Подсистема администрирования

Руководство пользователя

Январь, 2002 г.

KASKAD Development Team

Содержание:

Описание.

Подсистема администрирования предназначена для ограничения доступа пользователей к различным ресурсам SCADA-системы «КАСКАД». Управление подсистемой осуществляется «Конфигуратором подсистемы администрирования» (КПА). Исполняемый файл КПА - SheriffCfg.exe.

КПА позволяет:

1. Регистрировать и удалять приложения, доступ к функциям которых нужно разрешить/запретить.
2. Управлять пользователями SCADA-системы «КАСКАД». Сюда входит добавление и удаление пользователей, объединение пользователей в группы для удобства администрирования, добавление и удаление групп, настройка пользователей.
3. Настраивать права на доступ пользователей к ресурсам системы. Можно назначить/запретить следующие права:
   - На различные действия пользователя в системе.
   - На доступ пользователя к системе в определенное время.
   - На доступ пользователя к системе с разных рабочих станций.
   - На доступ пользователя к технологическим параметрам (паспортам) по записи и по чтению.

Для интеграции подсистемы администрирования в SCADA-систему служит динамически подключаемая библиотека «Sheriff.dll», которую загружают приложения системы и вызывают ее функции для проверки прав пользователей на выполнение своих защищенных действий. Наличие этого модуля в каталоге исполняемых файлов (<Kaskad>\Bin) является обязательным условием функционирования системы, так как без этого модуля приложения работать не будут.

Подсистема администрирования имеет клиент - серверную архитектуру. Рабочие станции, на которых выполняются приложения SCADA-системы, выполняющие обращение к подсистеме администрирования (ПА) являются клиентами в этой архитектуре. Для работы подсистемы должен существовать по

крайней мере один сервер администрирования, на котором хранится БД пользователей и осуществляется вся настройка подсистемы. Этот сервер может размещаться на одной из рабочих станций, либо на выделенном сервере. Станции должны быть объединены в сеть, поддерживающую протокол TCP\IP. Возможен также вариант, когда клиент и сервер размещаются на одной рабочей станции. В этом случае наличие сети между станциями необязательно.

Всю информацию о пользователях подсистема хранит в базе данных пользователей, управляемой через сервер СУБД InterBase. Таким образом, для функционирования подсистемы на клиентской РС необходимо наличие на этой РС установленной клиентской части InterBase. А на сервере администрирования, где ведется БД пользователей, обязательно наличие как клиентской, так и серверной части InterBase.

Установка.

Установка ПА осуществляется на станции, где располагается сервер администрирования. Перед установкой подсистемы необходимо убедиться в доступности с этой станции всех исполняемых модулей приложений SCADA-системы, использующих функции подсистемы (они должны располагаться на локальном диске или на доступном сетевом ресурсе). Необходимо также убедиться в наличии установленной InterBase (клиент и сервер). Если СУБД InterBase была установлена только что, рекомендуется сменить пароль для пользователя SYSDBA, который имеется у этой учетной записи InterBase по умолчанию при установке сервера InterBase. Для этого запустите приложение IBConsole.exe (устанавливается вместе с InterBase), зарегистрируйтесь на локальном сервере, оставив имя учетной записи SYSDBA и введя пароль по умолчанию для только что установленного InterBase сервера - «masterkey» (маленькими латинскими буквами). Затем выберите пункт меню Server->User Security. Введите новый пароль (там, где звездочки), нажмите Apply. Закройте диалог и приложение.

Для установки подсистемы также необходимо наличие модуля `rtp_udf.dll` в подкаталоге \UDF установленного сервера InterBase. Рекомендуется закрыть доступ к этому файлу для пользователей как по записи, так и по чтению. Для

полноценного функционирования ПА необходимо (и достаточно), чтобы доступ к этому файлу по чтению был у учетной записи SYSTEM, ели операционная система на этой станции Windows NT/2000.

Далее необходимо запустить конфигуратор подсистемы администрирования (КПА). Он сообщит, что БД пользователей не существует и предложит настроить подключение к ней. В окне «параметры БД пользователей» (рис. 1) нужно выбрать

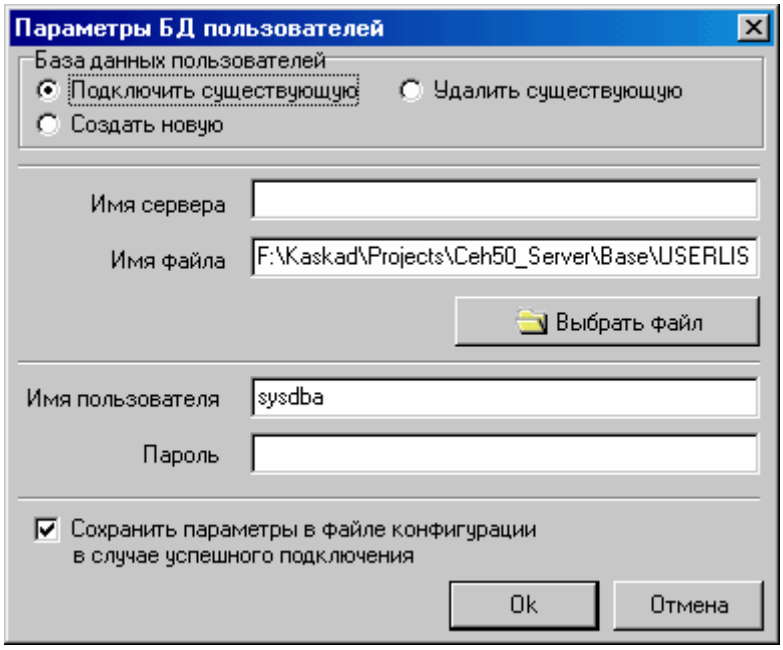

Рис. 1. Параметры БД пользователей.

«создать новую БД», указать путь к файлу БД и параметры подключения - имя пользователя и пароль учетной записи InterBase. Рекомендуется создавать БД в недоступном пользователям месте (на защищенном диске или сетевом ресурсе). Затем КПА сообщит о необходимости создания учетной записи администратора и выведет диалог для этого. После успешного создания администратора система готова к работе. Только что созданного администратора нельзя удалить. Также у него нельзя отобрать администраторские права. Это необходимо для невозможности случайного удаления всех пользователей, которые могли бы осуществлять настройку ПА.

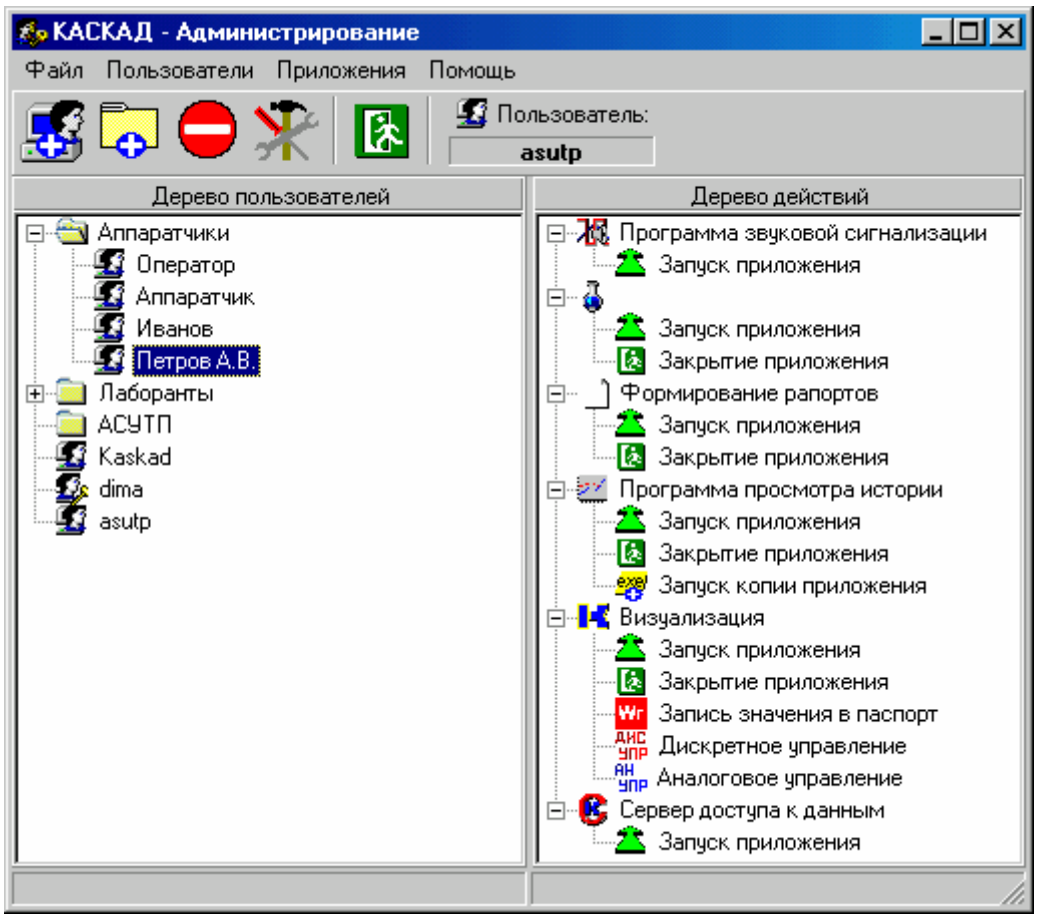

Рис. 2. Конфигуратор подсистемы администрирования. Главное окно.

Теперь можно зарегистрировать приложения SCADA-системы, использующие подсистему администрирования. Для этого выберите пункт главного меню «Приложения», щелкните на пиктограмме «добавить приложение». В появившемся диалоге выберите нужные приложения и нажмите кнопку «ОК».

Настройка сервера администрирования.

Пользователи с правами администратора имеют доступ ко всем защищенным действиям системы.

Назначение и запрещение прав других пользователей на выполнение защищенных действий системы осуществляется путем установки/снятия «галочек» и «крестиков» в списках действий на закладке «Действия» настроек пользователя/группы (см рис. 3.).

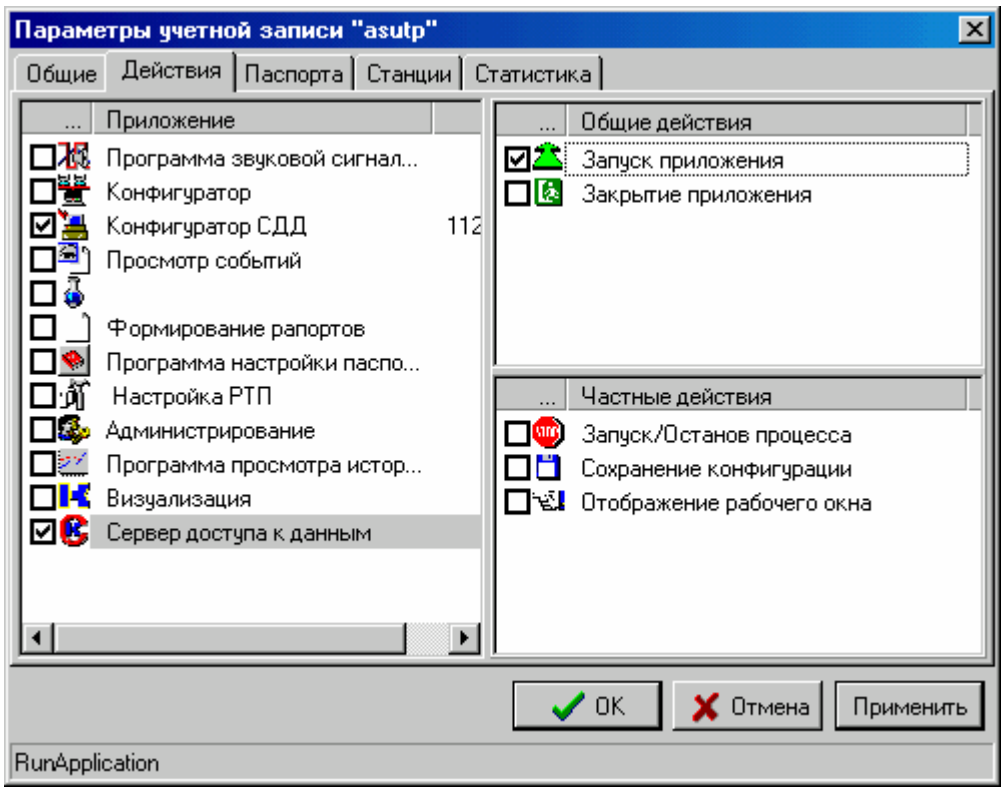

Рис. 3. Параметры учетной записи.

Будет ли действие разрешено пользователю, определяется как настройками группы на данное действие, в которой состоит пользователь, так и настройками самого пользователя на это действие. Если в этих двух полях настроек есть хотя бы одна «галочка», и нет ни одного «крестика», то данное действие пользователю разрешено. Разрешенные действия отображаются в правой части главного окна КПА в виде дерева.

На других закладках диалогового окна конфигурации пользователя можно осуществлять другие настройки пользователей:

Закладка «Общие».

- Полное имя.

Можно изменить полное имя пользователя

- Изменить группу.

Изменить группу пользователя.

- Назначить права администратора.

- Потребовать смену пароля при следующем входе.

Когда пользователь попробует войти в систему, ему будет предложено сменить его пароль.

- Разрешить смену пароля пользователем.

Если отмечена, пользователь сможет менять свой пароль по своему усмотрению с любой клиентской PC.

- Разрешить запоминать имя и пароль на локальной PC.

Если отмечена, пользователь сможет назначить себя пользователем по умолчанию или отменить это назначение на клиентской PC.

- Запомнить имя и пароль текущего пользователя.

Назначить конфигурируемого пользователя пользователем по умолчанию на текущей PC.

- Срок действия пароля, дней.

Если выставить значение, большее нуля, то, если пользователь вошел в систему, и с момента последней смены его пароля прошло больше времени, чем это значение, ему будет предложено сменить его пароль.

- Сменить пароль.

Вызывает диалог смены пароля пользователя.

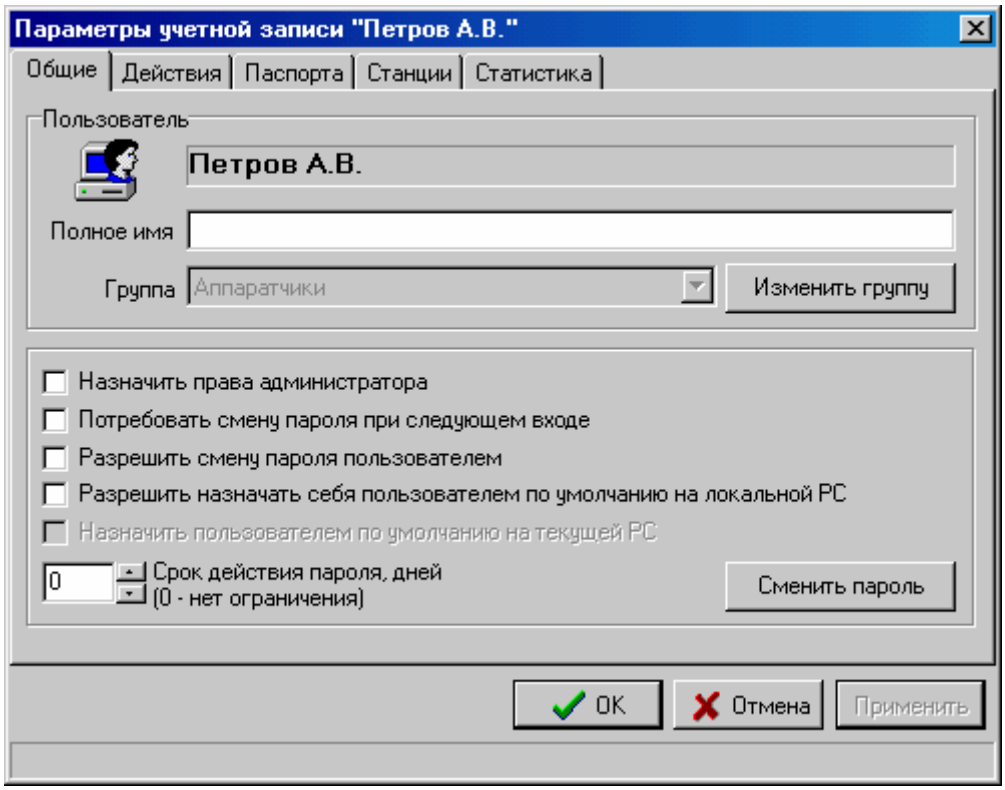

Рис. 4. Закладка «Общие»

Закладка «Паспорта».

Здесь можно выбрать диапазоны паспортов, для разрешения или запрета пользователю доступа к ним по записи или чтению. Для каждого пользователя определяются четыре множества паспортов:

1. Паспорта, разрешенные для чтения.
2. Паспорта, запрещенные для чтения.
3. Паспорта, разрешенные для записи.
4. Паспорта, запрещенные для записи.

Те же самые множества определяются и для группы, в которую входит пользователь. Разрешение на доступ пользователя к конкретному паспорту определяется следующим образом: если паспорт входит в объединение множеств разрешенных паспортов для группы и пользователя и не входит в объединение множеств запрещенных, то доступ разрешен.

Контроль доступа пользователей к паспортам осуществляет Сервер доступа к данным.

Закладка «Время работы».

Закладка «Станции».

Закладка «Статистика».

Настройка клиентской РС.

При первом запуске или при переконфигурировании SCADA-системы на клиентской РС, ПА сообщит, что не может связаться с БД пользователей и даст возможность указать расположение этой БД. В этом случае появится окно «Параметры БД пользователей», подобное окну на рис. 1, в котором следует указать имя сервера, где располагается БД, локальный путь файла БД на сервере, имя учетной записи и пароль сервера InterBase, установленного там. Оставьте галочку «сохранить параметры…» включенной и нажмите «ОК».

Работа.

Под запуском SCADA-системы будем понимать запуск первого приложения системы с защищенными действиями. Под входом в систему будем понимать первую проверку права пользователя на выполнение какого-либо действия. Обычно, это проверка права на запуск первого приложения системы (имеется в виду «первого» по времени запуска).

При входе в систему ПА ищет **пользователя по умолчанию** для данной РС. Если такой пользователь не найден, ПА запрашивает имя и пароль пользователя. (рис. 5). Если пользователь с таким паролем существует, ПА проверяет его права

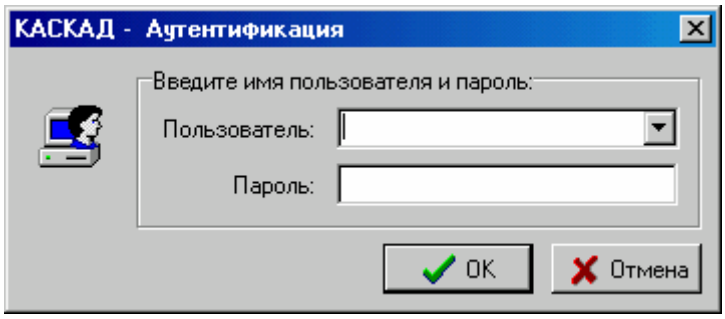

Рис. 5. Аутентификация

на вход в систему (см. абзац выше). Если его прав достаточно на выполнение этого действия, то осуществляется вход в систему, а этот пользователь становится **базовым пользователем** системы (не путать с пользователем по умолчанию).

В дальнейшем, при проверке прав пользователя на выполнение действий, ПА проверяет права **базового пользователя**. Если его прав недостаточно, ПА отображает окно, где сообщает об этом и предлагает ввести имя и пароль пользователя, которому разрешено производить действие (рис. 6).

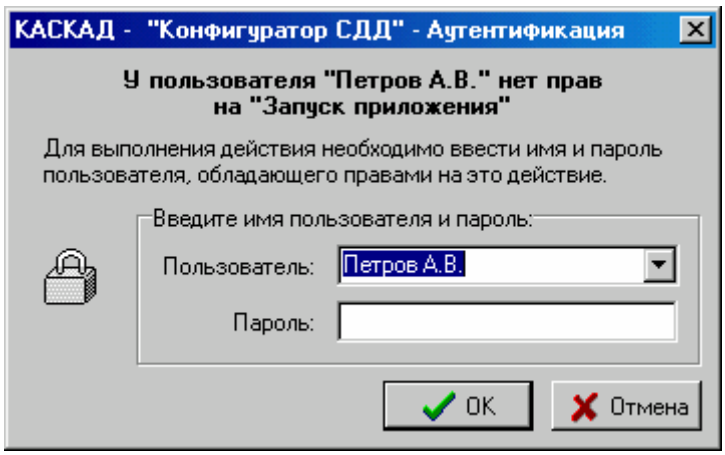

Рис. 6. Доступ запрещен

Если в этом окне введено имя и пароль пользователя с достаточными правами, действие выполняется, но базовый пользователь остается прежним. Таким образом, в следующий раз, когда пользователь пытается повторно выполнить это же действие, ПА вновь попросит его ввести имя и пароль пользователя с достаточными правами.

Базового пользователя системы можно сменить, выбрав пункт меню «пользователь» (см. ниже).

После выхода из SCADA-системы (выгрузка последнего приложения) базовый пользователь перестает существовать, а пользователь по умолчанию остается (если он был задан).

Пользователь может назначить себя пользователем по умолчанию, сменить свой пароль (если эти действия ему разрешены) или сменить базового пользователя, выбрав пункт меню «пользователь». При этом появиться диалоговое окно, отображенное на рис 7.

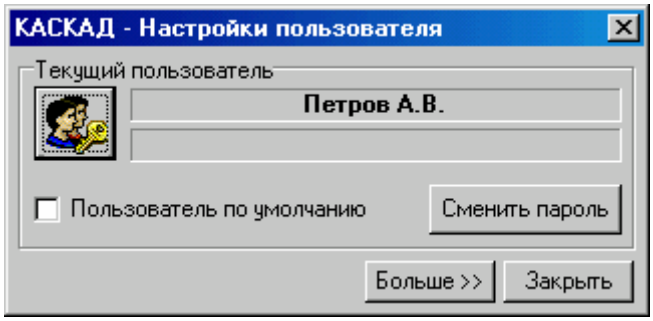

Рис. 7. Настройки пользователя

Здесь можно сменить базового пользователя, щелкнув на кнопку с пиктограммой «Пользователи». Например, администратор может назначить себя базовым пользователем системы. После этого практически все защищенные действия будут выполняться беспрепятственно. Для возврата системы в исходное состояние, надо сменить базового пользователя на предыдущего.

Здесь можно также сбросить базового пользователя. После выполнения этого действия при попытке выполнить любое защищенное действие, будет запрошена регистрация пользователя (рис. 7) с последующей установкой зарегистрированного пользователя как базового.