УТВЕРЖДЕН
11443195.4012-053 ИЗ.2 2012 ЛУ

СИСТЕМА УДАЛЕННОГО ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ СЗИ ОТ НСД АККОРД

Руководство Оператора ИБ

Листов 14

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

СОДЕРЖАНИЕ

1 Введение

1.1 Область применения

Деятельность Оператора ИБ СУЦУ.

1.2 Функции Оператора ИБ СУЦУ

Оператор ИБ СУЦУ выполняет следующие функции:

- обеспечивает мониторинг состояния информационной безопасности в части защиты от несанкционированного доступа средствами СУЦУ;
- в случае выявления фактов несанкционированного доступа ИБ СУЦУ сообщает о них Администратору информационной безопасности СУЦУ;
- осуществляет регулярное создание отчетов о зафиксированных событиях ИБ СУЦУ и уведомляет о результатах Администратора ИБ 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, далее по тексту ПКО);
- 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 – 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 подконтрольным объектам;
- возможность централизованного управления средствами защиты информации от несанкционированного доступа на подконтрольных объектах;
- 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

3.1 Обеспечение мониторинга состояния информационной безопасности

Оператор ИБ обеспечивает мониторинг состояния информационной безопасности в части защиты от несанкционированного доступа средствами СУЦУ.

Оператор ИБ имеет возможность наблюдать за пользователями, работающими под контролем ПАК СЗИ от НСД Аккорд в составе ЛВС.

Кроме того, в СУЦУ происходит получение журналов регистрации работ ПАК СЗИ от НСД Аккорд в режиме реального времени, то есть все попытки НСД тут же отображаются на экране сервера управления.

3.2 Контроль событий информационной безопасности

В случае обнаружения попытки несанкционированного доступа Оператор ИБ должен сообщить о факте нарушения Администратору ИБ.

3.3 Работа с журналами

Открыв вкладку «Журналы», Оператор ИБ 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).

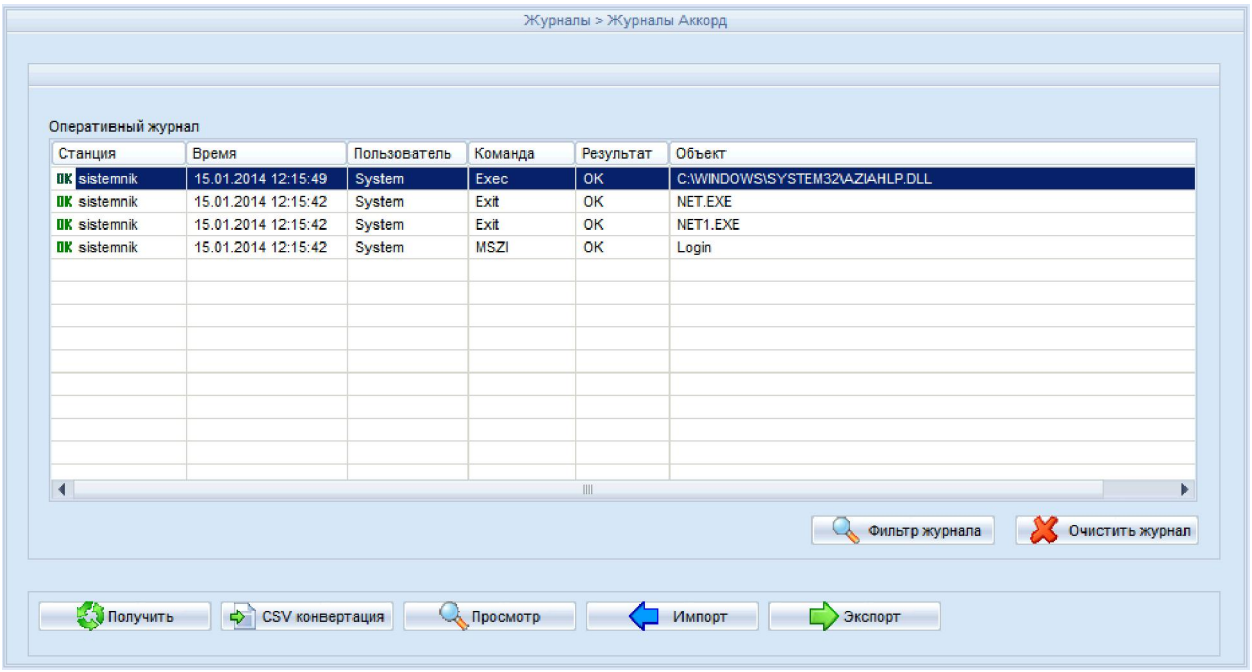

Рисунок 1 - Журналы «Аккорд»

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).

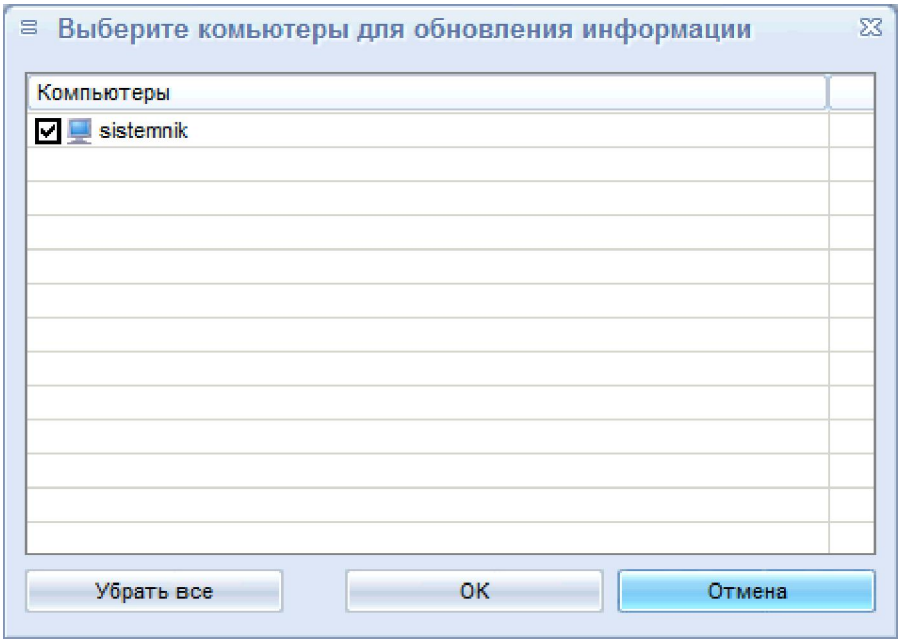

Рисунок 2 – Выбор ПКО, с которых планируется получить журналы[1)]

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

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.

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

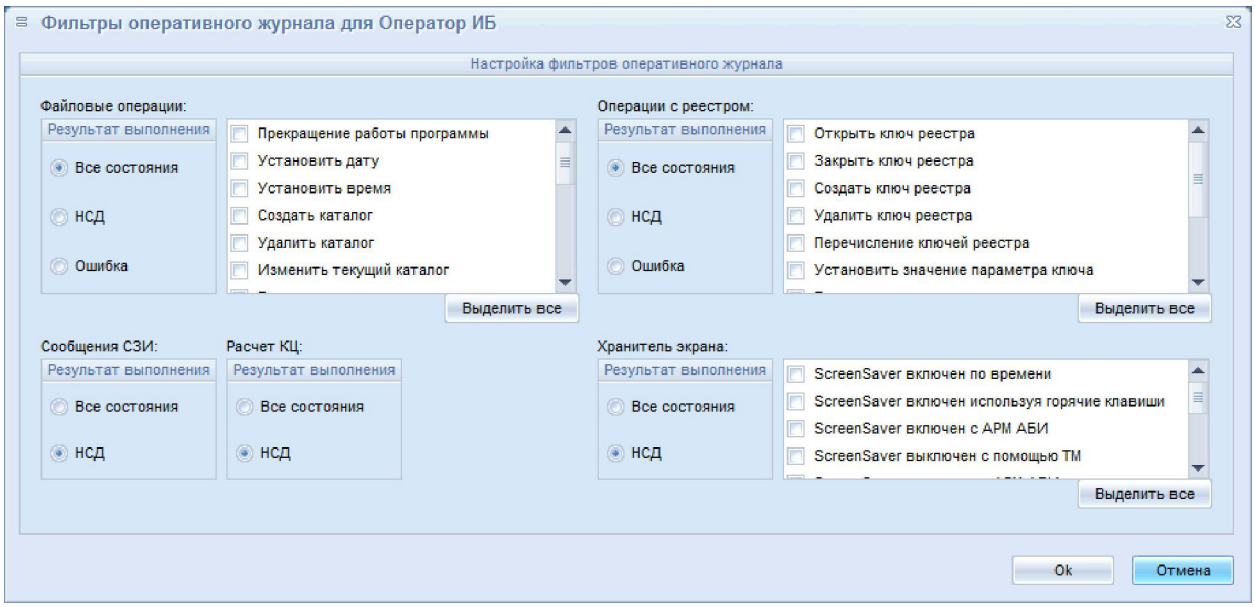

Рисунок 3 – Фильтры оперативного журнала для текущей учетной записи

В нем можно выбрать типы событий, информация о которых передается в оперативный журнал, для текущей учетной записи (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,

[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.

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).

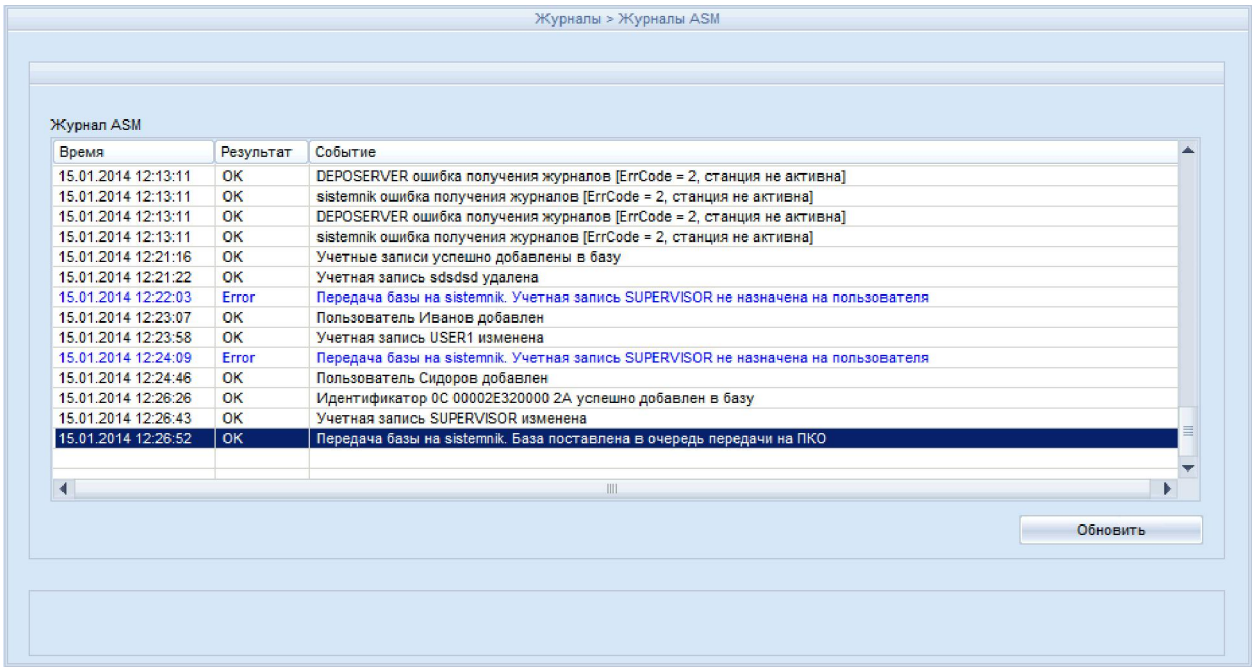

Рисунок 4 - Журнал ASM

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

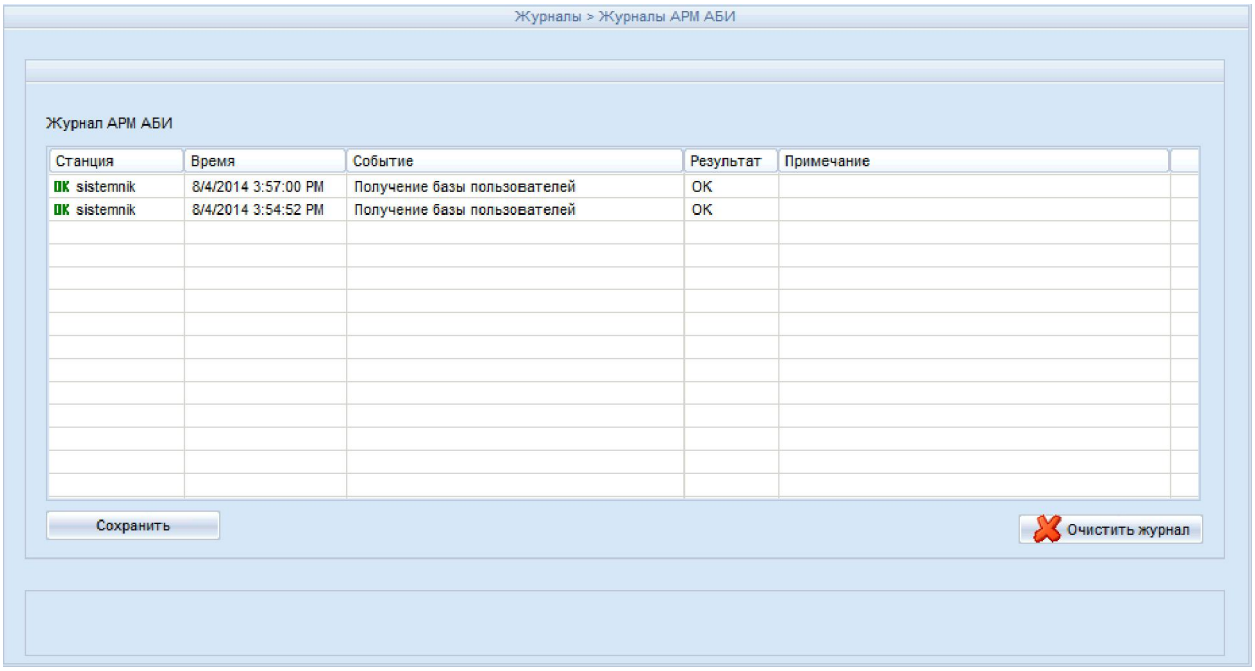

Рисунок 5 – Журнал АРМ АБИ

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).

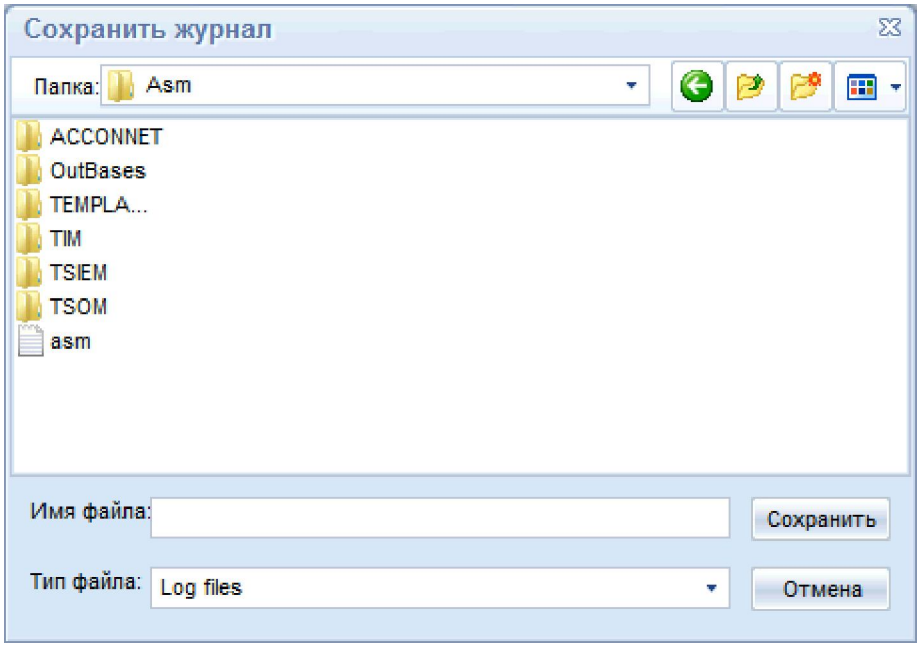

Рисунок 6 – Сохранение журнала АРМ АБИ в текстовый файл

4 Сообщения программных средств комплекса и порядок действий по ним

При работе на СВТ, оснащенном СЗИ от НСД «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
РФ	Российская Федерация
СВТ	Средства вычислительной техники
СЗИ	Средство защиты информации
СУЦУ	Система централизованного управления
СУ	Система управления
УП	Управление персоналом
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	аннулированных					

СОГЛАСОВАНО

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