УТВЕРЖДЕН
11443195.4012-053 93 2012 ЛУ

СИСТЕМА УДАЛЕННОГО ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ СЗИ ОТ НСД АККОРД

Руководство Администратора нештатного режима функционирования

Листов 13

Москва
2014

Формат А4

АННОТАЦИЯ

Специализированная система удаленного централизованного управления средствами защиты информации от несанкционированного доступа Аккорд (в дальнейшем также СУЦУ, Система) предназначена для реализации требований нормативных документов Банка России по ИБ, централизованного мониторинга событий ИБ и управления средствами защиты информации от несанкционированного доступа, функционирующими в АС Банка России.

Данный документ описывает действия Администратора нештатного режима СУЦУ (Администратор НШР СЗИ от НСД), связанные с непосредственной работой подсистемы в штатном режиме функционирования.

СОДЕРЖАНИЕ

1 Введение

1.1 Область применения

Деятельность Администратора нештатного режима функционирования СУЦУ.

1.2 Функции Администратора нештатного режима функционирования СУЦУ

Администратор нештатного режима функционирования СУЦУ:

- создает учетные записи управляющего персонала СУЦУ: Администратора информационной безопасности СУЦУ и Администратора СУЦУ;
- осуществляет мероприятия по восстановлению работоспособности СУЦУ в случаях сбоев и аварийных ситуаций;
- осуществляет функции только в нештатном режиме СУЦУ;
- в случае необходимости может выполнять любые функции ASM.

1.3 Комплект поставки

СУЦУ является подсистемой, внедряемой путем поставки, установки и настройки следующих компонентов:

- сервер централизованного управления.
- клиент централизованного управления (на каждый АРМ, являющийся подконтрольным объектом).
- серверные и клиентские компоненты, реализующие транспортные функции (подсистема распределенного аудита и управления), серверные компоненты, реализующие функции управления (подсистема Accord Security Management Special Edition (ASM SE)) СЗИ от НСД подконтрольных объектов (далее по тексту ПКО) – на CD;
- лицензии на подключения управляемых объектов к СУЦУ на DS 1996;
- комплект рабочей документации на CD.

1.4 Регламент и режимы работы оборудования

СУЦУ может функционировать в следующих режимах:

- штатный режим функционирования;
- нештатный режим функционирования:
  - сервисный режим;
  - аварийный режим.

Изменение режима эксплуатации СУЦУ не влияет на работоспособность ПКО.

Нарушение функционирования СУЦУ не приводит к нарушению функционирования других подсистем и объектов защиты.

2 Порядок работы

2.1 Сервисный режим

Сервисный режим функционирования задействуется при проведении регламентных работ с техническими средствами СУЦУ, включающих обслуживание и переконфигурирование компонентов СУЦУ.

Эксплуатация СУЦУ в сервисном режиме должна осуществляться только в рамках плановых мероприятий и регламентов обслуживания, согласованных в установленном порядке.

2.2 Действия Администратора нештатного режима функционирования в сервисном режиме

В сервисном режиме Администратор нештатного режима функционирования обеспечивает доступность всех событий ИБ, зарегистрированных СУЦУ для анализа и контроля персонала СУЦУ после завершения технического обслуживания;

Открыв вкладку «Журналы», Администратор нештатного режима средств защиты информации от НСД может работать с тремя типами журналов.

Первый тип – Журналы «Аккорд», в которых содержатся сведения о работе пользователей на рабочих местах (рисунок 1). (Журналы «Аккорд» хранятся в каталоге ASM/ACCONNET/Client.Log/XXX/YYY/, где XXX – имя каталога, соответствующего имени ПКО, YYY – имя каталога, соответствующего дате в формате дата – месяц- год.

Например: C:/Asm/ACCONNET/Client.Log/Demo_PC/18_01_2013/20131005172617.LOW). Маска файла журнала следующая: «*******.LOW», где знак «*******» обозначает дату с точностью до секунды).

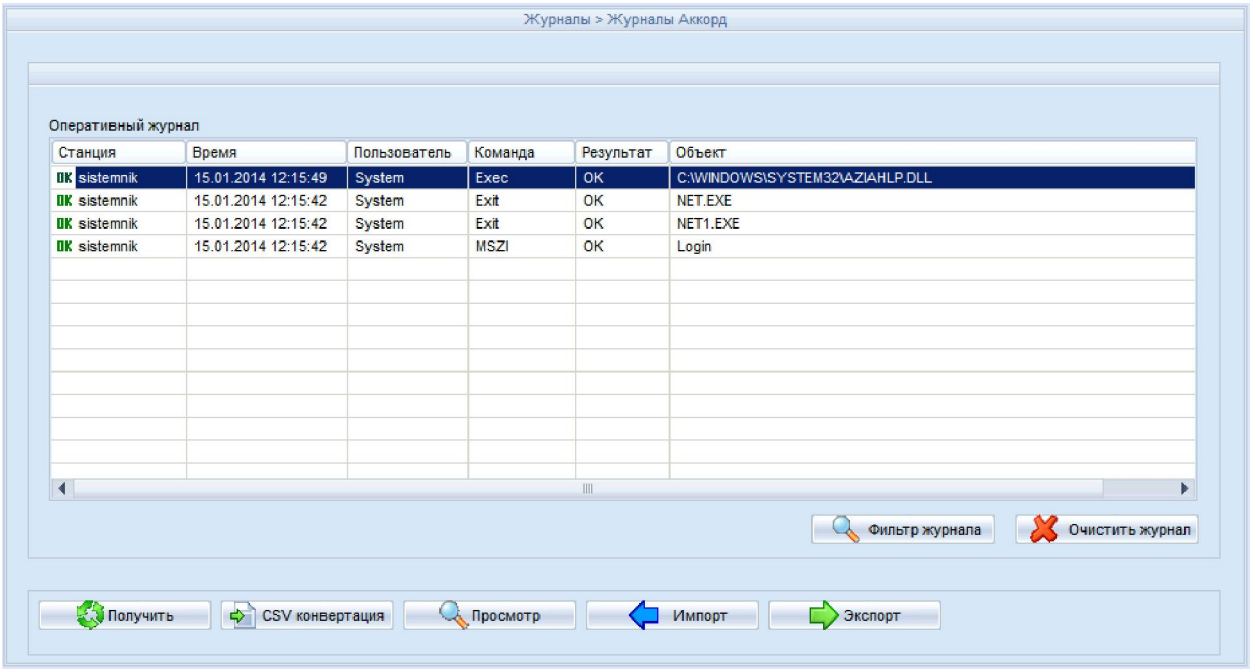

Рисунок 1 - Журналы «Аккорд»

Сведения, хранящиеся в журнале, обновляются в режиме реального времени.

Получить журналы с ПКО (по централизованной схеме) можно по нажатии кнопки <Получить>. По нажатии кнопки на экране появляется окно, в котором следует выбрать ПКО, с которых планируется получить журналы (рисунок 2).

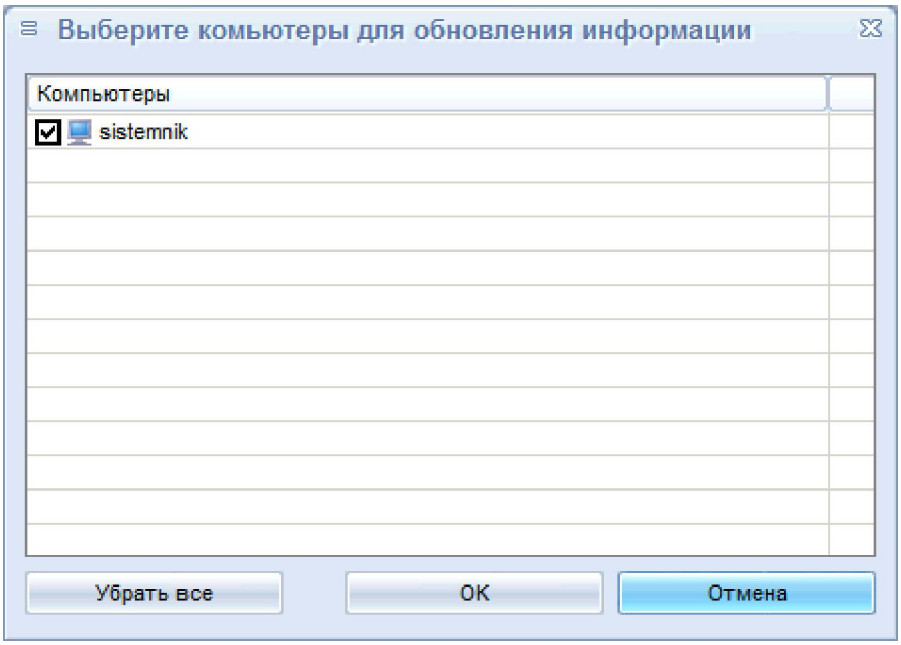

Рисунок 2 – Выбор ПКО, с которых планируется получить журналы[1)]

Для просмотра журнала необходимо нажать кнопку <Просмотр>. После этого на экране появляется окно выбора каталога, в котором нужно выбрать необходимый файл.

Конвертировать журнал в общепринятые форматы можно, нажав кнопку <CSV конвертация> (или <XML конвертация>, если в настройках фильтров экспорта журналов выбрать пункт «XML файл для конвертации журналов»[2)]) в окне, показанном на рисунке 1.. В результате этой операции в каталоге, указанном в поле «CSV файл для конвертации журналов:» (или в каталоге, указанном в поле «XML файл для конвертации журналов» (в зависимости от выбранных настроек), появляется файл в формате csv (или в формате xml в зависимости от выбранных настроек), предназначенный для работы с фильтрами экспорта журналов.

ВНИМАНИЕ! Файл *.csv по умолчанию имеет разделители в виде символа «=». Чтобы изменить указанный символ на другой, следует в файле asm.ini указать параметр «Separator».

Журнал «Аккорд» можно экспортировать (например, для дальнейшего анализа в системах мониторинга), для этого необходимо нажать кнопку <Экспорт>. Далее на экране появляется окно выбора каталога, в котором необходимо выбрать каталог и нажать кнопку <Применить>.

Кнопка <Импорт> необходима для получения журналов с ПКО по децентрализованной схеме.

[1)] В случае эксплуатации ПП СУЦУ СЗИ от НСД версии 1.0.8.52 и выше сбор журналов происходит в автоматическом режиме.

[2)] Настройку фильтров экспорта журналов выполняет Администратор ИБ СУЦУ в соответствии с подразделом 4.3.3 документа «Руководство Администратора ИБ СУЦУ» 11443195.4012-053 91.

По нажатии кнопки <Фильтр журнала> на экране появляется окно смены фильтров оперативного журнала (рисунок 3).

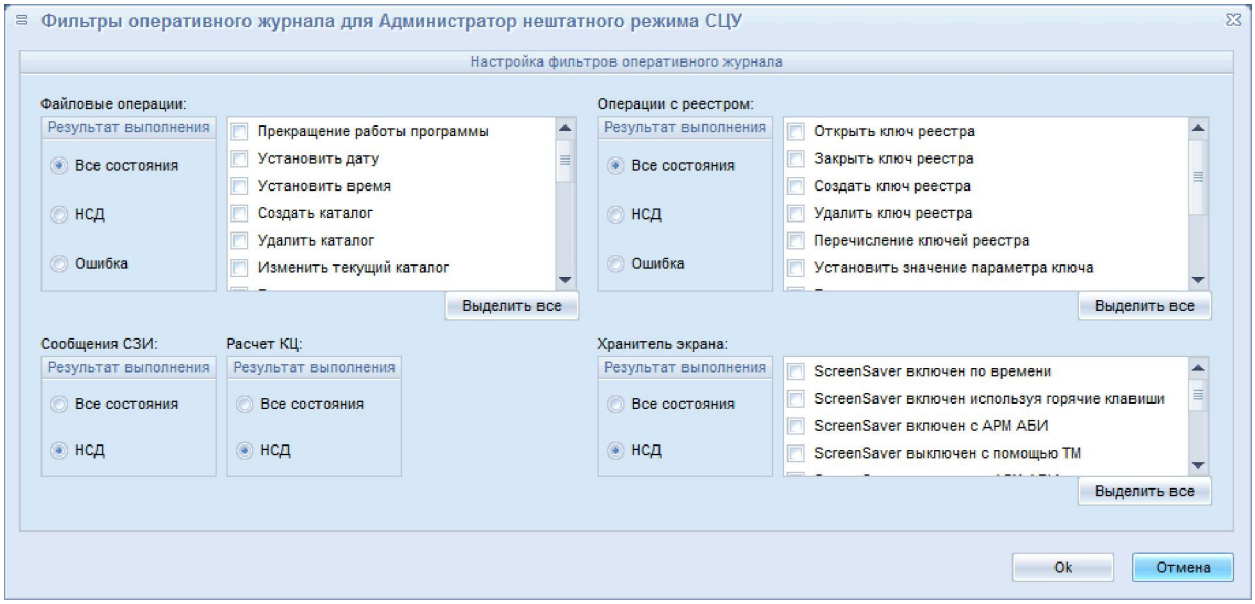

Рисунок 3 – Фильтры оперативного журнала для текущей учетной записи

В нем можно выбрать типы событий, информация о которых передается в оперативный журнал, для текущей учетной записи (см. рисунок 3). События хранятся в каталоге ASM\AccountName_FilterParam.ini, где параметр «AccountName» – это имя учетной записи.

Второй тип – журналы ASM, касающиеся работы утилиты ASM (рисунок 4). В них записываются дата и время выполнения операций в ASM, сами эти операции, информация о попытках несанкционированного доступа, информация об изменении параметров ASM (сообщения об изменении параметров имеют префикс CFG). (Журналы ASM хранятся в каталоге ASM/ACCONNET/Client.Log в следующей форме: «asm*****.LOW», где знак «*****» обозначает дату с точностью до секунды).

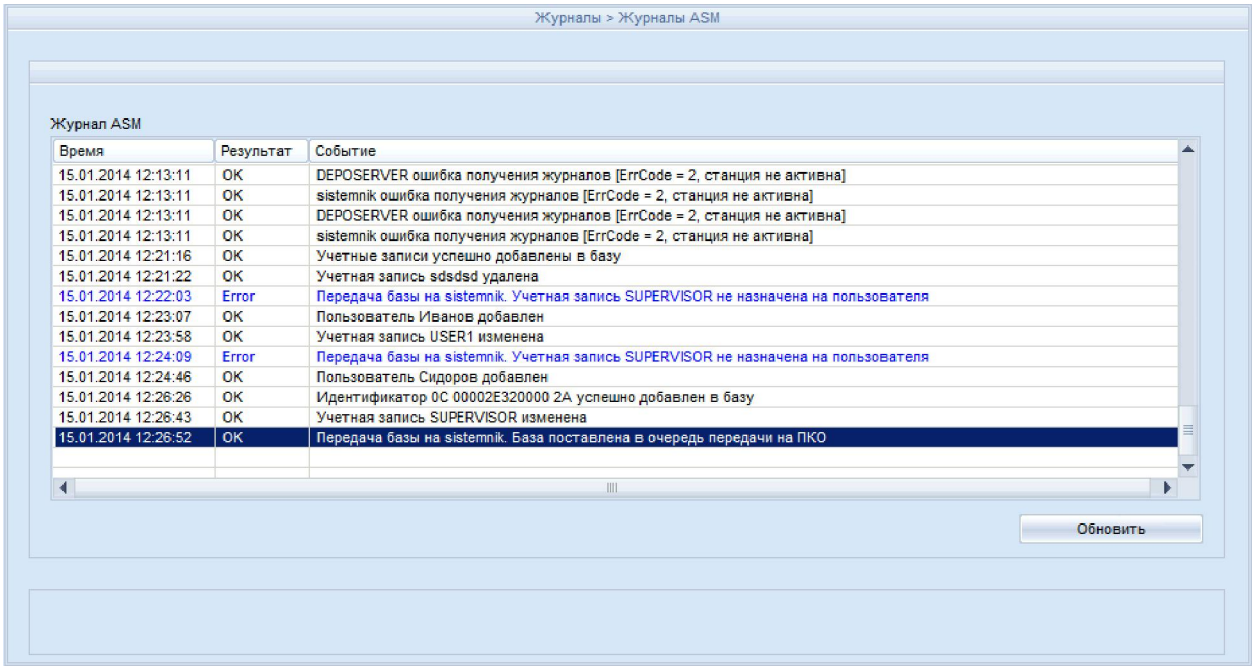

Рисунок 4 - Журнал ASM

Третий тип журналов - журнал АРМ АБИ, касающийся работы утилиты AcConnet (рисунок 5). Он необходим для просмотра сетевых сообщений.

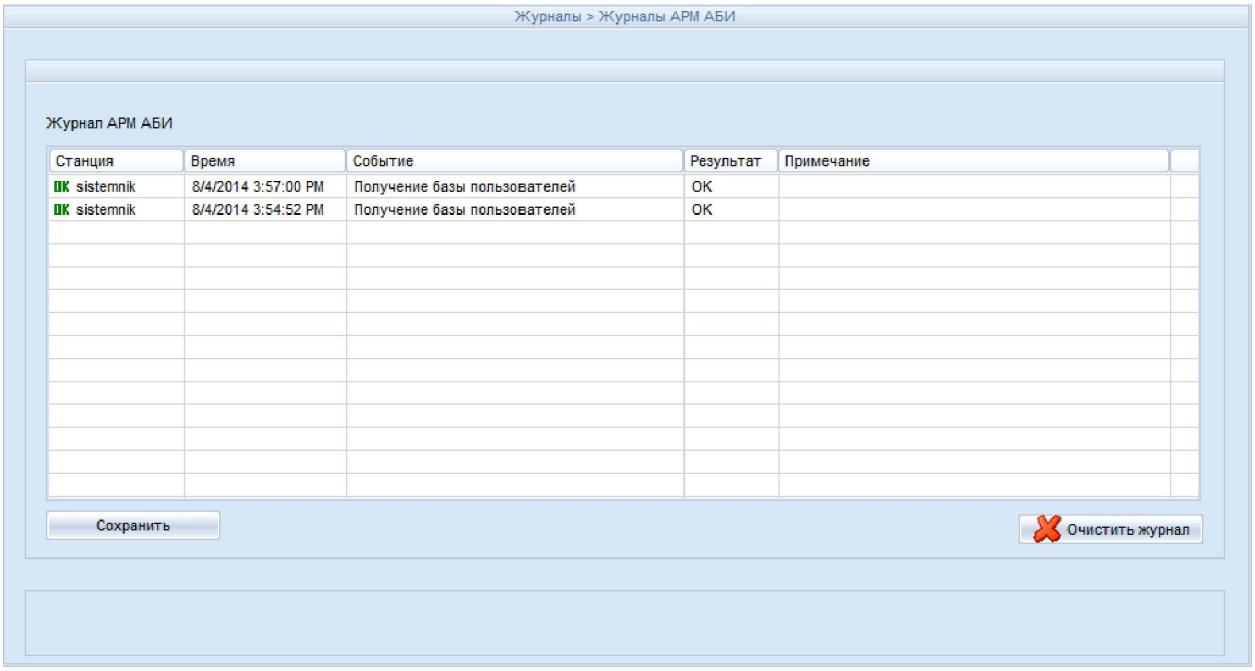

Рисунок 5 – Журнал АРМ АБИ

Журнал АРМ АБИ можно сохранить в текстовый файл с разделителем «|». Для этого необходимо нажать кнопку <Сохранить> (рисунок 5). По нажатии кнопки на экране появляется окно, в котором нужно ввести название файла и нажать кнопку <Сохранить> (рисунок 6).

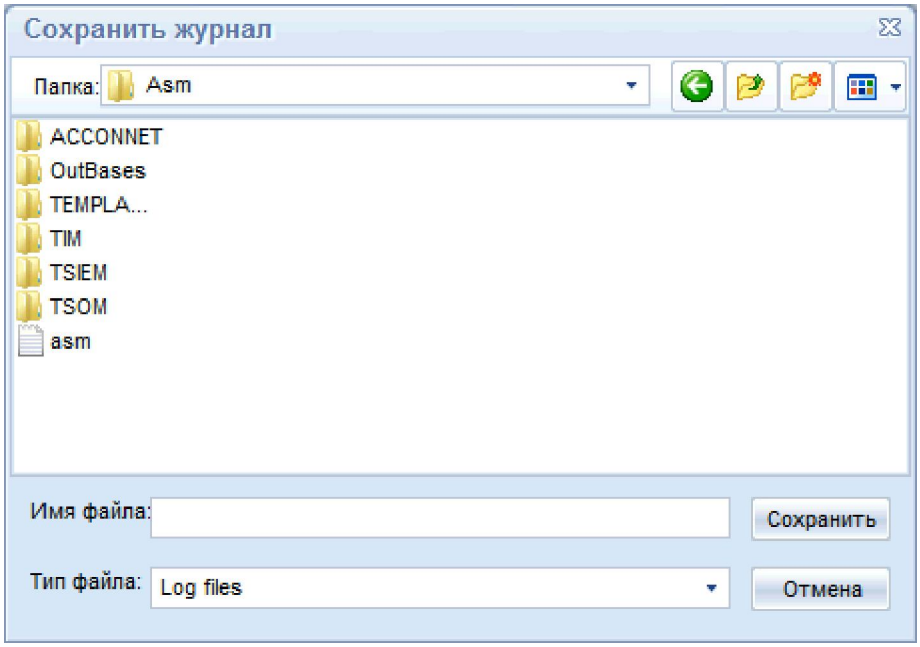

Рисунок 6 – Сохранение журнала АРМ АБИ в текстовый файл

После завершения технического обслуживания Администратор НШР предоставляет информацию о зарегистрированных событиях Администратору ИБ СУЦУ.

2.3 Аварийный режим

Аварийный режим функционирования СУЦУ характеризуется возникновением нештатных ситуации в работе компонентов сервера централизованного управления и/или полным или частичным отказом в предоставляемых сервисах ПКО, возникшим вследствие работы СУЦУ. Работа в данном режиме функционирования СУЦУ сервере централизованного управления осуществляется только под учетной записью Администратора НШР СУЦУ.

Принятие решения о переводе СУЦУ в аварийный режим должно производиться в установленном порядке, указанный порядок определяется на этапе рабочего проектирования и отражен в соответствующих руководствах.

2.4 Действия Администратора нештатного режима функционирования в аварийном режиме

1) Администратор нештатного режима функционирования обеспечивает доступность всех событий ИБ, зарегистрированных СУЦУ в аварийном режиме, для анализа и контроля персонала СУЦУ после устранения нештатной ситуации. Действия Администратора нештатного режима в случае аварийного сбоя системы идентичны действиям в случае сервисного режима в рамках ПО «ASM»;

2) в случае необходимости Администратор нештатного режима связывается с Администратором СУЦУ для устранения возникшего сбоя в системе;

3) в случае нарушения сетевого взаимодействия между сервером централизованного управления и ПКО администратор нештатного режима обеспечивает возможность получения журналов событий ИБ от ПКО, с которыми отсутствует сетевое соединение. Данная функциональность позволяет сохранить журналы на

какой-либо носитель и перенести их с ПКО на сервере централизованного управления.

3 Перечень принятых сокращений

АБИ	Администратор безопасности информации (то же, что АИБ)
АИБ	Администратор информационной безопасности
АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ИБ	Информационная безопасность
ИС	Информационная система
НСД	Несанкционированный доступ
НШР	Нештатный режим
ПКО	Подконтрольный объект
ПО	Программное обеспечение
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СУЦУ	Система централизованного управления
СУ	Система управления
ASM	Accord Security Management

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводительного документа	Подпись	Дата
	измененных	замененных	новых	Аннулированых					

СОГЛАСОВАНО

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата