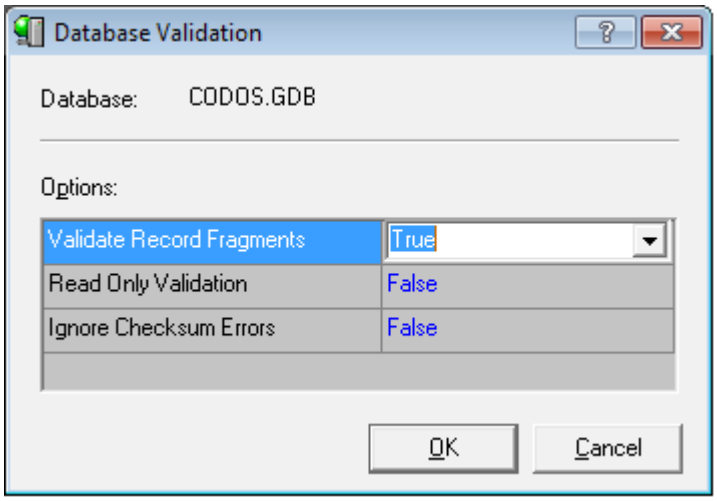



**Рисунок Ж-13**

Если в базе данных отсутствуют ошибки, то в окне «Validation Report» появится сообщение «No database validation errors were found» (рисунок Ж.14). Нажать «OK».

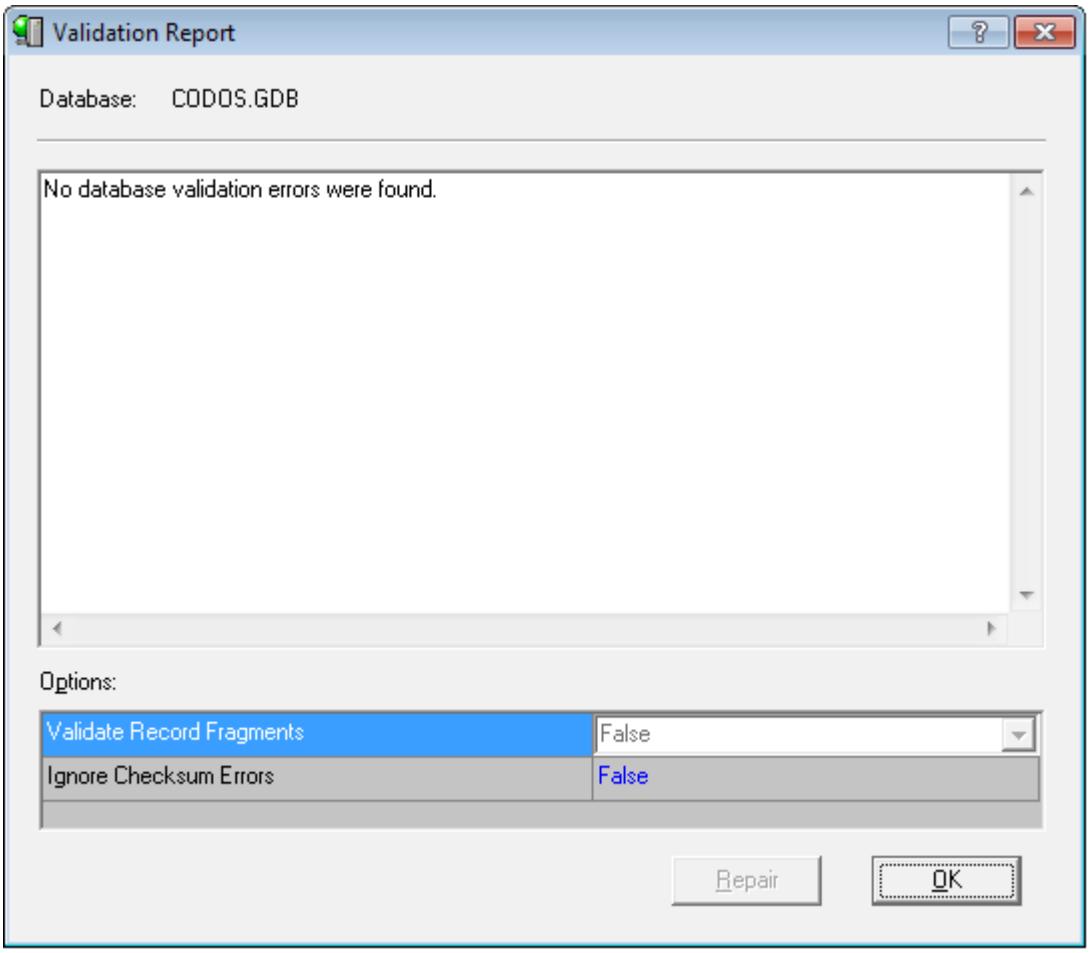



**Рисунок Ж-14**

Если в базе данных присутствуют ошибки, то возможны следующие варианты:

- Окно «Validation Report» сформирует отчёт о найденных ошибках и отчёт о том, что все эти ошибки исправлены.
- Окно «Validation Report» сформирует отчёт о найденных ошибках и отчёт о том, что найденные ошибки не удаётся исправить средствами «IBConsole». Тогда необходимо обратиться в отдел технической поддержки ООО «КОДОС».

После устранения ошибок базы данных необходимо выполнить процедуры «Backup/Restore».

Если в файле базы данных были обнаружены и исправлены ошибки, проведёны архивное копирование и восстановление отремонтированной базы данных, то необходимо файл базы данных из папки «c:\bases\» скопировать с заменой в папку: «c:\ssa\skd\codos_db\».

Запустить «Сервер ИКБ».

# ПРИЛОЖЕНИЕ 3 Образцы таблиц программирования

## 3.1 Установка параметров СК-Е

| № п.п | Параметры конфигурации | СК-Е | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | … | N |
| 1 | Обозначение | | | | | |
| 2 | Имя | | | | | |
| 3 | Описание | | | | | |
| 4 | IP-адрес | | | | | |
| 5 | Порт | | | | | |

Пример заполнения:

| № п.п | Параметры конфигурации | 1 |
|---|---|---|
| 1 | Обозначение | S12 |
| 2 | Имя | СКЕ-корпуса1 |
| 3 | Описание | корпус1этаж2 |
| 4 | IP-адрес | 192.168.139.1 |
| 5 | Порт | 21305 |

## 3.2 Установка параметров А-20

| №п.п. | Параметры конфигурации | 1 | 2 | 3 | … | N |
|---|---|---|---|---|---|---|
| 1 | Обозначение | | | | | |
| 2 | Наименование | | | | | |
| 3 | Адрес | | | | | |

Пример заполнения:

| №п.п. | Параметры конфигурации | 1 |
|---|---|---|
| 1 | Обозначение | A1 |
| 2 | Наименование | Периметр |
| 3 | Адрес | 1 |

## 3.3 Установка параметров зон и каналов

| Тип АБ | Параметры конфигурации | Номера зон | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | … | 200 |
| | Обозначение | | | | | |
| | Описание (наименование) | | | | | |
| | Объект | | | | | |
| | Владелец | | | | | |
| | Тип датчика | | | | | |
| A-06/2<br>A-06/8 | Ставить на охрану | | | | | |
| | Контроль шлейфа | | | | | |
| | Отложенное срабатывание | | | | | |
| | Автопостановка | | | | | |
| A-07/4<br>A-07/8 | Ставить на охрану | | | | | |
| | Нормально-замкнутый | | | | | |
| | Контроль шлейфа | | | | | |
| | Отложенное срабатывание | | | | | |
| | Отложенная постановка | | | | | |
| | Автопостановка | | | | | |
| A-08,<br>A-08/24,<br>A-08/220,<br>A-08/220A | Канал активен | | | | | |
| | Контроль канала | | | | | |
| | Отложенное срабатывание | | | | | |
| | Время работы | | | | | |
| A-09 | Ставить на охрану | | | | | |
| | Нормально-замкнутый | | | | | |
| | Контроль шлейфа | | | | | |