

# 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 ТСР, доступный ресурс – сервер СУФД, шлюза MAIL –

# **Структура СЗИ НСД АСФК:**

**Сервер безопасности (СБ);**

**Агент Сервера безопасности;**

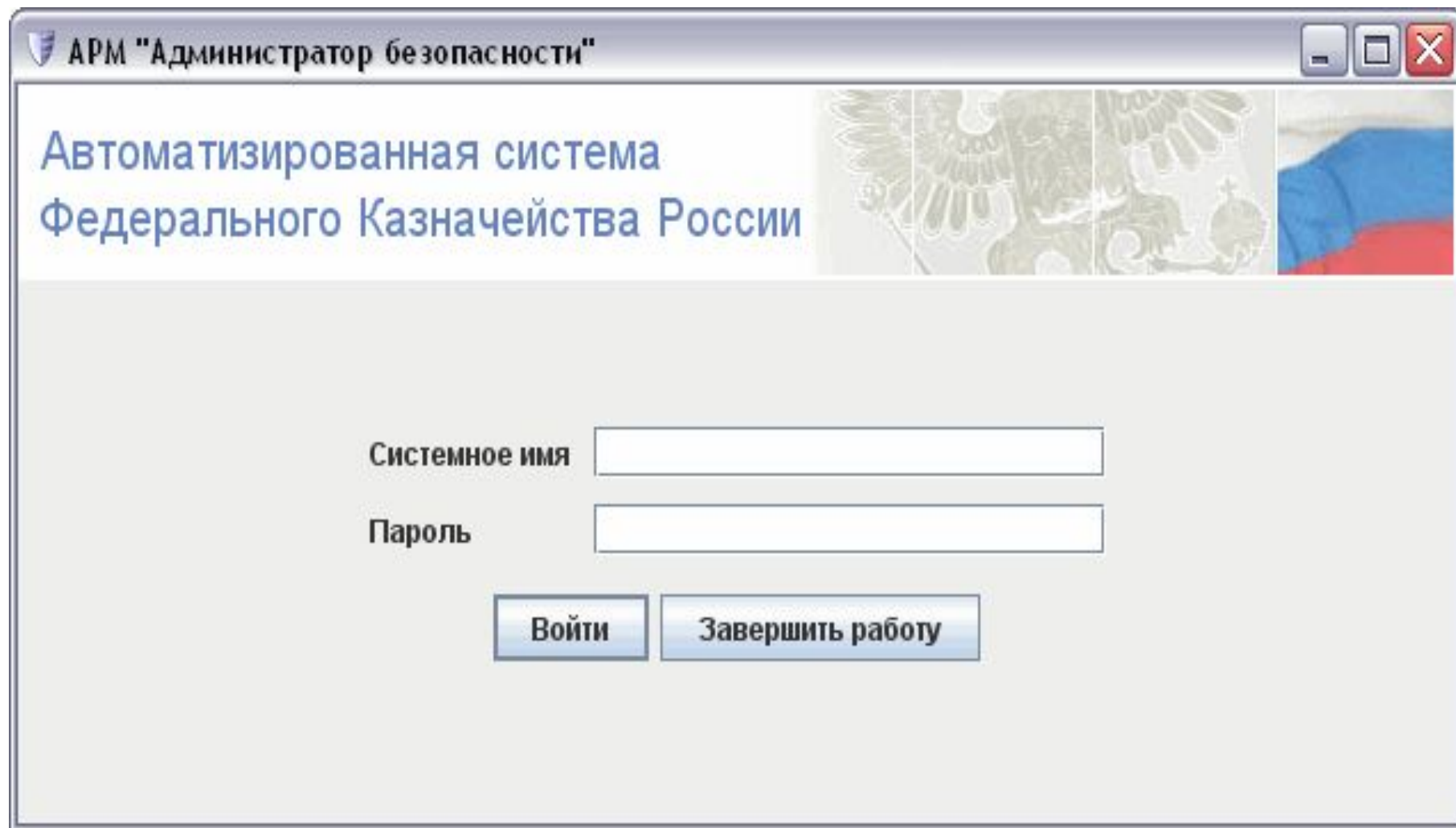
**АРМ Администратора безопасности**

# Логическая схема взаимодействия клиентского и серверного ППО с сервером безопасности

# Архитектура СБ



# Окно авторизации



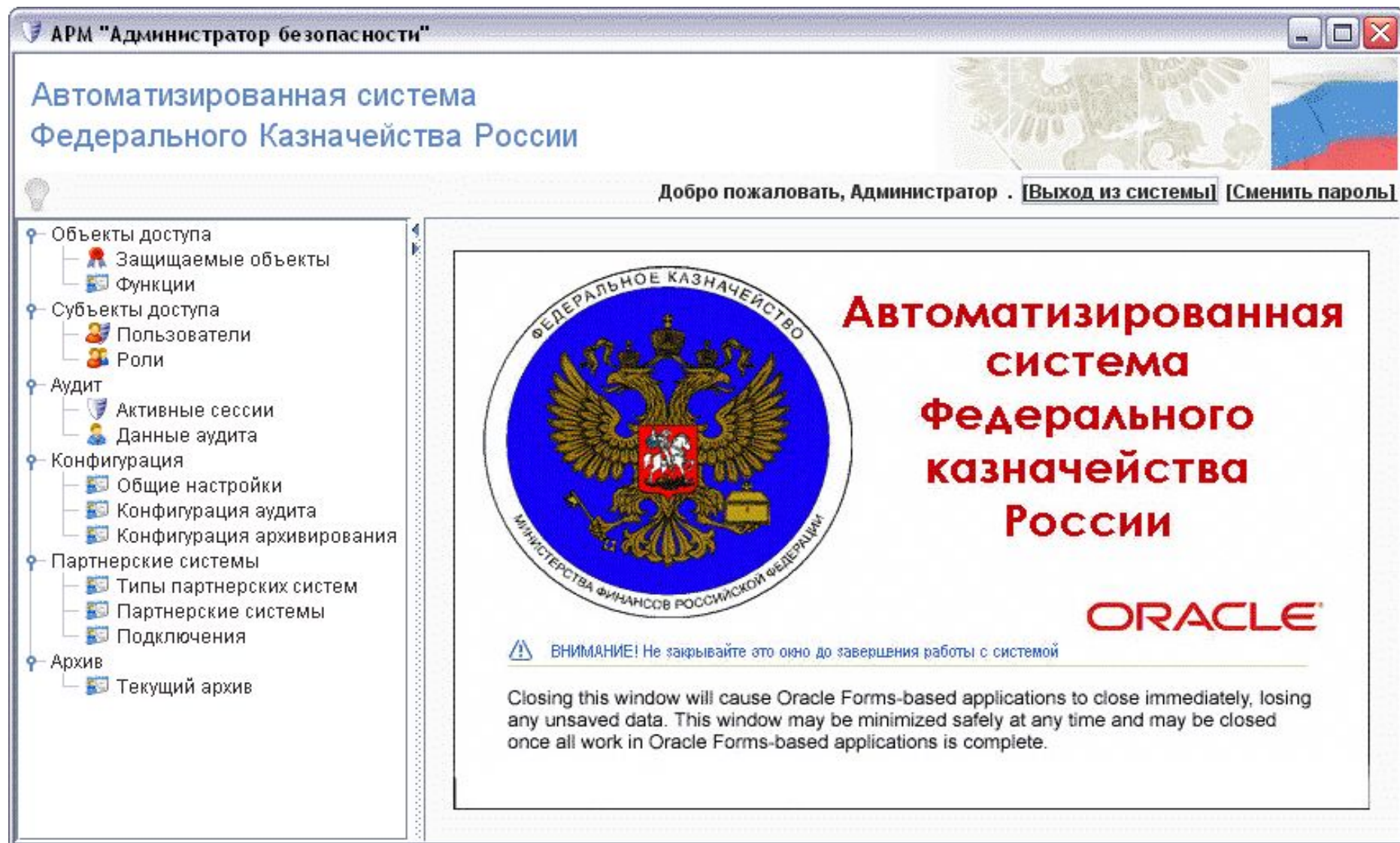
АРМ "Администратор безопасности"

Автоматизированная система  
Федерального Казначейства России

Системное имя

Пароль

# Главное окно АРМ «Администратор безопасности»



АРМ "Администратор безопасности"

Автоматизированная система  
Федерального Казначейства России

Добро пожаловать, Администратор . [\[Выход из системы\]](#) [\[Сменить пароль\]](#)

- Объекты доступа
  - Защищаемые объекты
  - Функции
- Субъекты доступа
  - Пользователи
  - Роли
- Аудит
  - Активные сессии
  - Данные аудита
- Конфигурация
  - Общие настройки
  - Конфигурация аудита
  - Конфигурация архивирования
- Партнерские системы
  - Типы партнерских систем
  - Партнерские системы
  - Подключения
- Архив
  - Текущий архив

**Автоматизированная система  
Федерального  
казначейства  
России**

**ORACLE**

**ВНИМАНИЕ!** Не закрывайте это окно до завершения работы с системой

Closing this window will cause Oracle Forms-based applications to close immediately, losing any unsaved data. This window may be minimized safely at any time and may be closed once all work in Oracle Forms-based applications is complete.

# 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»

АРМ "Администратор безопасности"

Автоматизированная система  
Федерального Казначейства России

Добро пожаловать, Администратор . [Выход из системы] [Сменить пароль]

1

2

3

Код	Наименование
AUDIT	Аудит безопасности
CONFIG	Конфигурация
SESSIONS	Сессии пользователя
SYSOBJECTS	Системные объекты

Количество строк: 4 № текущей строки: 1

4

Правила получения атрибутов по умолчанию (4)

Общие (1) Категории (2) Формат данных по умолчанию (3)

Код: AUDIT

Наименование: Аудит безопасности

5

Операции

Код операции	Наименование операции	Тип	
ARCHIVING	Архивация данных аудита	Авторизация результата	x
EXPORT	Экспорт данных аудита	Авторизация результата	x
READ	Просмотр данных аудита	Авторизация результата	x
READADMIN		Авторизация результата	x

Добавить

# 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 5.0С для открытого контура
- . Настройка SecretNet 5.0С 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

АРМ "Администратор безопасности"

Автоматизированная система  
Федерального Казначейства России

Добро пожаловать, Администратор . [\[Выход из системы\]](#) [\[Сменить пароль\]](#)

- Объекты доступа
  - Защищаемые объекты
  - Функции
- Субъекты доступа
- Аудит
- Конфигурация
- Партнерские системы
- Архив

Фильтры. Для очистки всех фильтров нажмите Ctrl+O. Для применения фильтров нажмите Ctrl+P

Код	Наименование
AUDIT	Аудит безопасности
CONFIG	Конфигурация
SESSIONS	Сессии пользователя
SYSOBJECTS	Системные объекты

Количество строк: 4 № текущей строки: 1

Общие (1) Категории (2) Формат данных по умолчанию (3) Правила получения атрибутов по умолчанию (4)

Код: SYSOBJECTS

Наименование: Системные объекты

Операции

Код операции	Наименование операции	Тип	
CREATE	Создать	Создание нового объекта	x
DELETE	Удалить	Авторизация запроса	x
READ	Просмотр	Авторизация результата	x
UPDATE	Изменить	Авторизация запроса	x

Добавить

# 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

The screenshot shows the ARМ 'Администратор безопасности' (Security Administrator) interface. The window title is 'АРМ "Администратор безопасности"'. The main header displays 'Автоматизированная система Федерального Казначейства России' (Automated system of the Federal Treasury of Russia) along with the Russian coat of arms and flag. A navigation pane on the left lists: 'Объекты доступа', 'Субъекты доступа' (with sub-items 'Пользователи' and 'Роли'), 'Аудит', 'Конфигурация', 'Партнерские системы', and 'Архив'. The main content area shows a toolbar with icons for file operations and user management. Below the toolbar, a filter section contains the text: 'Фильтры. Для очистки всех фильтров нажмите Ctrl+O. Для применения фильтров нажмите Ctrl+П'. A table lists user entries:

Системное имя	Имя	Блокирован
admin	Администратор	<input type="checkbox"/>

Below the table, it indicates 'Количество строк: 1' and '№ текущей строки: 1'. The 'Общие (1)' tab is active, showing the following fields for the selected user:

- Системное имя: admin
- Фамилия: [empty field]
- Имя: Администратор
- Отчество: [empty field]
- Блокирован
- Последнее изменение пароля: 2009-04-14 13:09:56



- **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

АРМ "Администратор безопасности"

Автоматизированная система  
Федерального Казначейства России

Добро пожаловать, Администратор . [\[Выход из системы\]](#) [\[Сменить пароль\]](#)

- Объекты доступа
- Субъекты доступа
  - Пользователи
  - Роли**
- Аудит
- Конфигурация
- Партнерские системы
- Архив

Фильтры. Для очистки всех фильтров нажмите Ctrl+O. Для применения фильтров нажмите Ctrl+P

Код	Наименование	Описание
ADMIN	Администратор	Администратор безопасности
ReadOnlyAdm	Просмотр метаданных	Просмотр административных данных

Количество строк:  Не текущей строки:

**Общие (1)** Родительские роли (2) Доступ (3) Пользователи (4)

Код: ADMIN

Наименование: Администратор

Описание: Администратор безопасности

# • Администрирование подсистемы аудита

АРМ "Администратор безопасности"

Автоматизированная система  
Федерального Казначейства России

Добро пожаловать, Администратор . [\[Выход из системы\]](#) [\[Сменить пароль\]](#)

- Объекты доступа
- Субъекты доступа
- Аудит
  - Активные сессии
  - Данные аудита
- Конфигурация
- Партнерские системы
- Архив

Фильтры. Для очистки всех фильтров нажмите Ctrl+O. Для применения фильтров нажмите Ctrl+P

Системное имя	Имя	Уровень доступа	Начало сессии	Последнее обращение
admin	Администратор	Особой важности	04.06.2008 11:42:17	04.06.2008 13:40:41

Количество строк:  № текущей строки:

# Журнал данных аудита

АРМ "Администратор безопасности"

Автоматизированная система  
Федерального Казначейства России

Добро пожаловать, Администратор . [\[Выход из системы\]](#) [\[Сменить пароль\]](#)

- Объекты доступа
- Субъекты доступа
- Аудит
  - Активные сессии
  - Данные аудита**
- Конфигурация
- Партнерские системы
- Архив

Фильтры. Для очистки всех фильтров нажмите Ctrl+O. Для применения фильтров нажмите Ctrl+P

Результат	Системное имя	Имя	Событие	Дата	Тип	Категория
	<system>		Проверка цело...	04.06.2008 12:45:36		
	<system>		Доступ к админ...	04.06.2008 12:43:35	SESSIONS	Сессии
	<system>		Проверка цело...	04.06.2008 13:45:36		
	<system>		Проверка цело...	04.06.2008 13:40:36		

Количество строк: 53 № текущей строки: 2

Дата: 04.06.2008 13:45:36 | Уровень: инфо | Тип события: Проверка целостности

Субъект доступа

Системное имя: <system> | Имя:

Объект доступа

Тип: | Действие: Проверка целостности

Категория: | Устройство:

ID объекта: | Метка конфиденциальности:

Комментарий

Проверка целостности модулей прошла успешно

# 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.

АРМ "Администратор безопасности"

Автоматизированная система  
Федерального Казначейства России

Добро пожаловать, Администратор . [Выход из системы] [Сменить пароль]

- Объекты доступа
- Субъекты доступа
- Аудит
- Конфигурация
  - Общие настройки
  - Конфигурация аудита
  - Конфигурация архивирования
- Партнерские системы
- Архив

Системный аудит    Аудит объектов

Событие аудита	Регистрировать	Уведомлять
<b>Аудит безопасности</b>		
Архивация данных аудита	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Экспорт данных аудита	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Просмотр данных аудита	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>Конфигурация</b>		
Изменение конфигурации	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Экспорт данных конфигур...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Просмотр конфигурации	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>Сессии пользователя</b>		
Прервать работу пользов...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Просмотр сессий пользов...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Открывать новые сессии п...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>Системные объекты</b>		
Создать	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Удалить	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Просмотр	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Изменить	<input checked="" type="checkbox"/>	<input type="checkbox"/>

# Конфигурация архивирования. «Аудит объектов»

The screenshot shows the ARM 'Administrator of Security' interface. The window title is 'АРМ "Администратор безопасности"'. The main header displays 'Автоматизированная система Федерального Казначейства России' with a logo and the Russian flag. Below the header, a navigation pane on the left lists: 'Объекты доступа', 'Субъекты доступа', 'Аудит', 'Конфигурация' (with sub-items: 'Общие настройки', 'Конфигурация аудита', 'Конфигурация архивирования'), 'Партнерские системы', and 'Архив'. The 'Конфигурация архивирования' item is selected. The main content area has tabs for 'Фильтры' and 'Автоматическое архивирование'. Under 'Автоматическое архивирование', there are sub-tabs for 'Системный аудит' and 'Аудит объектов'. The 'Аудит объектов' sub-tab is active, displaying a table with two columns: 'Событие аудита' and 'Архивировать'. The table lists various audit events with checkboxes in the 'Архивировать' column, all of which are checked.

АРМ "Администратор безопасности"

Автоматизированная система  
Федерального  
Казначейства России

Добро пожаловать, Администратор . [Выход из системы] [Сменить пароль]

- Объекты доступа
- Субъекты доступа
- Аудит
- Конфигурация
  - Общие настройки
  - Конфигурация аудита
  - Конфигурация архивирования
- Партнерские системы
- Архив

Фильтры    Автоматическое архивирование

Системный аудит    Аудит объектов

Событие аудита	Архивировать
<b>Аудит безопасности</b>	
Архивация данных аудита	<input checked="" type="checkbox"/>
Экспорт данных аудита	<input checked="" type="checkbox"/>
Просмотр данных аудита	<input checked="" type="checkbox"/>
	<input checked="" type="checkbox"/>
<b>Конфигурация</b>	
Изменение конфигурации	<input checked="" type="checkbox"/>
Экспорт данных конфигу...	<input checked="" type="checkbox"/>
Просмотр конфигурации	<input checked="" type="checkbox"/>
<b>Сессии пользователя</b>	
Прервать работу пользо...	<input checked="" type="checkbox"/>
Просмотр сессий пользо...	<input checked="" type="checkbox"/>
Открывать новые сессии ...	<input checked="" type="checkbox"/>
<b>Системные объекты</b>	
Создать	<input checked="" type="checkbox"/>
Удалить	<input checked="" type="checkbox"/>
Просмотр	<input checked="" type="checkbox"/>
Изменить	<input checked="" type="checkbox"/>