

УТВЕРЖДЕН
11443195.4012-053 ИЗ 2012 ЛУ

**СИСТЕМА УДАЛЕННОГО ЦЕНТРАЛИЗОВАННОГО
УПРАВЛЕНИЯ СЗИ ОТ НСД АККОРД**

Руководство Оператора

Листов 10

Москва
2014

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 Оператора СУЦУ, связанные с непосредственной работой подсистемы в штатном режиме функционирования.

СОДЕРЖАНИЕ

1 Введение	4
1.1 Область применения	4
1.2 Функции Оператора СУЦУ	4
1.3 Комплект поставки	4
2 Назначение и условия применения	5
2.1 Назначение	5
2.2 Условия применения	5
3 Порядок работы	6
4 Сообщения программных средств комплекса и порядок действий по ним	7
5 Перечень принятых сокращений	8

1 Введение

1.1 Область применения

Деятельность Оператора СУЦУ.

1.2 Функции Оператора СУЦУ

Оператор СУЦУ выполняет следующие функции:

- обеспечивает мониторинг взаимодействия и функционирования технических и программных средств СУЦУ;
- регистрирует нештатные ситуации на КТС СУЦУ, КТС смежных подсистем, на которых размещены компоненты СУЦУ, или каналах их взаимодействия и уведомляет о них Администратора СУЦУ.

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.

2 Назначение и условия применения

2.1 Назначение

СУЦУ обеспечивает:

- централизованный сбор и хранение информации о зарегистрированных событиях доступа к ПКО;
- возможность централизованного управления средствами защиты информации от несанкционированного доступа на ПКО;
- единую точку контроля доступа к периферийным устройствам и контроля использования отчуждаемых машинных носителей.

2.2 Условия применения

Обязательным условием применения Системы является оснащение элементов АС следующими программно-аппаратными средствами:

На рабочих станциях

- ПАК СЗИ от НСД «Аккорд»;
- клиент централизованного управления.

На сервере централизованного управления

- ПАК СЗИ от НСД «Аккорд»;
- сервер централизованного управления.

3 Порядок работы

Оператор СУЦУ обеспечивает мониторинг взаимодействия и функционирования технических и программных средств Системы.

Оператор регистрирует нештатные ситуации на комплексе технических средств (КТС) Системы, КТС смежных подсистем, на которых размещены компоненты СУЦУ, или каналах их взаимодействия и уведомляет о них администратора СУЦУ.

4 Сообщения программных средств комплекса и порядок действий по ним

При работе на СВТ, оснащенный комплексом «Аккорд» и ASM, могут возникать ситуации, при появлении которых комплекс выдает сообщения. Выводимые на экран монитора сообщения, причины их появления и методы их устранения приведены в таблице 1.

Таблица 1 – Сообщения программных средств комплекса и методы их устранения

Сообщение на экране	Причины появления сообщения	Порядок действий
«Ошибка чтения ТМ...» (на красном фоне)	ТМ-идентификатор был неправильно прислонен к съемнику информации.	Снова приложить ТМ-идентификатор к съемнику информации после появления соответствующего запроса.
Это не сетевой ТМ	Прислонен неверный ТМ-идентификатор	Прислонить правильный ТМ-идентификатор
«В данное время вход в систему запрещен»	Для данного пользователя не разрешен вход в систему в данное время	Вызвать Администратора ИБ и уточнить разрешенное время работы
«Ваш пароль просрочен. Обратитесь к администратору для смены» (на красном фоне)	Окончилось время жизни пароля. Закончились все попытки смены пароля.	Вызвать Администратора ИБ. Изменить параметры пароля.
«Доступ не разрешен!» (на красном фоне)	Не зарегистрированный идентификатор. Не правильно введен пароль. В данное время работают временные ограничения.	Обратиться к Администратору ИБ для регистрации. Повторить процедуры идентификации / аутентификации.
«Требуется Администратор» (на красном фоне) «Разберитесь с ошибками» (на оранжевом фоне)	Несовпадение контрольных и текущих параметров аппаратной и программной частей системы.	Вызвать Администратора ИБ. Выявить и устранить причины изменения параметров.
«Такую комбинацию символов недопустимо использовать в качестве пароля»	Это сообщение появляется в случае, если пользователь вводит комбинацию символов, которую легко подобрать (например, qwerty).	Ввести более сложную комбинацию символов.
«Отсутствует разрешение на смену пароля»	Это сообщение появляется, если у пользователя нет прав на смену пароля.	Попросить администратора дать пользователю права на самостоятельную смену пароля.
В идентификаторе нет свободных страниц для записи»	Объем идентификатора DS1996 позволяет хранить данные о 31 рабочей станции и их открытые ключи. Если Вы уже зарегистрировали 31 станцию, то при попытке зарегистрировать следующую выдается сообщение	Если в сети остались незарегистрированные станции, то следует добавить список на АРМ АБИ и после очистки памяти ТМ провести регистрацию остальных рабочих станций.

5 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
КТС	Комплекс технических средств
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
НШР	Нештатный режим
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПКО	Подконтрольный объект
ПО	Программное обеспечение
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СУЦУ	Система централизованного управления
СУ	Система управления
УП	Управление персоналом
ASM	Accord Security Management

