Система защиты информации от несанкционированного доступа ППО АСФК.

- Назначение и условия применения
- Описание операций:

- Администрирование объектов доступа
- Настройка параметров идентификации и аутентификации пользователей
- Администрирование подсистемы аудита
- Конфигурирование АРМ СБ
- Настройка партнерских систем
- Архив

- Возможные ошибки и способы их устранения

Четырехуровневая модель обеспечения информационной безопасности

Внешний уровень определяет взаимодействие АСФК с системами других организаций. На этом уровне должны пресекаться, как попытки внешних нарушителей несанкционированно получить, или нанести ущерб информационным сервисам АСФК, так и попытки собственных внутренних нарушителей осуществить подобные операции по отношению к внешним сервисам или несанкционированно передать конфиденциальную информацию.
В АСФК на этом уровне, в открытом контуре, реализована защита с помощью АПКШ «Континент». В защищенном контуре непосредственное взаимодействие с внешними системами отсутствует.
Сетевой уровень связан с функционированием объектов АСФК.
Безопасность информации на этом уровне обеспечивается средствами проверки подлинности пользователей и разграничением доступа к ресурсам локальной сети (аутентификация и авторизация).
Системный уровень связан, прежде всего, с управлением доступом пользователей к ресурсам ОС на компьютерах.
Именно на этом уровне реализуется непосредственное взаимодействие с пользователями, запускаются приложения, определяется политика взаимодействия между ППО и пользователем.
Защита информации на данном уровне заключается в определении, к каким ресурсам ОС и приложениям, какой пользователь, когда и с какими правами может быть допущен. Достигается применением агентов СЗИ SecretNet для платформы Windows.
Уровень приложений связан с использованием прикладных ресурсов АСФК.
Приложения работают с пользовательскими данными, поэтому для них необходимы собственные механизмы защиты.

Ресурсы АСФК подлежащие защите

Внешний уровень.

На внешнем уровне каналы связи защищаются в зависимости от типа взаимодействия ОрФК с ДУБП. При использовании ДУБП VPN-клиента Континент-АП шифрование трафика происходит средствами Континент, на сервере доступа Континент дается доступ ДУБП только к тем ресурсам ОрФК, которых достаточно для ведения бюджетного процесса.

При использовании шлюза TCP, доступный ресурс – сервер СУФД, шлюза MAIL –

Структура СЗИ НСД АСФК:

Сервер безопасности (СБ);

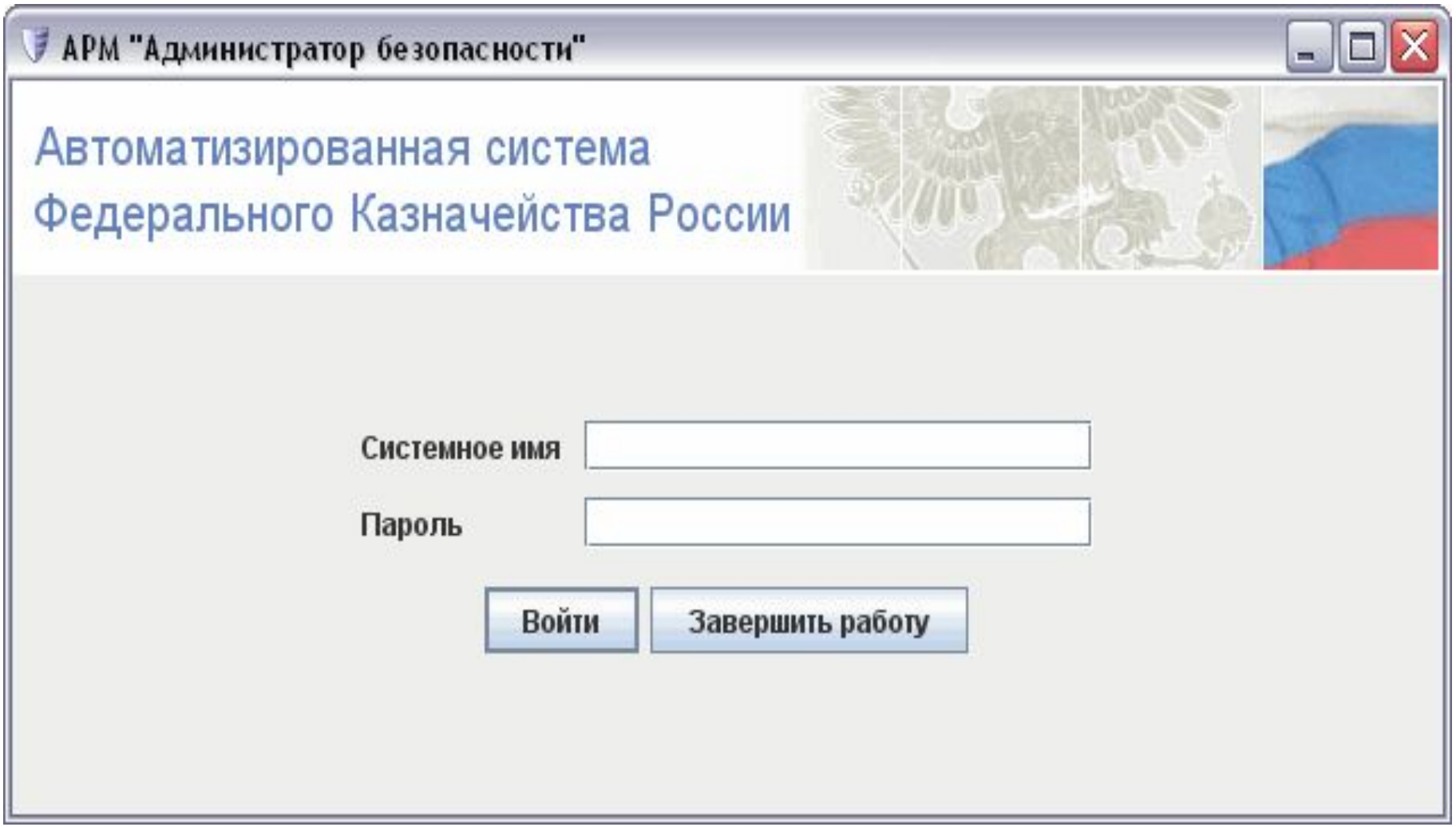
Агент Сервера безопасности;

АРМ Администратора безопасности

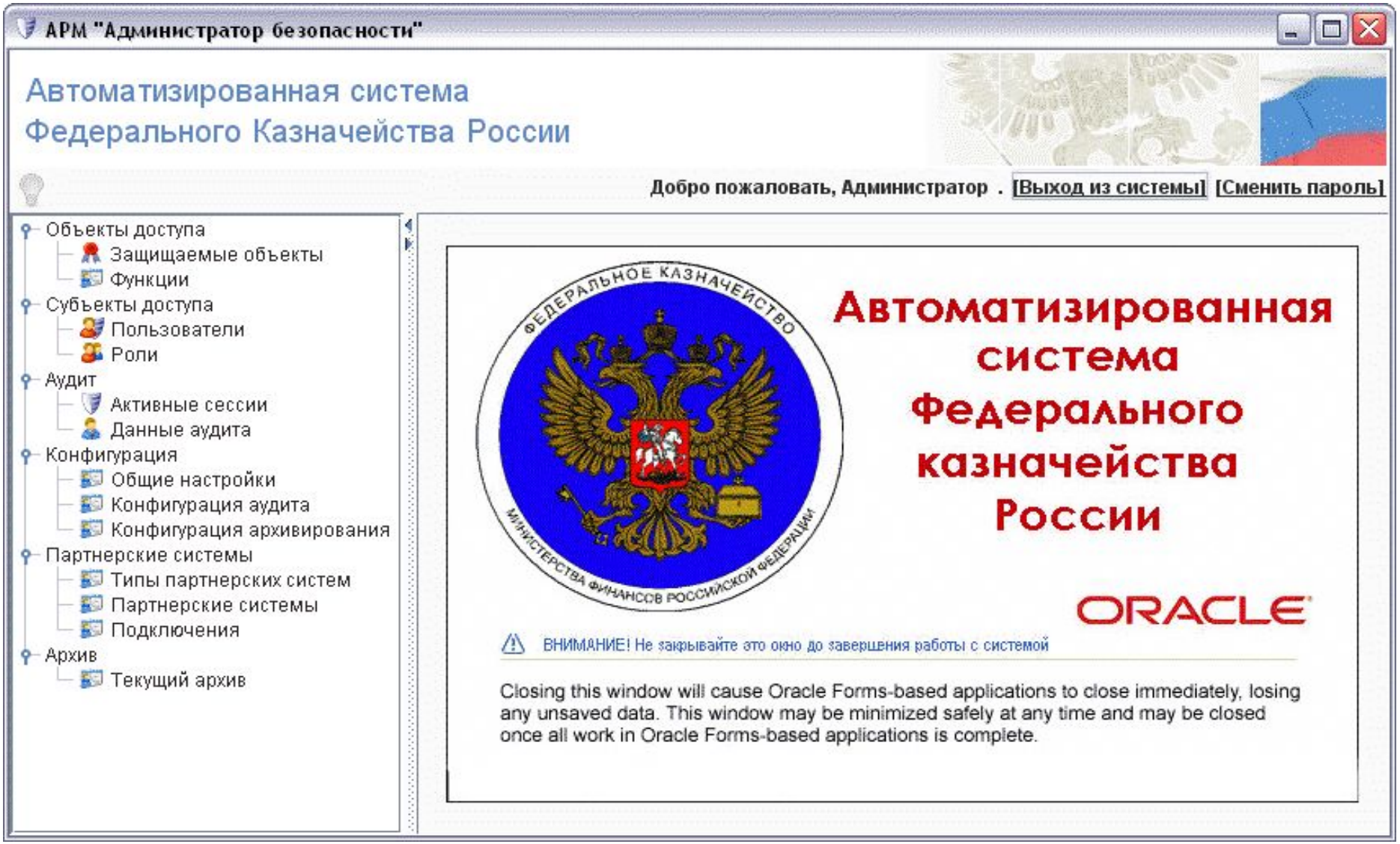
Логическая схема взаимодействия клиентского и серверного ППО с сервером безопасности

Архитектура СБ

Окно авторизации



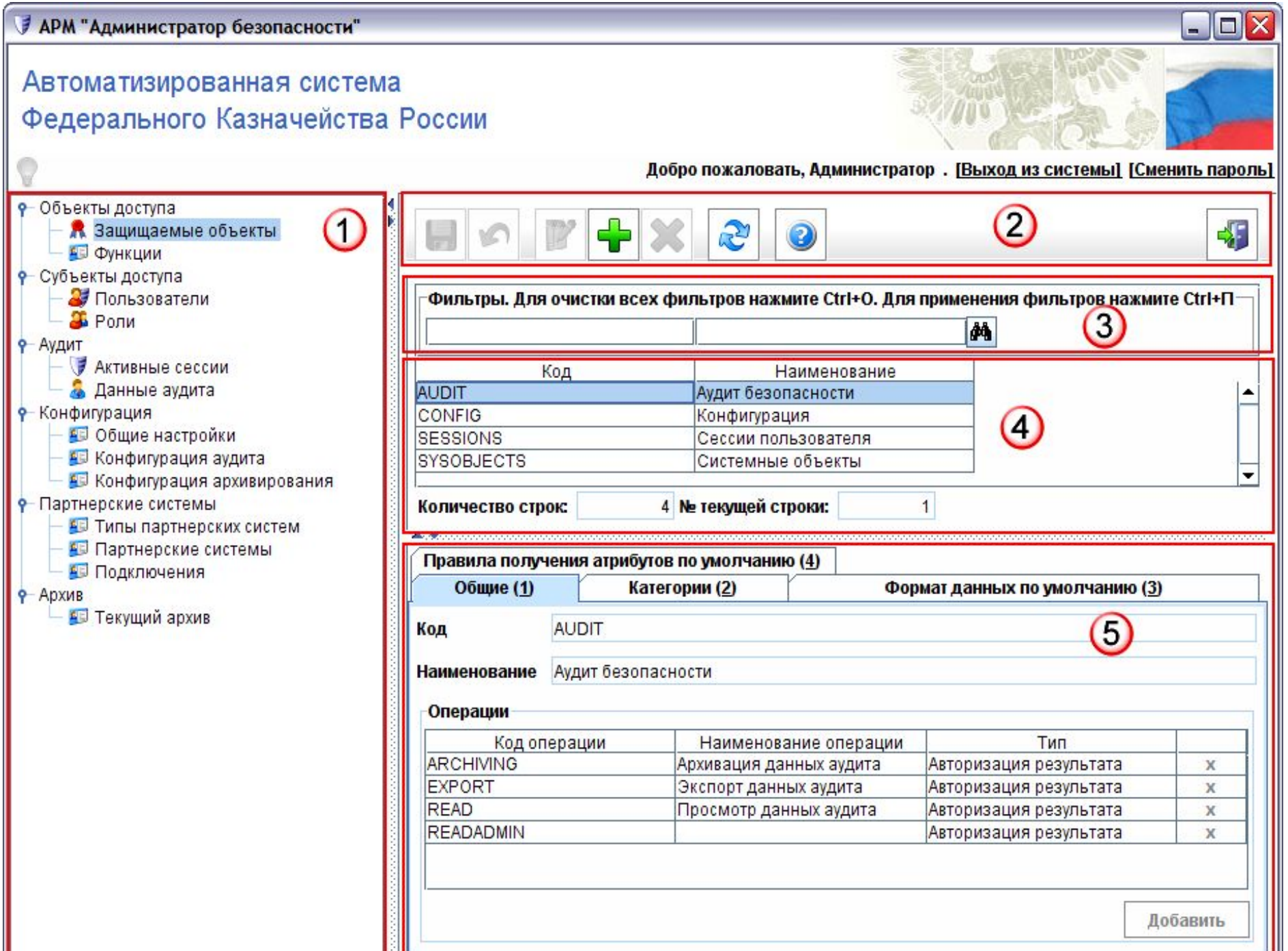
Главное окно АРМ «Администратор безопасности»



Главное окно АРМ «Администратор безопасности»

В левой части окна расположена панель навигации (1), позволяющая получить доступ к настройкам объектов администрирования и настройкам конфигурации сервера.
На панели инструментов (2) расположен набор кнопок, каждая из которых соответствует определенной операции.
Система фильтров (3) предназначена для быстрого поиска необходимых данных при работе с АРМ.
Перечень объектов администрирования отображается в правой части окна АРМ в виде списка (4). Если речь идет о разделах АРМ предназначенных для конфигурирования СБ, то вместо списка объектов в правой части окна могут располагаться группы полей для настройки СБ.
Подробная информация о параметрах каждого объекта из списка (4) отображается на закладках (5), расположенных ниже списка. На этих же закладках происходит редактирование параметров выделенного объекта.

Интерфейс АРМ «Администратор безопасности»



Операции в АРМ «Администратор безопасности»

Администрирование объектов доступа

. Настройка параметров идентификации и аутентификации пользователей
. Администрирование подсистемы аудита
. Конфигурирование АРМ СБ
. Настройка партнерских систем
. Архив

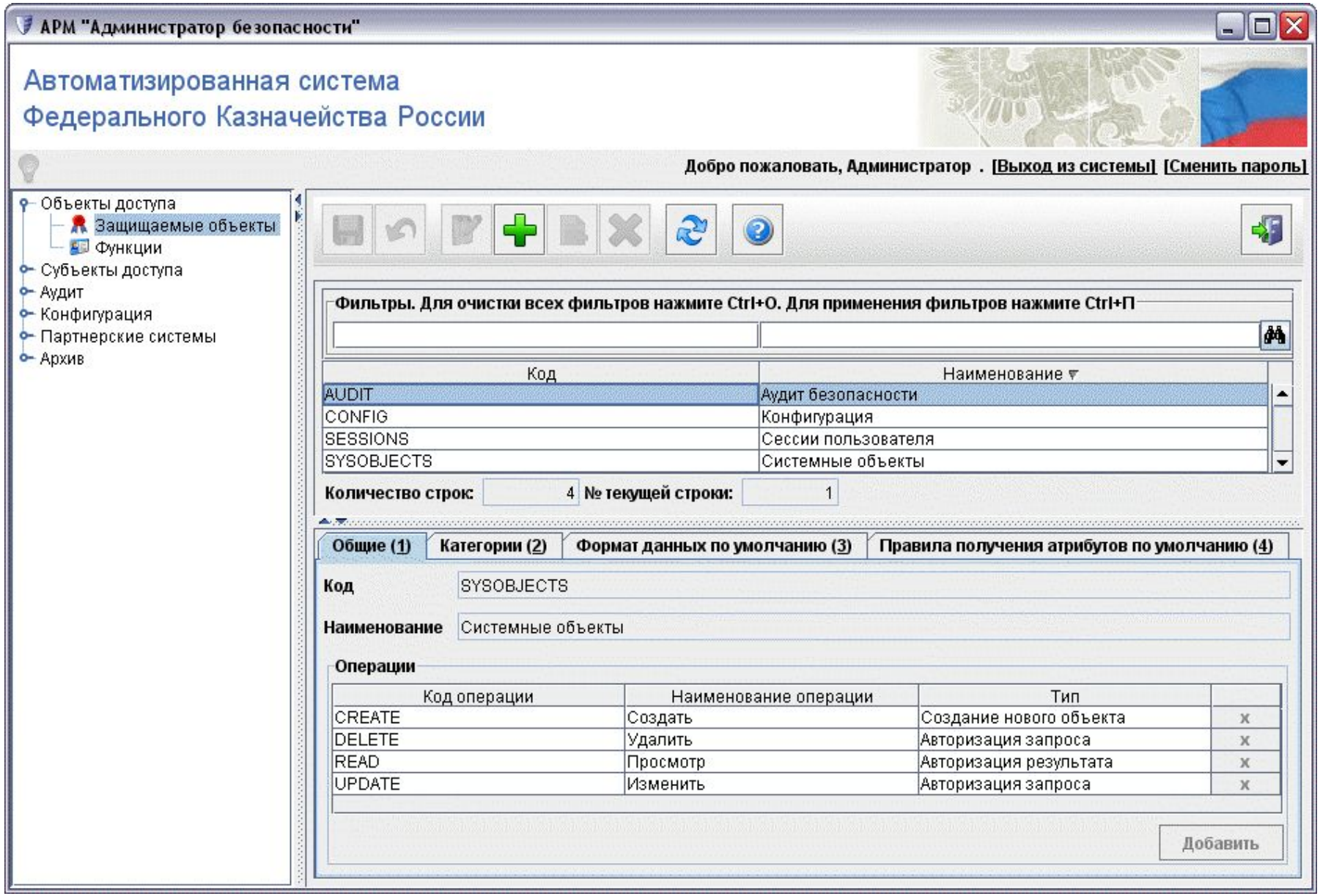
Установка и настройка АРМ контроля передаваемой информации

. Настройка СБ
. Указание каталогов для входящих/проверенных/заблокированных пакетов
. Дополнительная настройка АРМ КПИ
. Работа с АРМ КПИ

Настройка дополнительных средств защиты АСФК.

. Настройка Internet Explorer в открытом и защищенном контуре.
. Настройка корректного отображения объектных идентификаторов в сертификатах
. Настройка SecretNet 5.0C для открытого контура
. Настройка SecretNet 5.0C для защищенного контура
. Настройка ЭЗ «Соболь» для открытого контура
. Настройка ЭЗ «Соболь» в защищенном контуре
. Настройки СЗИ «ФИКС-UNIX 1.0»

Администрирование объектов доступа
Защищаемые объекты



Администрирование объектов доступа

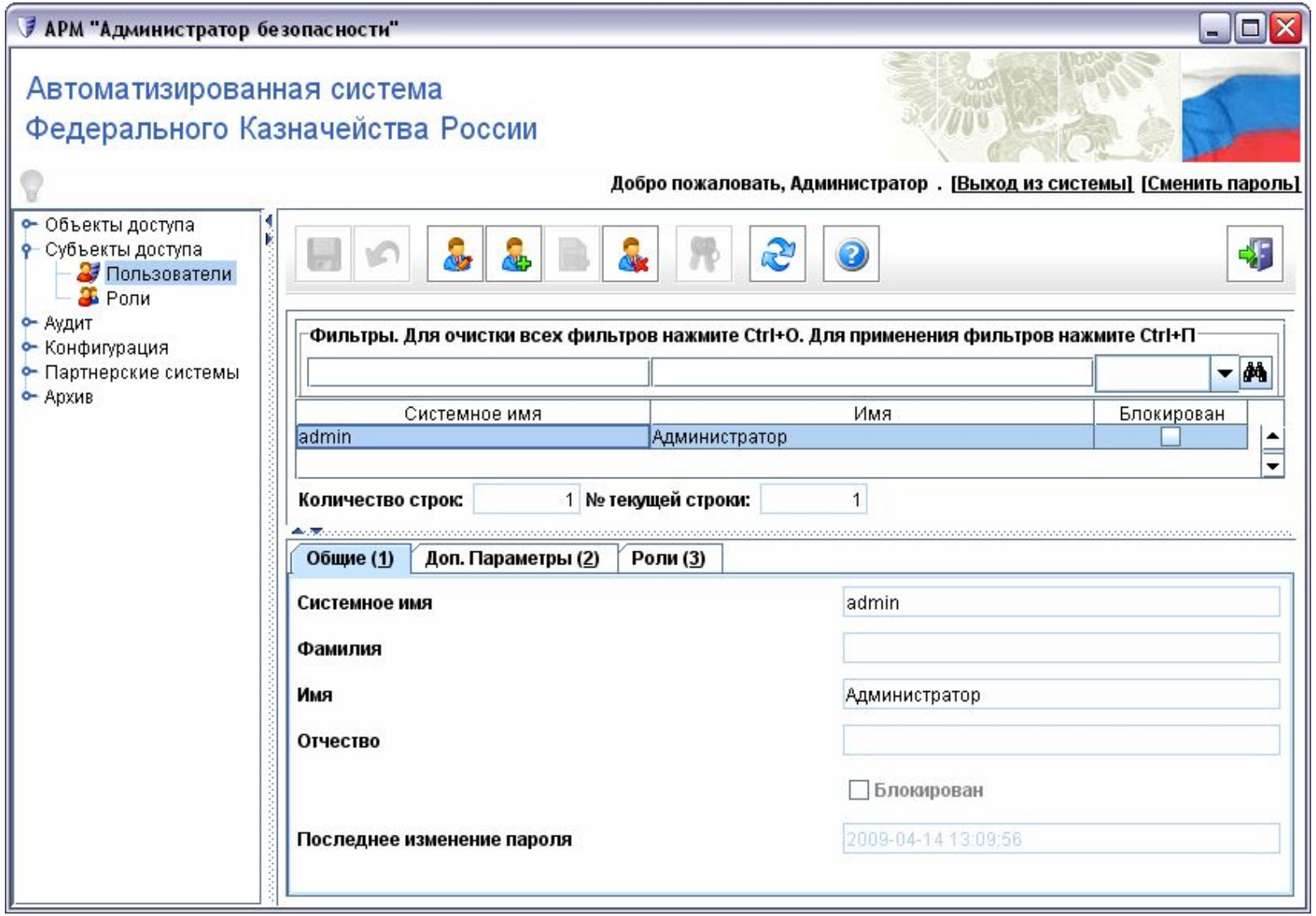
Для проверки доступа к объекту данных должны быть заданы шесть параметров (кроме логина):

- Тип объекта – строковый код, например ‘DOC’ или ‘PATH’.
- Категория объекта – строковый код, например ‘RUR_BO’.
- Код операции – строковый код, например ‘CREATE’, ‘UPDATE’, ‘PRINT’.
- Код формата данных (может быть пустым) – строковый код, ссылающийся на XSLT преобразование, трансформирующее исходные параметры в формат, обрабатываемый СБ
- Данные объекта – XML, форматирование которого через XSLT код, заданный выше, приводится к XML, формат которого описан в Приложении 2 (аналог значений параметров для функции).

К защищаемым объектам применимы следующие операции:

- добавление нового объекта;
- редактирование свойств и параметров существующего объекта;
- удаление объекта.

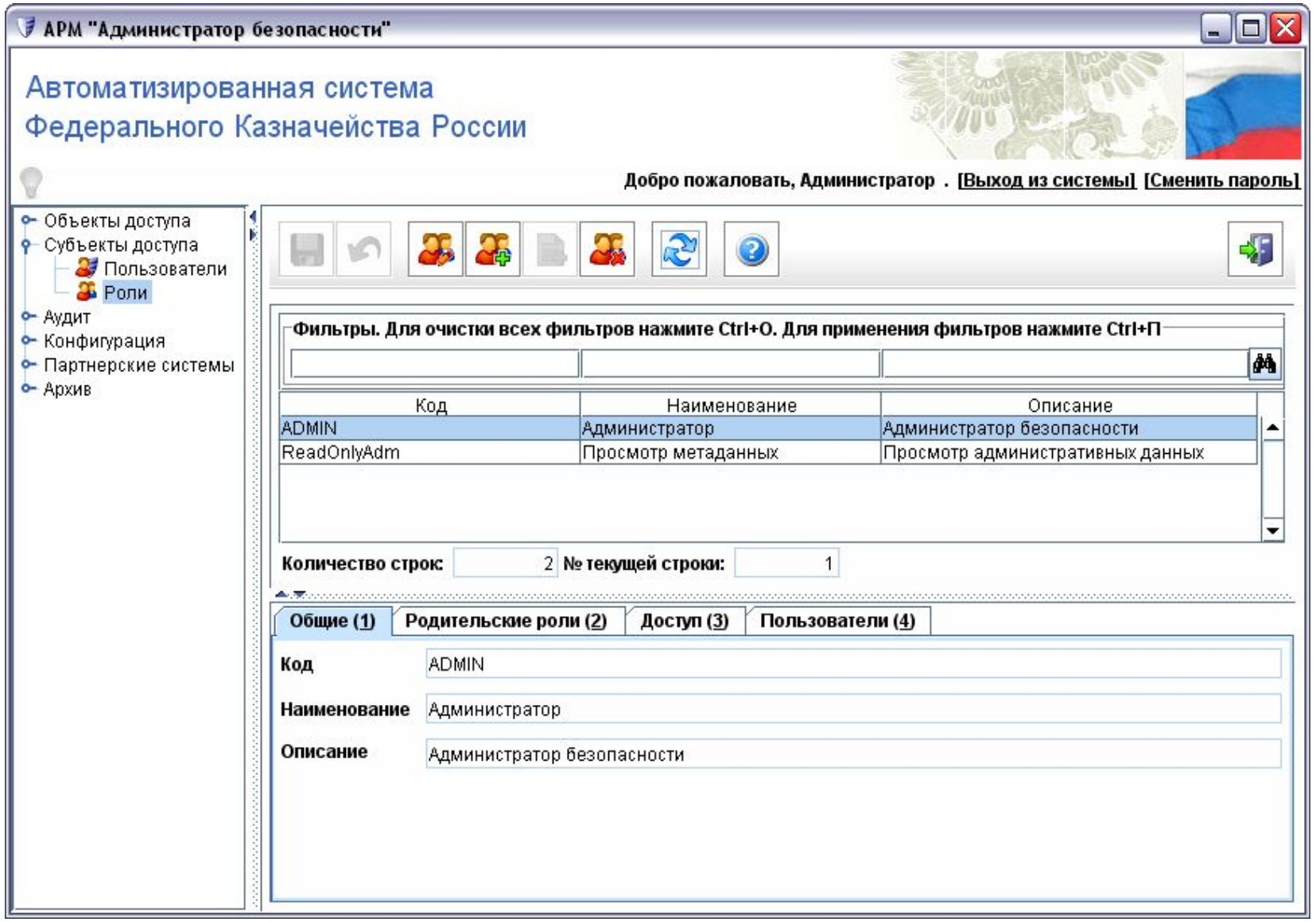
. Настройка параметров идентификации и аутентификации пользователей



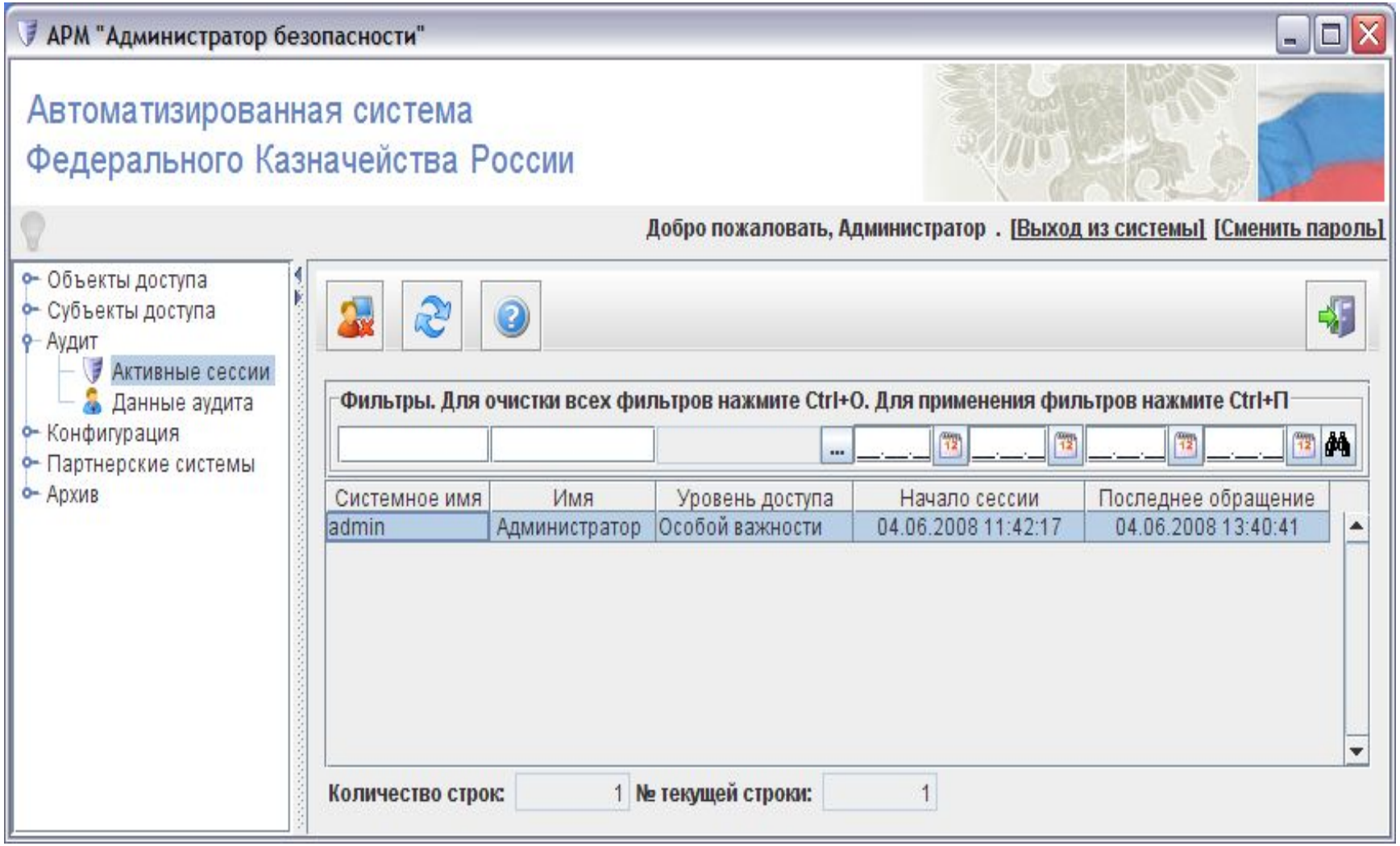
- **Действия по идентификации и аутентификации пользователей**

Добавление учетной записи.
Блокирование/разблокирование пользователя
Назначение пользователю пароля.
Редактирование параметров пользователя.
Удаление пользователя.
Определение ролей и назначение ролей пользователям
Добавление новой роли
Разграничение прав доступа в зависимости от значений параметров

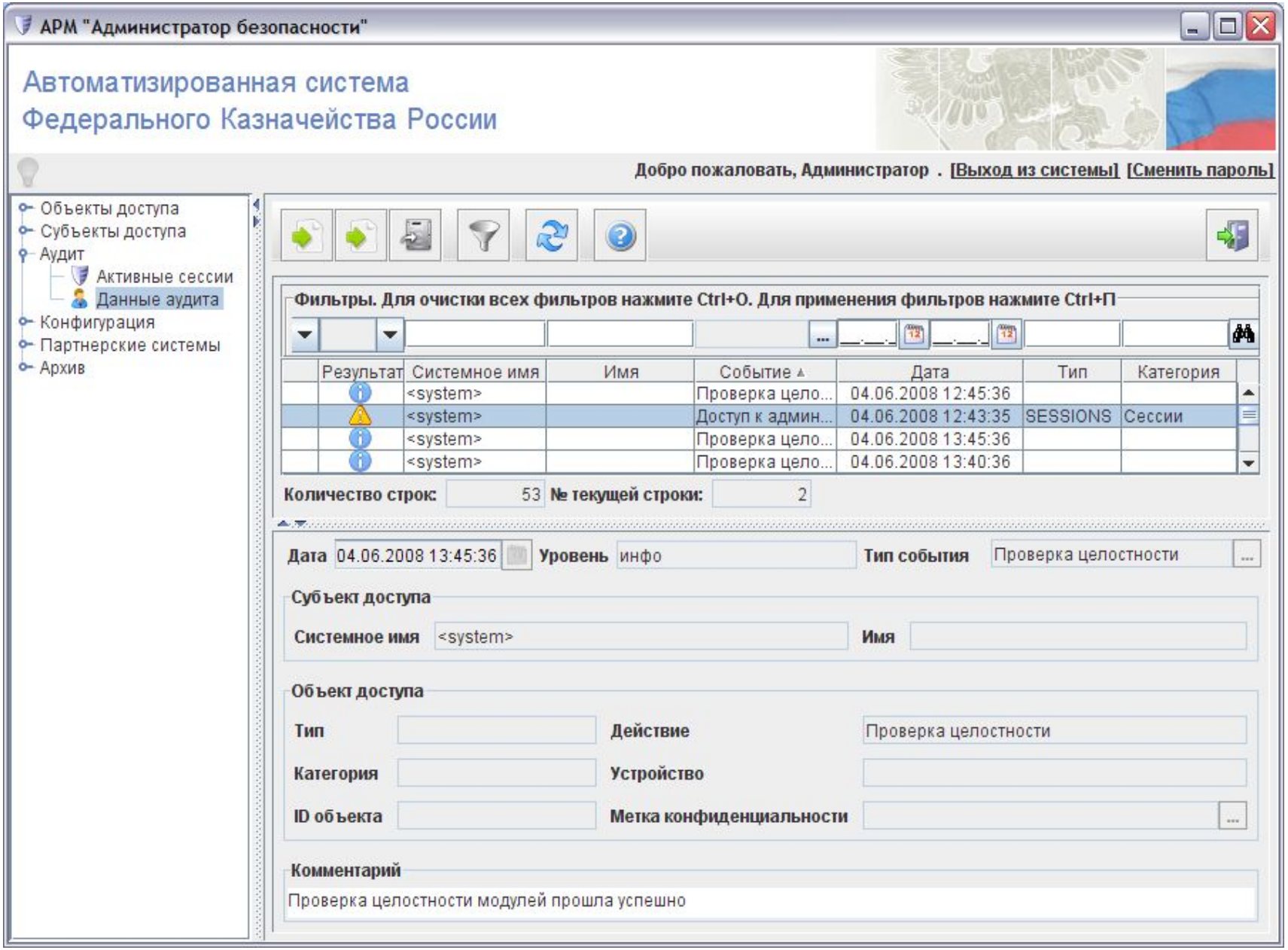
Раздел «Роли» АРМ СБ



. Администрирование подсистемы аудита



Журнал данных аудита



Действия с данными аудита

Для каждой активной сессии в журнале отображается следующая информация:

Системное имя пользователя.

Имя пользователя.

Уровень доступа.

Начало сессии.

Время последнего обращения

Доступные операции

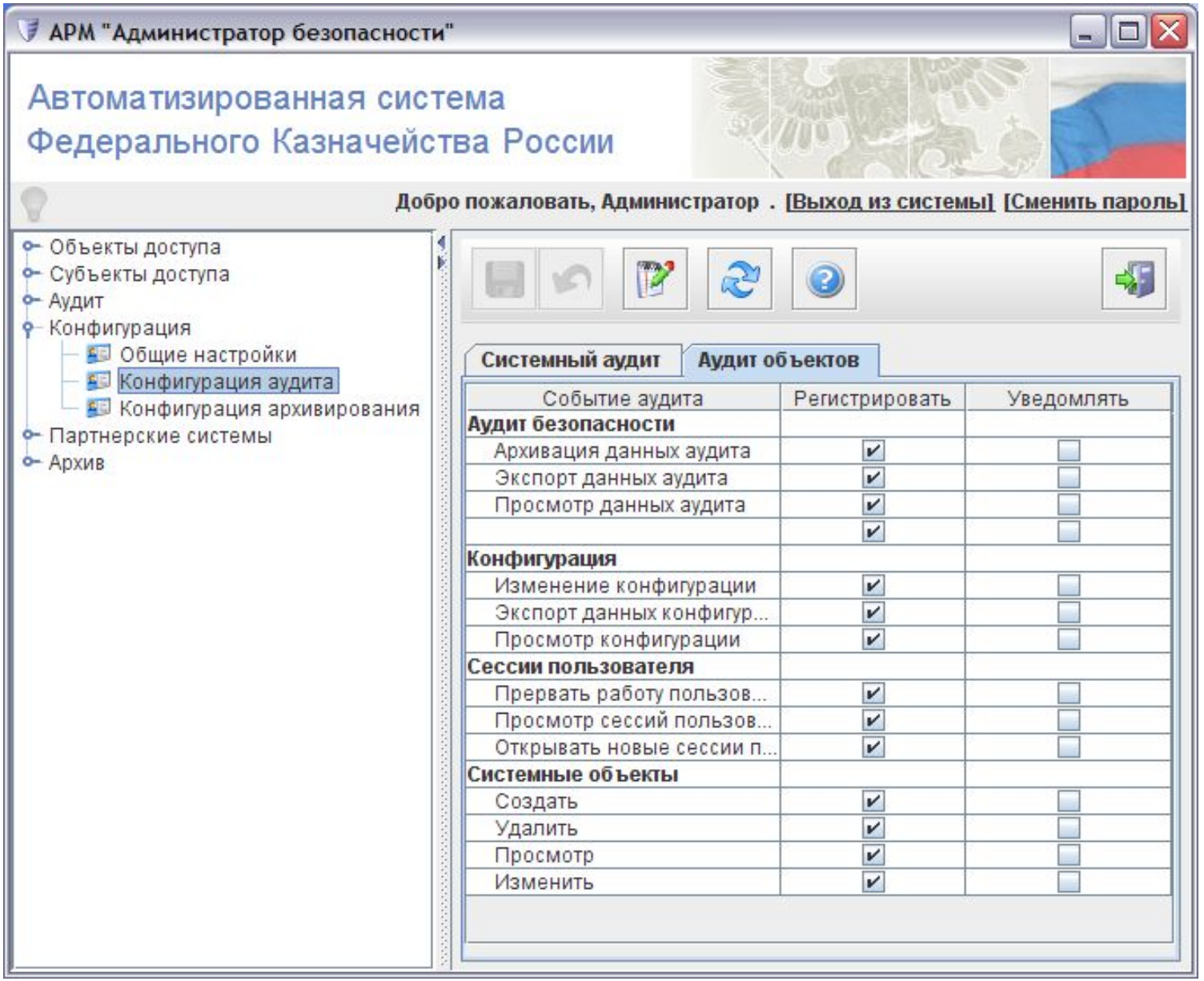
Удаление сессии

Экспорт данных аудита.

Архивирование данных аудита

Конфигурирование аудита

Конфигурация аудита. Аудит объектов.



Конфигурация архивирования. «Аудит объектов»