УТВЕРЖДЕН 11443195.4012-053 92 2012 ЛУ

СИСТЕМА УДАЛЕННОГО ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ СЗИ ОТ НСД АККОРД

Руководство Администратора ИБ средств защиты информации от НСД (АИБ технологического участка)

Листов 56

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 Администратора ИБ технологического участка СУЦУ (далее по тексту Администратор ИБ ТУ СУЦУ), связанные с непосредственной работой СУЦУ в штатном режиме функционирования.

СОДЕРЖАНИЕ

1 Введение	4
1.1 Область применения	4
1.2 Функции Администратора ИБ (АИБ технологического участка)	4
2 Планирование работы и эксплуатация комплекса	5
3 Работа с ASM	6
3.1 Управление	6
3.2 Вкладки ASM	6
3.2.1 Вкладка «Роли»	6
3.2.2 Вкладка «Идентификаторы»	16
3.2.3 Вкладка «Компьютеры»	21
3.2.4 Вкладка «Учетные записи»	34
3.2.5 Создание пользователя технологического участка	44
3.3 Работа с журналами	45
4 Сообщения программных средств комплекса и порядок действий по	
НИМ	52
5 Сообщения программных средств подконтрольных объектов	53
6 Перечень принятых сокращений	54

1 Введение

1.1 Область применения

Деятельность Администратора ИБ СУЦУ (АИБ технологического участка)

1.2 Функции Администратора ИБ (АИБ технологического участ-ка)

Администратор ИБ СУЦУ (АИБ технологического участка) в рамках полномочий, делегированных ему Администратором ИБ СУЦУ:

•производит следующие настройки СУЦУ:

- настройка политики безопасности;
- настройка контроля доступа;
- настройка разрешенных коммуникационных портов;
- •проводит контроль управляющего воздействия на компоненты СУЦУ в части:
 - изменения настроек (включая настройки мониторинга);
 - применения шаблонов настроек;
- участвует в разборе и устранении нештатных ситуаций, связанных как с работой СУЦУ, так и с работой СЗИ от НСД.

2 Планирование работы и эксплуатация комплекса

Для более эффективного применения комплекса «Аккорд» и поддержания уровня защищенности Администратор ИБ ТУ СУЦУ выполняет следующие задачи:

• поддерживает средства защиты в работоспособном состоянии и периодически контролирует корректность их работы;

• проводит изменения настроек средств защиты в соответствии с корректировками плана защиты, вызванными изменением состава пользователей, перечня решаемых задач и соответствующими изменениями функциональных обязанностей сотрудников.

3 Работа с ASM

3.1 Управление

Пункты 4.1.1-4.1.5 посвящены описанию функций управления ASM.

Пользовательский интерфейс вкладок ASM, доступных для обслуживающего персонала СУЦУ в рамках реализации процедур управления, подчиняется единому принципу:

- кнопка <Добавить> предназначена для добавления той или иной сущности;
- •кнопка <Удалить> предназначена для удаления той или иной сущности;
- •с помощью кнопки <Импорт> можно импортировать настройки с компьютеров Системы в ASM.
- •с помощью кнопки <Экспорт> можно экспортировать настройки из ASM на компьютеры системы.

При работе с ASM следует помнить, что максимальное количество символов в именах ролей, технологических участков, компьютеров и учетных записей пользователей составляет 100 символов.

3.2 Вкладки ASM

3.2.1 Вкладка «Роли»

Права доступа (ПРД) для учетной записи определяются ролью.

В ASM предусмотрены следующие встроенные роли:

• Admins_NSHR - используется для первоначальной настройки системы, характеризуется правом полного доступа в ASM, под этой ролью работает Администратор нештатного режима (Администратор НШР) СУЦУ;

- •Admins_SCM под этой ролью работает Администратор ИБ СУЦУ.
- •Admins соответствует группе 'Администраторы' в «Аккорде»;
- Admins_XXX¹⁾ автоматически создается при создании нового технологического участка и уничтожается только при удалении данного участка; соответствует группе 'Администраторы' в «Аккорде»;
- •Everyone соответствует группе 'Обычные' в «Аккорде»; в ASM;
- •Everyone_XXX автоматически создается при создании нового технологического участка и уничтожается только при удалении данного участка; соответствует группе 'Обычные' в «Аккорде»; в ASM;
- •AIBs_SCM Администратор информационной безопасности специализированной подсистемы управления и мониторинга средств защиты информации от несанкционированного доступа;

¹⁾ Номер **XXX** соответствует номеру участка.

- •AIB_TU: имя роли роль, под которой работает Администратор ИБ технологического участка; создается после добавления технологического участка Администратором ИБ;
- •OIBs_SCM под этой ролью работает Оператор информационной безопасности СУЦУ.

Для того чтобы создать новую роль, редактировать или удалить уже существующую, следует открыть в ASM вкладку Управление>Роли (рис. 1).

я роли	Описание роли	Участки
ADMINS_1	Встроенная роль: Администраторы Аккорд	Тех.участок_1
EVERYONE_1	Встроенная роль: Пользователи Аккорд	Тех.участок_1
Puinter pos		Чиспо объектор

Рисунок 1 - Роли системы

Для добавления новой роли необходимо нажать кнопку <Добавить>. В появившемся окне (рисунок 2) необходимо задать роли имя (имя роли следует вводить корректно, так как после создания роли изменить имя нельзя), указать принадлежность роли технологическому участку¹⁾. Также можно дать описание роли (это поле не является обязательным для заполнения).

¹⁾ При создании ролей пользователей ПКО необходимо обязательно указывать их принадлежность соответствующему технологическому участку

	Упра	вление > Роли системы > Добаві	ИТЬ
Имя роли:	Описание		Участок к которому относится роль
Пользователи	<		
		Привилегии роли	
			Тех.участок_1
🗸 Добавить			
🗸 Назад			
· · · · · · · · · · · · · · · · · · ·			

Рисунок 2 – Создание роли

По нажатии кнопки <Добавить> (рисунок 2) на экране появляется редактор ПРД, в котором следует выбрать необходимые параметры роли и сохранить изменения.

При создании роли по шаблону необходимо левой кнопкой мыши выбрать раскрывающийся список в поле «Имя роли» (рисунок 2). На экране появляется окно, в котором необходимо выбрать роль и нажать кнопку <Ok> (рисунок 3).

00	Создать новую роль	ь по шаблону		23
	Роль	Тех.участок		
	BK ADMINS	Вся система		
	IK ADMINS_1	Тех.участок_1		
	IK ADMINS_2	Тех.участок_2		
	IK EVERYONE	Вся система		
	IK EVERYONE_1	Тех.участок_1		
	IK EVERYONE_2	Тех.участок_2		
			Ok Отме	на

Рисунок 3 – Создание роли по шаблону

После выполнения данной процедуры у новой роли будут определены такие же задачи для запуска и файлы для проверки КЦ, как и у выбранной из шаблона роли.

Для редактирования следует дважды щелкнуть по роли системы либо нажать кнопку <Редактировать>, после чего на экране появляется следующее окно (рисунок 4):

	Упр	авление > Роли системы > Редактировать	
Имя роли: Admin	Описание		Участок к которому относится роль Тех.участок 1
		-	
		Привилегии роли	
		Задачи для запуска	Файлы для проверки КЦ
		назначены	не определены
		Редактировать	Редактировать
✔ Редактировать			
Назад			

Рисунок 4 - Редактирование роли

Чтобы задать или редактировать задачи для запуска роли необходимо нажать кнопку <Редактировать> в поле «Задачи для запуска». После этого на экране появляется окно (рисунок 5), в котором нужно редактировать необходимые параметры и нажать кнопку <Сохранить>.

Редактирование списка задач для запуска для роли admin	23
[Group1] GroupName=Группа 1 [Task1.1] DisplayName=FAR Manager ImagePath=c:\progra~1\Far.exe	
[Task1.2] #Комментарий DisplayName=Volcov Commander ImagePath=c:\vc\vc.com	
[Group2] GroupName=Группа 2 (Ярлыки) [Task2.1] DisplayName=Acdsee ImagePath=C:\Program Files\ACDSee32\Shortcuts\ACDSee32.Ink WorkDir=C:\Program Files Parameters=c:\test.jpg WaitEndTask=No	
[RUN_BEFORE] GroupName=Автозапуск	
[RunTask1]	¥
Удалить Из шаблона Из файла Сохранить Отмена	

Рисунок 5 – Редактирование списка задач для запуска

При создании списка задач для запуска по шаблону необходимо нажать кнопку <Из шаблона> (рисунок 5). После выполнения описанной процедуры на экране появляется окно:

В Создать список задач по шаблону				
Задачи	Тех.участок			
OK admin.ACT				
BK ADMINS_1.ACT	Тех.участок_1			
IK EVERYONE_1.ACT	Тех.участок_1			
		_		
		_		
		_		
		_		
1				
	Ок Отмена			

Рисунок 6 – Создание списка задач по шаблону

Нужно выбрать необходимый шаблон с именем роли, задачи которой планируется назначить редактируемой роли, и нажать кнопку <Ok>.

При создании списка задач для запуска из файла необходимо нажать кнопку <Из файла>. После выполнения описанной процедуры на экране появляется окно:

Выбор списка задач для запуска	23
Папка: 🛺 Аѕт 🔹	G 🖻 📂 💷 -
ACCONNET OutBases OutBases_Te TEMPLA TIM TSIEM TSIEM	
Имя файла:	Открыть
Тип файла: ACT files	• Отмена

Рисунок 7 – Создание списка задач из файла

Необходимо выбрать нужный каталог (рисунок 7) и нажать кнопку <От-крыть>.

В появившемся на экране окне необходимо выбрать нужный файл (рисунок 8) и нажать кнопку <Открыть>.

Выбор спи	ска задач дл	я запуска		23
Папка: 鷆 ТЕ	MPLATE		• (3)	1 1 1
admin_1 admin_1 ADMINS_1 EVERYONE_ sfdfasf Templ	1			
Имя файла: _S	UPERVISOR.ACT	Γ		Открыть
Тип файла: 🛛	ACT files		•	Отмена

Рисунок 8 – Выбор задач для запуска из файла

После того, как изменения внесены, необходимо нажать кнопку <Сохранить> (рисунок 5), для отмены операции – кнопку <Отмена> (рисунок 5).

Чтобы задать или редактировать файлы для проверки КЦ необходимо нажать кнопку <Редактировать> в поле «Файлы для проверки КЦ». После этого на экране появляется окно:



Рисунок 9 – Редактирование списка КЦ для роли

Для создания списка файлов для проверки КЦ по шаблону необходимо нажать кнопку <Из шаблона> (рисунок 9). После выполнения описанной процедуры на экране появляется окно (рисунок 10), в котором необходимо выбрать нужный шаблон и нажать кнопку <Ok>.

В Создать список	КЦ по шаблону	23
КЦ	Тех.участок	
OK admin.HSH		
OK admin_1.HSH		
	Ok	Отмена

Рисунок 10 – Создание списка файлов для проверки КЦ по шаблону

Для создания списка файлов для проверки КЦ из файла необходимо нажать кнопку <Из файла> (рисунок 9). После выполнения описанной процедуры на экране появляется окно выбора каталога. Необходимо выбрать нужный каталог и нажать кнопку <Открыть>.

В появившемся на экране окне необходимо выбрать нужный файл и нажать кнопку <Открыть> (рисунок 11).

Выбор сп	иска КЦ						Σ	3
Папка: 鷆 Т	TEMPLATE		•	G	ø	10		-
admin admin_1								
Имя файла:	admin.hsh					Откры	ть	
Тип файла:	HSH files			•		Отме	на	

Рисунок 11 – Выбор файлов для проверки КЦ

После того, как изменения внесены, необходимо нажать кнопку <Сохранить> (рисунок 9), для отмены операции – кнопку <Отмена> (рисунок 9).

Далее необходимо нажать кнопку <Редактировать> (рисунок 4). На экране появляется редактор прав доступа ACED32 (рисунок 12), в котором можно изменить ПРД роли, а также осуществить предварительный просмотр базы пользова-

телей (без возможности модификации и сохранения), полученной от подконтрольного объекта. Для этого нужно выбрать команду Файл>Импорт базы, после выполнения которой загрузится файл базы пользователей ПКО (при выходе из редактора изменения в базе не сохраняются).

🎦 АСЕD32 Редактор базы пользова	телей ПАК "Аккорд"	IX
<u>Ф</u> айл <u>К</u> оманды <u>?</u>		
2 *× ⊅ ♥ ⊥品 ⊅	🗩 🛛 🕹 🗐 📃	
ADMIN		
E Администраторы Гл.Администратор ASM_ACCOUNT	Идентификация/Аутентификация NT группы Шипка Не назначен	
	Вход в систему Параметры пароля Временные ограничения Нет Блокирован Подконтрольный	
	Программная среда Спартовый каталог Стартовая задача Детальность журнала	
	Гашение экрана И СТВL+F12 ALT+F12 5 Опции Результаты И/А 000000000 IIIII000 Контроль целостности Разграничение доступа Нет Доступ к объектам	

Рисунок 12 - Редактирование базы пользователей «Аккорд»

Чтобы установить доступ к коммутационным портам и периферийным устройствам, необходимо левой кнопкой мыши выбрать раскрывающийся список в поле «Разграничение доступа». Далее на экране появляется окно редактирования списка объектов, в котором можно выбрать необходимый объект и определить для него права доступа. На рисунке 13 показан список объектов (устройства, файловая система, реестр), для которых могут быть заданы правила разграничения доступа (подробнее см. документ «ПАК "Аккорд-Win32" (версия 4.0). Установка правил разграничения доступа. Программа ACED32» 11443195.4012-036 97"», подраздел 6.15 или «ПАК "Аккорд-Win64" (версия 5.0). Установка правил разграничения доступа. Программа ACED32» 11443195.4012-036 97"»,

🎦 Редактирование правил разграничения доступа для Обычные		- 🗆 🗙
Объекты Процессы		
Объеклы	Права доступ	a 🔺
NHKEY_DYN_DATAN	RWCDNVOMEGn	S
NHKEY_LOCAL_MACHINEN	RWCDNVOMEGn	S
\HKEY_USERS\	RWCDNVOMEGn	S
	RWCDNV MEGn	XS
{Generic Bluetooth Adaptor}		
{IEEE1394 Bus host controllers}		
{Network adapters\Microsoft Virtual WiFi miniport		
{Ports (COM & LPT)}		
{Smart card readers}		
{Universal Serial Bus controllers}		
{USB controllers}		
{Контроллеры USB}		
{Контроллеры универсальной последовательной шины U		
{Порты (COM u LPT)}		
{Paguoмogyлu Bluetooth}		
{Семевые aganmepы\Aganmep мини-порта виртуального		
{Устрои́ства чтения смарт-карт}		
{Хост-контроллеры шины IEEE 1394}		
<u></u>		
INSERT DELETE ENTER	F2	ESC
Новый Удалить Редактировать 🚭 USB/SD	Сохранить	Отмена

Рисунок 13 – Перечень объектов для установки прав доступа

Для удаления роли во вкладке Управление>Роли необходимо выбрать роль и нажать кнопку <Удалить> (рисунок 1). После этого на экране появляется следующее сообщение (рисунок 14):



Рисунок 14 – Удаление роли

Если действительно необходимо удалить роль, следует нажать кнопку <Да>.

ВНИМАНИЕ! Если роль сопоставлена некоторому технологическому участку, ее могут редактировать только Администратор ИБ соответствующего технологического участка!

3.2.2 Вкладка «Идентификаторы»

Для того чтобы работать с идентификаторами, следует открыть в ASM вкладку Управление>Идентификаторы (рисунок 15).

	припадлежат учетным записям	Unincanne
L 0C 000057810000 52	ADMIN_NSHR, SUPERVISOR	Идентификатор Адм
2 OC 000125A50000 48	AIB_TU	
Выбрать все		Число объектов: 3

Рисунок 15 - Идентификаторы системы

При добавлении или изменении идентификатора, надо выбрать опцию «уже записан» или «сгенерировать» - в последнем случае в идентификаторе генерируется новый секретный ключ взамен старого. Далее необходимо нажать кнопку <Прочитать> и прислонить таблетку (рисунок 16). Для добавления идентификатора в базу необходимо нажать кнопку <Добавить>.

	Управ	вление > Идентификаторы системы > Добавить
1дентификатор:	Описание	e
Секретный ключ:	роверить	Новый идентификатор Предъявите идентификатор! Отмена
Назад		

Рисунок 16 - Требование предъявить идентификатор

По нажатии кнопки <Проверить> осуществляется проверка соответствия открытых ключей базам ПКО. Если открытые ключи соответствуют базам ПКО, на экране появляется соответствующее сообщение (рисунок 17):



Рисунок 17 – Проверка соответствия открытых ключей базам ПКО

Чтобы удалить идентификатор, необходимо во вкладке «Идентификаторы» (рисунок 15) выбрать нужный идентификатор и нажать кнопку <Удалить>. После выполнения данной процедуры на экране появляется следующее сообщение:

Accord Se	curity Management V1.0.8.55
1	Вы действительно хотите удалить идентификатор 0С 00002E320000 2A?
	<u>Y</u> es <u>No</u>

Рисунок 18 – Удаление идентификатора

Если действительно необходимо удалить идентификатор, следует нажать кнопку <Да> (рисунок 18).

Идентификаторы можно импортировать из базы СЗИ от НСД «Аккорд» (например C:\Accord.NT\ ACCORD.AMZ). Для этого во вкладке «Идентификаторы» (рисунок 15) необходимо нажать кнопку <Импорт>. На экране появляется окно (рисунок 20), в котором нужно нажать кнопку <Обновить>, чтобы обновить базы «Аккорда». По нажатии кнопки <Обновить> на экране появляется окно (рисунок 34), в котором следует отметить необходимые ПКО и нажать кнопку <OK> (в окне, показанном на рисунке 34, отображаются только те компьютеры, которые находятся в сети).

Выберите комьютеры для обновления информации	23
Компьютеры	
🗹 💻 sistemnik	
	_
	_
	_
	_
	_
Убрать все ОК Отмена	

Рисунок 19 – Выбор компьютеров для обновления информации

Далее необходимо нажать кнопку <Импортировать> (рисунок 20).

Управление > Идентификаторы системы > Импорт
можете импортировать идентификаторы из:
Gasu Accord
бновить базы Аккорд-а, используя АРМ АБИ
🗸 Обновить
Импортировать
🗶 Назад
× · · · · · · · · · · · · · · · · · · ·

Рисунок 20 – Импорт идентификатора

По нажатии кнопки <Импортировать> (рисунок 20) на экране появляется окно выбора каталога (рисунок 21), в котором следует выбрать необходимый файл.

Папка: 🌇 sistemnik 🔹 🗸 🧭 📂	- 💷
sistemnik	
Имя файла: sistemnik.amz	оыть
Тип файла: Accord files (*.amz, *.atf) • Отп	иена

Рисунок 21 – Окно выбора каталога

После этого в правой части окна появятся импортированные идентификаторы, следует выбрать из них необходимые для добавления в базу (для выбора всех идентификаторов нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 22).

		Импортированные идентификаторы:
базы Accord	Импортированные идентифин	аторы, выберите необходимые для добавления в базу:
	Идентификаторы	Описание
новить базы Аккорд-а, используя АРМ АБИ	C 00002E320000 2A	Импортирован от USER1(sistemnik)
	OC 000057810000 52	Импортирован от SUPERVISOR(sistemnik)
🗸 Обновить		
🖉 Импортировать	4	
	Выбрать все	Добавить

Рисунок 22 - Выбор импортированных идентификаторов(импорт из базы «Аккорда»)

Если необходимо определить, добавлен ли идентификатор в базу ASM, следует нажать кнопку <Поиск> на вкладке «Идентификаторы» (рисунок 15). Появится окно с сообщением «Предъявите идентификатор» (рисунок 23).

яттификаторы системы	Принадлежат учетным записям	Описание
C 000057810000 52	ADMIN_NSHR, SUPERVISOR	Идентификатор Адм
C 000125A50000 48	AIB_TU	
Π	онск	
	Предъявите идентификатор	
¥		
	Отмена	
BUSDATH BOA		Uwana afa arman:

Рисунок 23 - Сообщение «Предъявите идентификатор»

Если данный идентификатор добавлен в базу ASM, то этот идентификатор будет выделен (рисунок 24), иначе в нижней части окна появится сообщение «Идентификатор не зарегистрирован!» (рисунок 25).

	принадлежа тучетным записям	Описание
	ADMIN_NSHR, SUPERVISOR	Идентификатор Адм.
00 000125A50000 48	AIB_TU	

Рисунок 24 - Найдена учетная запись, которой назначен идентификатор

ентификаторы системы	Принадлежат учетным записям	Описание
C 000057810000 52	ADMIN_NSHR, SUPERVISOR	Идентификатор Адм
C 000125A50000 48	AIB_TU	
Выбрать все		Число объектов:
•		E a Davian

Рисунок 25 - Сообщение о том, что идентификатор не зарегистрирован в базе ASM

3.2.3 Вкладка «Компьютеры»

Для того чтобы работать с компьютерами, следует открыть в ASM вкладку Управление>Компьютеры (рисунок 26).

омпьютеры системы	Назначенные пользователи	Тех. участок	Описание
E comp1	<не назначен>	Тех.участок1	
Выбрать все Обновить		Чи	сло объектов: 1

Рисунок 26 – Компьютеры системы

Кнопка <Печать> позволяет распечатать выбранную информацию на принтере, а также сохранить в файл (с указанным разделителем). По нажатии кнопки <Печать> на экране появляется окно, в котором следует выбрать способ печати: в файл или на принтер, тип выводимой информации (имя компьютера, описание компьютера, тех. участок и т.д.); при печати в файл следует также указать разделитель (рисунок 27). В случае печати в файл выбранные параметры сохраняются в файле ASM\AccountName_PrinterParam.ini, где AccountName – имя учетной записи.

🗏 Печать		23
Вывод информации	Выводить на печать	
 В файл Разделитель: На принтер 	 Имя компьютера Описание компьютера Тех.участок IP-адрес компьютера Имя. № Компьютера 	
Выводить шапку	ок	Отмена

Рисунок 27 - Печать информации о подконтрольном объекте

Для добавления компьютера необходимо нажать кнопку <Добавить> (рисунок 26). В появившемся окне (рисунок 28) можно задать имя компьютера, его описание и назначить этот компьютер технологическому участку (последние два условия не являются обязательными для заполнения).

ия компьютера.		Описание ког	ипьютера:	Принадлежит тех.участку:	
				Тех.участок_1	
			Описание компьютеров		
Учетные записи, п	ринадлежащие ком	пьютеру и свободные:	🔲 Показывать только назначен	Тех.участок_1 ные	
Учетная запись	Логин	Роль	Пользователи	-	
Супервизор	supervisor	ADMINS_1	Пользователь_Сидоров		
🗸 Примени	ть			📕 Конфи	
					пурация согт

Рисунок 28 – Добавление компьютера

Для редактирования компьютера необходимо нажать кнопку <Редактировать (рисунок 26). В появившемся окне можно редактировать имя компьютера, его описание, а также принадлежность компьютера к технологическому участку.

По нажатии кнопки <Конфигурация C3И> на экране появляется окно, в котором отображаются настройки C3И выбранного ПКО, версия его программного обеспечения и IP-адрес, серийный номер контроллера, а также инвентарные номера ПКО и контроллера «Аккорд-АМДЗ» (последние поля заполняются вручную, рисунок 29).

Конфигурация СЗИ		гурация СЗИ Верси	Версии ПО	
Основная		Синхронизация Windows:	6.1.0.7601	
Страница ТМ Таймаут для идентификатора Таймаут для пароля	0 ‡ 15 ‡ 15 ‡	 С базой АМДЗ С стевой агент: С базой пользователей NT Удалять незарег. пользователей Использовать полное имя в учетных записях NT Драйвер контроллера: Завершать сессию только перезагрузкой Процессор контроллера: По контроллера: 	2.3.19.22 5.0.7.35 3.54.0.0 1.48.0.0 2.1.15	
Механизмы разграничения Дискреционный Мандатный	я доступа	Разное Число проходов, при очистке файлов: 1 ↓ Очищать файл подкачки IP-адрес:	55038435 192.168.0.2	
Включить контроль доступа к	устройствам	 Очищать сетевые файлы Выводить на экран сообщения о НСД Мягкий режим Записывать в журнал логические имена дисков Печатать гриф приложения в заголовке окна Блокировать USB-устройства при работе SS Записывать в журнал НСД при поиске файлов 	я информация 12346 654321	

Рисунок 29 – Конфигурация СЗИ на подконтрольном объекте

ВНИМАНИЕ! Для получения версии ПО требуется наличие сетевого клиента не ниже v.2.3.15.15. Версию ПО контроллера можно получить в том случае, если на ПКО имеется «Аккорд-АМДЗ» (DOS) v. 2.1.15. Для ранних версий «Аккорда-АМДЗ» (DOS) и «Аккорда» (LE) версия предоставляется на основании версии прошивки процессора.

Если необходимо определить, зарегистрирован ли компьютер в системе, следует нажать кнопку <Поиск> во вкладке «Компьютеры» (рисунок 26). По нажатии кнопки на экране появляется окно (рисунок 30), в котором необходимо указать IP-адрес компьютера или его имя

Рисунок 30 – Поиск компьютера по имени или IP-адресу

Если данный компьютер зарегистрирован в системе, то этот компьютер будет выделен (рисунок 31), иначе в нижней части окна появится сообщение «Компьютер не найден!» (рисунок 32).

мпьютеры системы	Назначенные пользователи	Тех. участок
sistemnik	Администратор нештатного режима CUV[SUPERVISOR], Ад	министратор Тех.участок_1
Выбрать все		Unero efit error:
		HIGHO BERTOD.

Рисунок 31 – Найден компьютер

мпьютеры системы	Назначенные пользователи	Тех. участок
📃 sistemnik	Администратор нештатного режима CUV[SUPERVISOR], Администрат	гор Тех.участок_1
Выбрать все		Число объектов:

Рисунок 32 – Сообщение о том, что компьютер не найден

Чтобы удалить компьютер, необходимо выделить его и нажать кнопку <Удалить> на вкладке «Компьютеры» (рисунок 26). Появится окно подтверждения этого действия (рисунок 33), следует нажать кнопку <Да>, если действительно нужно удалить компьютер.

Accord Se	curity Management V1.0.8.55
1	Вы действительно хотите удалить компьютер sistemnik?
	Yes No

Рисунок 33 – Окно подтверждения удаления компьютера

По нажатии кнопки <Да> происходит очистка каталогов, содержащих файлы ПКО (каталоги \Asm\ACCONNET\OUT\CompName\), а также каталогов \Asm\OutBases_Temp и \Asm\ACCONNET\IN.

Кнопка <Передача баз> необходима для передачи баз пользователей на подконтрольные объекты (подробнее ниже).

Кнопка <Проверка баз> предоставляет возможность автоматического применения изменений ролей и баз пользователей, произведенных на ПКО.

ВНИМАНИЕ! Синхронизировать базы пользователей могут только Администраторы ИБ соответствующих технологических участков!

Кнопка <Обновить> во вкладке «Компьютеры» (рисунок 26) необходима для обновления списка активных ПКО.

Кнопка <Импорт> во вкладке «Компьютеры» (рисунок 26) необходима для регистрации ПКО. По нажатии данной кнопки на экране появляется окно импорта компьютеров (рисунок 35). Чтобы импортировать компьютеры из базы «Аккорда-РАУ», необходимо установить соответствующий флаг («Вы можете импортировать компьютеры из:» - «базы Accord -PAУ») в окне, показанном на рисунок 35, и нажать кнопку <Импортировать>. При необходимости обновить базы перед выполнением этой операции следует нажать кнопку <Обновить>. По нажатии кнопки <Обновить> на экране появляется окно (рисунок 34), в котором следует отметить необходимые ПКО и нажать кнопку <OK> (в окне, показанном на рисунке 34, отображаются только те компьютеры, которые находятся в сети).

🖻 Выберите комьютеры для обновления информации 🛛 Σ	3
Компьютеры]
🗹 💻 sistemnik	
]
Убрать все ОК Отмена	



Далее необходимо нажать кнопку <Импортировать> (рисунок 35).

	Управление > Компьютеры системы > Импорт
Вы можете импортировать компьютеры из:	
базы Accord-РАУ	
💿 от подконтрольных объектов	
Обновить базы Аккорд-а, используя АРМ АБИ	
🗸 Обновить	
Импортировать	
Назад	

Рисунок 35 - Импорт компьютеров

Далее на экране появляется окно (рисунок 36), в котором следует указать файл, из которого необходимо импортировать компьютеры.

Открыть файл	X
Папка: 📗 ACCONNET	- 🔇 🖻 📂 💷 -
Client.Log Client.Upd IN OUT ACNODE	
Имя файла: ACNODE.LST	Открыть
Тип файла: Accord PAY files (AcNode.lst)	• Отмена

Рисунок 36 - Выбор каталога для импорта компьютеров

После этого в правой части окна появятся импортированные компьютеры; следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 37).

можете импортировать компьютеры из:		Импортированные компьютеры:	
базы Accord-PAУ	Импортированные компь	ютеры, выберите необходимые для добав:	ения в базу:
от подконтрольных объектов	Компьютеры	Описание	
бновить базы Аккорд-а, используя АРМ АБИ			
🗸 Обновить			
/ Импортировать			•
	Выбрать все		Добавить

Рисунок 37 - Выбор импортированных компьютеров (импорт из базы «Аккорда -РАУ»)

Чтобы импортировать компьютеры от подконтрольных объектов, необходимо установить соответствующий флаг («Вы можете импортировать компьютеры из:» - «от подконтрольных объектов») в окне, показанном на рисунок 38, и нажать кнопку <Импортировать>.

можете импортировать компьютеры из:		Импортированные компьютер	ы
базы Accord-PAY	Импортированные компь	ютеры, выберите необходимые для д	обавления в базу:
от подконтрольных объектов	Компьютеры	Описание	
бновить базы Аккорд-а, используя АРМ АБИ			
🖌 Обновить			
Имполтировать	4		Þ
	Выбрать все		Добавить

Рисунок 38 - Выбор импортированных компьютеров (импорт от ПКО)

После этого в правой части окна появятся импортированные компьютеры, следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 38).

Передача баз пользователей на ПКО в рамках централизованной схемы осуществляется посредством кнопки <Передача баз> (предварительно необходимо выбрать компьютеры (рисунок 26), на которые планируется передать базы). По нажатии этой кнопки на экране появляется окно передачи баз пользователей на ПКО (рисунок 39).

😑 Передать базы пользователей на ПКО 🛛 💈	3
Способ передачи баз:	
Используя АРМ АБИ	
💿 Экспортировать на диск	
	_
После передачи баз:	
Не перезагружать ПКО	
Перезагрузить ПКО	
🔘 Выключить ПКО	
ОК Отмена	

Рисунок 39 - Передача баз пользователей по централизованной схеме

Необходимо выбрать пункт «Используя АРМ АБИ» (рисунок 39) и нажать кнопку <OK>.

Если база пользователей передана на ПКО, на экране появляется сообщение (рисунок 40):

Компьютер	Результат экспорта	
📃 sistemnik	База передана на ПКО	

Рисунок 40 – Сообщение о том, что база пользователей передана на ПКО

Если во время выполнения процедуры передачи базы пользователей служба AcConNet загружена, на экране появляется сообщение (рисунок 41).

Компьютер	Результат экспорта	
📃 sistemnik	База поставлена в очередь передачи на ПКО	

Рисунок 41 – Сообщение о том, что база пользователей поставлена в очередь передачи на ПКО

По истечении некоторого времени база пользователей автоматически передается на ПКО и на экране появляется сообщение, показанное на рисунке 40.

Если во время выполнения процедуры передачи базы пользователей ПКО выключен, то на экране появляется сообщение (рисунок 42):

Компьютер	Результат экспорта	
📕 sistemnik	База создана и подготовлена для передачи на ПКО	
		-

Рисунок 42 – Сообщение о том, что база пользователей создана и подготовлена для передачи на ПКО

База пользователей автоматически передается при следующем включении ПКО, и на экране появляется сообщение, показанное на рисунке 40.

Передача баз пользователей на ПКО технологического участка в рамках децентрализованной схемы осуществляется посредством кнопки <Передача баз> (предварительно необходимо выбрать компьютеры (рисунок 26), на которые планируется передать базы). При этом производится копирование перечня учетных записей на внешний носитель, в качестве которого может использоваться USB флэш-накопитель или флоппи-диск. Если в качестве внешнего носителя используется USB флеш -накопитель, то перед тем, как выполнить процедуру передачи баз пользователей на ПКО в рамках децентрализованной схемы, необходимо добавить флеш -накопитель в единую базу USB-носителей (эта процедура выполняется Администратором СУЦУ в соответствии с документом «Руководство Администратора СУЦУ» 11443195.4012-053 90).

По нажатии кнопки <Передача баз> на экране появляется окно передачи баз пользователей на ПКО, в котором нужно выбрать пункт «Экспортировать на диск» (рисунок 43) и нажать кнопку <OK>.

😑 Передать базы пользователей на ПКО 🛛 Σ	3
Способ передачи баз:	
Используя АРМ АБИ	
Экспортировать на диск	
После передачи баз:	
💿 Не перезагружать ПКО	
🔘 Перезагрузить ПКО	
Выключить ПКО	
ОК Отмена	

Рисунок 43 - Передача баз пользователей по децентрализованной схеме

Далее на экране появляется окно выбора каталога, в котором нужно выбрать любой каталог на внешнем носителе и нажать кнопку <Применить>. Если процедура экспорта баз пользователей выполнена успешно, то на экране появляется сообщение (рисунок 44):

Компьютер	Результат экспорта	[
📕 sistemn <mark>i</mark> k	База экспортирована	
		i

Рисунок 44 – Сообщение о том, что база пользователей экспортирована на диск

Базы пользователей экспортируются в <выбраный_каталог>\Out\xxx\xxx.AMZ, где <выбранный_каталог> – каталог на внешнем носителе, xxx – имя ПКО, xxx.AMZ – файл, в котором находится список баз пользователей. Далее список на внешнем носителе должен быть доставлен на ПКО.

На ПКО соответствующего технологического участка необходимо выполнить следующие действия (чтобы функция импорта баз пользователей стала доступной, на ПКО в файле «AcWs32.ini» необходимо установить параметр NoNetManaged=Yes или в главном окне программы регистрации рабочей станции (ACSETWS.EXE) установить флаг «Станция не управляется по сети»):

- 1. в трее нужно выбрать правой кнопкой мыши сетевой клиент ПАК «Аккорд» (рисунок 45), на экране появляется меню (рисунок 46);
- 2. далее необходимо выбрать пункт «Импорт базы пользователей»;
- 3. на экране появляется сообщение «Предъявите идентификатор». Необходимо предъявить идентификатор Администратора «Аккорд» подконтрольного объекта.
- в появившемся на экране окне ввода пароля следует ввести пароль и нажать кнопку <OK> (рисунок 47);
- далее на экране появляется окно выбора каталога для импорта базы пользователей (рисунок 48), необходимо выбрать нужный каталог и нажать кнопку <OK>.

ПАК "Аккорд": Сетевой клиент V2.3.12 RU 🔇 💓 💭 🚾 😵 🔀 12:57

Рисунок 45 – Значок сетевого клиента ПАК «Аккорд» в трее



Рисунок 46 - Контекстное меню сетевого клиента ПАК «Аккорд» в трее

Ауте нтификац	ия 🔀
Введите пароль:	
1111111	
OK	Отмена [11]

Рисунок 47 – Окно ввода пароля

Выберите каталог с базой пользовате 🔀
Диски:
GSP1CULFRER (E:)
Каталоги:
123224 OUT SISTEMNIK UPGRADE VIRTUAL
Выбран каталог: Е:\
OK Cancel

Рисунок 48 - Выбор каталога для импорта базы пользователей

Если описанная процедура выполнена успешно, то на экране появляется следующее оповещение (рисунок 49).



Рисунок 49 - Оповещение об успешном выполнении процедуры импорта базы пользователей

При первом выполнении процедуры создания файлов базы пользователей на сервере централизованного управления создается каталог C:\Asm\OutBases\CompName (где «CompName» – имя ПКО). В нем хранятся файлы базы пользователей, которые создаются в ASM по нажатии кнопки <Передача баз>.

Далее при выполнении процедуры передачи баз пользователей на ПКО на сервере централизованного управления создается каталог C:\Asm\ACCONET\OUT\CompName (где «CompName» – имя ПКО), в котором хранятся копии файлов базы пользователей, эквивалентные переданным на ПКО.

Если файлы в каталоге C:\Asm\OutBases\CompName эквивалентны файлам в каталоге C:\Asm\ACCONET\OUT\CompName, то процедура передачи файлов базы пользователей на ПКО не производится. Если различия имеются, то файлы из каталога C:\Asm\OutBases\CompName переписываются в каталог C:\Asm\ACCONET\OUT\CompName и передаются на ПКО.

3.2.4 Вкладка «Учетные записи»

Для того чтобы работать с учетными записями, следует открыть в ASM вкладку Управление>Учетные записи (рисунок 50).

етные записи	Назначенные пользователи	Роли
🙎 AIB_TU	Иванов	АІВ_ТО: тех.участок_1
SUPERVISOR (sistemnik)	<не назначен>	ADMINS_1
Выбрать все		Число объектов:

Рисунок 50 - Учетные записи системы

Чтобы добавить новую учетную запись, необходимо нажать кнопку <Добавить>.

В появившемся окне (рисунок 51) следует ввести имя учетной записи, указать роль, назначить пользователя (сотрудника как физического лица)¹⁾, которому соответствует данная учетная запись, имя пользователя²⁾, ввести пароль и подтвердить его ввод, назначить пользователю идентификатор, полное имя пользователя³⁾ и выбрать компьютеры, на которых будет создана данная учетная запись. После ввода этих параметров необходимо нажать кнопку <Применить>.

При регистрации ПКО СУЦУСЗИ НСД создает «свою» учетную запись «ASM_ACCOUNT» в группе «Администраторы», с помощью которой становится возможным выполнение следующих операций: добавление, удаление пользователей, смена пароля пользователя и т.д. Данный механизм никак не связан с информацией, которая устанавливается в разделе «Результаты И/А» программы ACED32. Информация, установленная в разделе «Результаты И/А» определяет, какая информация о пользователе, полученная в результате процесса идентификации или аутентификации, передается из контроллера в программную подсистему разграничения доступа. Т.е. для успешного выполнения процедуры «Автологин» (процедуры, при которой пользователь авторизуется на аппаратном уровне, а программная часть автоматически подгружает его профиль доступа) необходимо включить первые пять флагов в разделе «Результатов И/А» (подробнее см. документ «Установка правил разграничения доступа. Программа ACED32» 11443195.4012-036 97).

	Описание учетной зап	писи
Имя учетной записи	Роль:	Назначить пользователю:
Петров_А	EVERYONE_1	 Пользователь_Петров
Имя пользователя:	Компьютеры:	
Petrov	✓ sistemnik	
Полное имя пользователя:		
Petrov_A		
Пароль:		
Подтверждение пароля:		
Идентификатор:		
[0C 000062300000 A7]	▼	
🖌 Применить		

Рисунок 51 - Добавление новой учетной записи

¹⁾ Действительные имя, фамилия и отчество соответствующего сотрудника (регистрируются Администратором СУЦУ во время выполнения процедуры добавления нового пользователя в соответствии с документом «Руководство Администратора СУЦУ» 11443195.4012-053 90).

²⁾ Логин в базе пользователей АМДЗ.

³⁾ Имя пользователя в домене

Чтобы отредактировать настройки учетной записи, следует выделить ее и нажать кнопку <Редактировать> на вкладке «Учетные записи» (рисунок 50), в появившемся окне (рисунок 52) изменить параметры учетной записи¹⁾. После завершения редактирования необходимо нажать кнопку <Применить>.

	Описание учетной	записи
1мя учетной записи	Роль:	Назначить пользователю:
Супервизор_системник	ADMINS_1	 Пользователь_Сидоров
1мя пользователя:	Компьютеры:	
supervisor	✓ sistemnik	
Іолное имя пользователя:		
supervisor_sistemnik_1		
ароль:		
одтверждение пароля:		
1дентификатор:		
[0C 0000622F0000 05]	·	
🖌 Применить		

Рисунок 52 - Редактирование параметров учетной записи

ВНИМАНИЕ! В ASM реализована функция централизованной смены паролей учетных записей пользователей ПКО. Для этого необходимо во вкладке Учетные записи\Редактировать изменить пароль учетной записи пользователя ПКО, затем выполнить процедуру передачи базы пользователей на ПКО (подробнее см.подраздел 3.1.3).

Администратор ИБ технологического участка может изменить свой пароль. Для этого необходимо во вкладке «Учетные записи» выбрать учетную запись Администратора ИБ технологического участка и нажать кнопку <Редактировать>. Затем в появившемся окне изменить пароль.

ВНИМАНИЕ! Если Администратор ИБ технологического участка изменил базы пользователей и не передал эти изменения на ПКО, то при выходе из ASM на экране появляется следующее оповещение (рисунок 53). При этом в статусбаре отображается счетчик ПКО, для которых осуществляется проверка изменений баз пользователей.

¹⁾ Во вкладке «Учетные записи>Редактировать» при выборе роли для редактируемой учетной записи отображаются только те компьютеры, которые принадлежат такому же технологическому участку, как и выбранная роль

мпьютеры системы	Назначенные пользователи	Тех участок Описание
sistemnik	wanov[SUPERVISOR], Petrov[USER1]	Тех.участок_1
	Accord Security Management V1.0.8.55	
	Yes No	
Выбрать все Об	новить	Число объектов: 1

Рисунок 53 – Оповещение о необходимости передачи обновленных баз пользователей на ПКО

По нажатии кнопки <Нет> на экране появляется окно для пересылки баз пользователей на ПКО (рисунок 39).

Чтобы удалить учетную запись, необходимо выделить ее и нажать кнопку <Удалить> на вкладке «Учетные записи» (рисунок 54). Появится окно подтверждения этого действия (рисунок 54), следует нажать кнопку <Да>, если действительно нужно удалить учетную запись.



Рисунок 54 - Окно подтверждения удаления учетной записи

Кнопка <Импорт> необходима для получения баз пользователей ПКО (подробнее ниже).

Если необходимо определить, какой учетной записи принадлежит данный идентификатор, следует нажать кнопку <Поиск> на вкладке «Учетные записи» (рисунок 50). Появится окно с сообщением «Предъявите идентификатор» (рисунок 55).

тные записи	Назначенные пользователи	Роли
AIB_TU	Иванов	АІВ_ТU: тех.участок_1
SUPERVISOR (sistemnik)	Сидоров	ADMINS_1
Выбрать все		Uncaro of the end of the

Рисунок 55 - Окно с сообщением «Предъявите идентификатор»

Если данный идентификатор назначен какой-либо учетной записи, то эта учетная запись будет выделена (рисунок 56), иначе в нижней части окна появится сообщение «Идентификатор не зарегистрирован!» (рисунок 57).

етные записи	Назначенные пользователи	Роли
AIB_TU	Иванов	AIB_TU: тех.участок_1
SUPERVISOR (sistemnik)	Сидоров	ADMINS_1
Выбрать все		livera efa error:
		HIGHO DOBERTOD.

Рисунок 56 - Учетная запись, которой назначен идентификатор

тные записи	Назначенные пользователи	Роли
AIB_TU	Иванов	АІВ_ТU: тех.участок_1
SUPERVISOR (sistemnik)	Сидоров	ADMINS_1
Выбрать все		Число объектов:

Рисунок 57 - Сообщение о том, что идентификатор не зарегистрирован

Для получения данных об учетных записях пользователей в рамках централизованной схемы необходимо во вкладке «Учетные записи» нажать кнопку <Импорт> (рисунок 50). Далее в появившемся окне (рисунок 62) нужно выбрать флаг «Вы можете импортировать учетные записи из:» - «базы пользователей NT».

После этого следует ввести IP-адрес или имя сервера, из базы пользователей которого будут импортированы учетные записи, а также имя и пароль Администратора данного сервера (рисунок 58).

		Управление > Учетные записи системы > Импорт
Вы может	е импортировать учетные записи из:	
🔘 базы /	Accord	
💿 базы і	пользователей NT	
	Выберите компьютер:	
Сервер:	192.168.33.135	
Имя:	Administrator	
Пароль:	•••••	
	ипортировать	
	🗲 Назад	

Рисунок 58 - Ввод данных о сервере, из базы пользователей которого будут импортированы учетные записи

После этого в правой части окна появятся импортированные учетные записи, следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 59).

	4d		rinnoproposarinato y termino aumon.	
оазы	Accord	Импортированные учетные	е записи, выберите необходимые для добавлени	я в базу:
базы	пользователей NT	Учетные записи	Описание	
	Выберите компьютер:	CTX_STREAMIN	Компьютер: Accord, ID = 00 000000000	00 00
		SUPERVISOR	Компьютер: Accord, ID = 00 000000000	00 00
DBeD.	192.168.33.135	USER USER	Компьютер: Accord, ID = 00 000000000	00 00
	I	USER_A	Компьютер: Accord, ID = 00 000000000	00 00
	Administrator	USER_A1	Компьютер: Accord, ID = 00 000000000	00 00
n.a.		USER_ICA	Компьютер: Accord, ID = 00 000000000	00 00
роль:	•••••	USER_L	Компьютер: Accord, ID = 00 000000000	00 00
		USER_L2	Компьютер: Accord, ID = 00 000000000	00 00
		USER_RDP	Компьютер: Accord, ID = 00 000000000	00 00
И	ипортировать			
-		Выбрать все		Лобавить
		baroparb bee		доодынь

Рисунок 59 - Выбор импортированных учетных записей (импорт из базы пользователей NT)

Для получения данных об учетных записях пользователей ПКО технологического участка в рамках децентрализованной схемы используется функция экспорта списка пользователей СЗИ от НСД ПКО (чтобы функция экспорта стала доступной, на ПКО в файле «AcWs32.ini» необходимо установить параметр NoNetManaged=Yes или в главном окне программы регистрации рабочей станции (ACSETWS.EXE) установить флаг «Станция не управляется по сети»). При этом производится копирование перечня учетных записей на внешний носитель, в качестве которого может использоваться USB флэш-накопитель или флоппи-диск. Если в качестве внешнего носителя используется USB флеш -накопитель, то перед тем, как выполнить процедуру получения баз пользователей ПКО в рамках децентрализованной схемы, необходимо добавить флеш -накопитель в единую базу USB-носителей (эта процедура выполняется Администратором СУЦУ в соответствии с документом «Руководство Администратора СУЦУ» 11443195.4012-053 90).

Чтобы передать базы пользователей, необходимо на ПКО в трее выбрать правой кнопкой мыши сетевой клиент ПАК «Аккорд» (рисунок 45). После этого на экране появляется контекстное меню (рисунок 46).

Далее необходимо выбрать команду «Экспорт базы пользователей» (рисунок 46).

После этого на экране появляется сообщение «Предъявите идентификатор». Необходимо установить идентификатор Администратора ИБ в свободный USB-разъем компьютера.

После этого на экране появится окно ввода пароля. Следует ввести пароль и нажать кнопку <OK> (рисунок 47):

После выполнения операции ввода пароля на экране появляется окно выбора каталога для сохранения базы пользователей (рисунок 60), необходимо выбрать нужный каталог и нажать кнопку <OK>.

Выберите каталог для экспорта базы 🔀
Диски:
GSP1CULFRER (E:)
Каталоги:
123224 OUT SISTEMNIK UPGRADE VIRTUAL
Выбран каталог: Е:\
OK Cancel

Рисунок 60 – Выбор каталога для сохранения базы пользователей

Если описанная процедура выполнена успешно, то на экране появляется следующее оповещение (рисунок 61):



Рисунок 61 - Оповещение об успешном выполнении процедуры экспорта базы пользователей

Далее базы пользователей на внешнем носителе должны быть доставлены на сервер централизованного управления.

Во вкладке «Учетные записи» ПО ASM на сервере централизованного управления необходимо нажать кнопку <Импорт> (рисунок 50). В появившемся окне (рисунок 62) необходимо выбрать флаг «Вы можете импортировать учетные записи из:» - «базы Accord» (предварительно следует обновить базы, нажав кнопку <Обновить>) и нажать кнопку <Импортировать> (учетные записи при этом импортируются из каталога, <выбранный_каталог>\IN\xxx\ xxx.AMZ, где <выбранный_каталог> – каталог на внешнем носителе, xxx – имя ПКО, xxx.AMZ – файл, в котором находится список баз пользователей).

Управление > Учетные записи системы > Импорт
и можете импортировать учетные записи из:
0 Gasa Accord
6asu non-sonateneŭ NT
Обновить базы Аккорд-а, используя АРМ АБИ
✓ Обновить
A MURDATURDETE
К Назад

Рисунок 62 - Импорт учетных записей из базы «Аккорда»

В появившемся на экране окне (рисунок 63) следует указать файл с именем ПКО, с которого необходимо импортировать учетные записи.

Открыть файл	23
Папка: 퉲 М 🔹 🏈	🤌 📂 🎞 🗸
comp1.amz	
Mun daŭna:	1 [
compl.amz	Открыть
Тип файла: Accord files (*.amz)	Отмена

Рисунок 63 - Выбор файла *.amz, из которого необходимо импортировать учетные записи

После этого в правой части окна появятся импортированные учетные записи; следует выбрать из них необходимые для добавления в базу (для выбора всех учетных записей нужно нажать кнопку <Выбрать все>) и нажать кнопку <Добавить> (рисунок 64).

		импортированные учетные записи:
базы Accord	Импортированные учетные	е записи, выберите необходимые для добавления в базу:
базы пользователей NT	Учетные записи	Описание
новить базы Аккорд-а, используя АРМ АБИ	CTX STREAMIN	Компьютер: Accord, ID = 00 0000000000 00
порять одова у каторда, испольбу у у ката у сут	SUPERVISOR	Компьютер: Accord, ID = 00 0000000000 00
	USER	Компьютер: Accord, ID = 00 0000000000 00
	USER_A	Компьютер: Accord, ID = 00 0000000000 00
Обновить	USER_A1	Компьютер: Accord, ID = 00 0000000000 00
	USER_ICA	Компьютер: Accord, ID = 00 0000000000 00
	USER_L	Компьютер: Accord, ID = 00 0000000000 00
	USER_L2	Компьютер: Accord, ID = 00 0000000000 00
	USER_RDP	Компьютер: Accord, ID = 00 0000000000 00
1 Muser Tupoparti	4	III
импортировать	Выбрать все	Добавить

Рисунок 64 - Выбор импортированных учетных записей (импорт из базы «Аккорда»)

При первом выполнении процедуры получения базы пользователей ПКО на сервере централизованного управления создается каталог С:\Asm\ACCONET\IN\CompName (где «CompName» – имя ПКО), в котором хранят-ся файлы базы пользователей ПКО. Сервер централизованного управления при-

нимает файлы базы пользователей ПКО (состоящие из файлов CompName.amz, CompName.ini, CompName.ver, *.act) только при наличии изменений в базе пользователей ПКО: если различие между файлами, хранящимися на ПКО, и файлами в каталоге C:\Asm\ACCONET\IN\CompName отсутствует, то файлы не принимаются.

3.2.5 Создание пользователя технологического участка

До выполнения процедуры создания пользователя технологического участка предварительно должны быть выполнены следующие действия:

- создание пользователя (выполняется Администратором СУЦУ в соответствии с документом «Руководство Администратора» 11443195.4012-053 90, подраздел 3.2.1.1);
- создание технологического участка (выполняется Администратором ИБ в соответствии с документом «Руководство Администратора ИБ» 11443195.4012-053 91, подраздел 4.1.2);
- создание Администратора ИБ технологического участка (выполняется Администратором ИБ в соответствии с документом «Руководство Администратора ИБ» 11443195.4012-053 91, подраздел 4.1.5).

Администратор ИБ технологического участка должен:

- добавить идентификатор для пользователя технологического участка (подраздел 3.2.2);
- добавить компьютер для пользователя технологического участка (подраздел 3.2.3);
- создать учетную запись пользователя технологического участка (3.2.4), указав имя пользователя и назначив ему роль, компьютер и идентификатор.

Чтобы создать пользователя технологического участка, необходимо:

- на подконтрольном объекте создать пользователя «Гл.Администратор» и других пользователей (выполняет Администратор ИБ ПКО);
- на сервере централизованного управления создать пользователей (выполняет Администратор СУЦУ в соответствии с п. 4.1.1 документа «Руководство Администратора» 11443195.4012-053 90);
- создать технологический участок (выполняет Администратор ИБ в соответствии с документом «Руководство Администратора ИБ» 11443195.4012-053 91, подраздел п. 3.1.4);
- во вкладке «Учетные записи» импортировать учетные записи пользователей ПКО посредством кнопки <Импорт> (выполняет Администратор ИБ технологического участка в соответствии с п 3.2.4 настоящего документа);
- выполнить операцию редактирования учетных записей пользователей ПКО, в рамках которой необходимо сопоставить созданного Администратором СУЦУ пользователя редактируемой учетной записи (выполняет Администратор ИБ технологического участка в соответствии с п 3.2.4 настоящего документа);

- сохранить изменения (выполняет Администратор ИБ технологического участка в соответствии с п 3.2.4 настоящего документа);
- передать базу пользователей на ПКО (выполняет Администратор ИБ технологического участка в соответствии с п 3.2.4 настоящего документа).

3.3 Работа с журналами

Открыв вкладку «Журналы», Администратор ИБ ТУ СУЦУ может работать с тремя типами журналов.

Первый тип – Журналы «Аккорд», в которых содержатся сведения о работе пользователей на рабочих местах (рисунок 65). (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).

Станция	Время	Пользователь	Команда	Результат	Объект
OK sistemnik	15.01.2014 14:28:36	SUPERVISOR	MSZI	OK	Login
4					•

Рисунок 65 - 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 66).

Выберите комьютеры для обновления информации	23
Компьютеры	
🗹 💻 sistemnik	
	_
	_
	-
Убрать все ОК Отмена	

Рисунок 66 – Выбор ПКО, с которых планируется получить журналы¹⁾

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

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>.

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») в окне, показанном на рисунке 65. 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)), появится 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».

Кнопка <Импорт> необходима для получения журналов с ПКО по децентрализованной схеме (см. ниже).

По нажатии кнопки <Фильтр журнала> на экране появляется окно смены фильтров оперативного журнала (рисунок 67).

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

	Ha	стройка филь	тров оперативного журнал	8
айловые операции:			Операции с реестром:	
Результат выполнения	📃 Прекращение работы программы	-	Результат выполнения	Открыть ключ реестра
Все состояния	🔲 Установить дату	=	Все состояния	🔲 Закрыть ключ реестра
	Установить время			Создать ключ реестра
🕥 нсд	Создать каталог		🔘 нсд	🔲 Удалить ключ реестра
	🔲 Удалить каталог			Перечисление ключей реестра
🔘 Ошибка	📃 Изменить текущий каталог	-	Ошибка	🔲 Установить значение параметра ключа
	Выд	елить все		Выделить все
ообщения СЗИ:	Расчет КЦ:		Хранитель экрана:	
Результат выполнения	Результат выполнения		Результат выполнения	ScreenSaver включен по времени
Все состояния	Все состояния		Все состояния	ScreenSaver включен используя горячие клавиши
				ScreenSaver включен с АРМ АБИ
🖲 нсд	🖲 нсд		🖲 нсд	ScreenSaver выключен с помощью TM
				Выделить все

Рисунок 67 – 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 67). События хранятся в каталоге ASM\AccountName_FilterParam.ini, где параметр «AccountName» – это имя учетной записи.

Второй тип – журналы ASM, касающиеся работы утилиты ASM (рисунок 68). 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).

Время	Результат	Событие	4
15.01.2014 12:13:11	OK	DEPOSERVER ошибка получения журналов [ErrCode = 2, станция не активна]	
15.01.2014 12:13:11	OK	sistemnik ошибка получения журналов [ErrCode = 2, станция не активна]	
15.01.2014 12:13:11	OK	DEPOSERVER ошибка получения журналов [ErrCode = 2, станция не активна]	
15.01.2014 12:13:11	OK	sistemnik ошибка получения журналов [ErrCode = 2, станция не активна]	
15.01.2014 12:21:16	OK	Учетные записи успешно добавлены в базу	
15.01.2014 12:21:22	OK	Учетная запись sdsdsd удалена	
15.01.2014 12:22:03	Error	Передача базы на sistemnik. Учетная запись SUPERVISOR не назначена на пользователя	
15.01.2014 12:23:07	OK	Пользователь Иванов добавлен	
15.01.2014 12:23:58	OK	Учетная запись USER1 изменена	
15.01.2014 12:24:09	Error	Передача базы на sistemnik. Учетная запись SUPERVISOR не назначена на пользователя	
15.01.2014 12:24:46	OK	Пользователь Сидоров добавлен	
15.01.2014 12:26:26	OK	Идентификатор ОС 00002E320000 2А успешно добавлен в базу	
15.01.2014 12:26:43	OK	Учетная запись SUPERVISOR изменена	
15.01.2014 12:26:52	OK	Передача базы на sistemnik. База поставлена в очередь передачи на ПКО	
15.01.2014 14:26:45	OK	Пользователь Логинов добавлен	
10 01 0014 14-00-00	or	Поли сополного Тихонопо соболлон	

Рисунок 68 - Журнал ASM

Третий тип журналов - журнал АРМ АБИ, касающийся работы утилиты АсСоппеt (рисунок 69). Он необходим для просмотра сетевых сообщений.

Станция	Время	Событие	Результат	Примечание	
IK sistemnik	8/4/2014 3:57:00 PM	Получение базы пользователей	OK		
OK sistemnik	8/4/2014 3:54:52 PM	Получение базы пользователей	OK		

Рисунок 69 - Журнал АРМ АБИ

Журнал АРМ АБИ можно сохранить в текстовый файл с разделителем «|». Для этого необходимо нажать кнопку <Сохранить> (рисунок 69). По нажатии кнопки на экране появляется окно, в котором нужно ввести название файла и нажать кнопку <Сохранить> (рисунок 70).

Сохранить журнал	X
Папка: 🕕 Asm	- 🕒 🧐 🕑 -
ACCONNET	
Ju OutBases	
EMPLA	
ТМ	
TSIEM	
asm	
Имя файла:	Сохранить
Тип файла: Log files	▼ Отмена

Рисунок 70 – Сохранение журнала АРМ АБИ в текстовый файл

Для получения журналов ПКО в рамках децентрализованной схемы используется функция экспорта журналов СЗИ от НСД ПКО. При этом производится копирование перечня журналов на внешний носитель, в качестве которого может использоваться USB флэш-накопитель или флоппи-диск (журналы экспортируются в каталог <выбранный_каталог>:\IN\xxxx\, где <выбранный_каталог> – каталог на внешнем носителе, xxx - имя станции.). Далее перечень на внешнем носителе должен быть доставлен на сервер централизованного управления.

Для передачи журналов с ПКО на сервер централизованного управления необходимо на ПКО в трее выбрать правой кнопкой мыши значок сетевого клиента ПАК «Аккорд» (рисунок 71), на экране появляется меню (рисунок 72):

A STATISTICS	
ПАК "Ак	корд": Сетевой клиент V2.3.12
RU	🔇 😲 🛃 🚾 🐯 🚰 12:57 -

Рисунок 71 – Значок сетевого клиента ПАК «Аккорд» в трее

Экспорт журналов
Экспорт базы пользователей
Импорт базы пользователей
- RU < 👽 👺 🔤 😻 🕎 12:56

Рисунок 72 – Контекстное меню значка сетевого клиента ПАК «Аккорд» в трее

Далее в контекстном меню необходимо выбрать команду «Экспорт журналов» (рисунок 72).

Во время выполнения процедуры экспорта журнала в рамках децентрализованной схемы текущий журнал автоматически закрывается, и создается новый файл журнала, в котором отражен факт закрытия предыдущего журнала Администратором ИБ (АИБ подразделения)¹⁾. Имеется возможность автоматического закрытия журнала по достижении 23 часов и 0 минут.

После этого на экране появляется сообщение «Предъявите идентификатор». Необходимо подключить персональный идентификатор Администратора информационной безопасности (АИБ подразделения).. Далее на экране появляется окно ввода пароля. Следует ввести пароль и нажать кнопку <OK> (рисунок 73):

Ауте нтификаци	ия 🚺
Введите пароль:	
1111111	
OK	Отмена [11]

Рисунок 73 – Окно ввода пароля

После выполнения операции ввода пароля на экране появляется окно выбора каталога для сохранения журналов (рисунок 74). Журналы экспортируются в каталог E:\IN\xxx\, где E – внешний носитель. xxx - имя ПКО. Необходимо нажать кнопку <OK>.

¹⁾ Актуально для ПАК «Аккорд-Win32» v.4.0.7.33 и ПАК «Аккорд-Win64» v.5.0.6.30

Выберите каталог для экспорта журн 🔀
Диски:
GSP1CULFRER (E:)
Каталоги:
123224 CLIENT.LOG OUT SISTEMNIK UPGRADE VIRTUAL
Выбран каталог: Е:\
OK Cancel

Рисунок 74 – Окно выбора каталога для сохранения журналов

Если описанная процедура выполнена успешно, то на экране появится следующее оповещение (рисунок 75):



Рисунок 75 – Оповещение об успешном выполнении процедуры экспорта журналов

Далее производится копирование перечня журналов на внешний носитель, в качестве которого может использоваться USB флэш-накопитель или флоппидиск (журналы экспортируются в каталог <выбранный_каталог>:\IN\xxxx\, где <выбранный_каталог> – каталог на внешнем носителе, xxx - имя станции.). Затем перечень на внешнем носителе должен быть доставлен на сервре централизованного управления. Если в качестве внешнего носителя используется USB флеш накопитель, то перед тем, как выполнить процедуру получения журналов СЗИ от НСД ПКО в рамках децентрализованной схемы, необходимо добавить флеш накопитель в единую базу USB-носителей (эта процедура выполняется Администратором СУЦУ в соответствии с документом «Руководство Администратора СУЦУ» 11443195.4012-053 90).

На АРМ управляющего персонала Администратор ИБ должен выполнить следующие действия:

- копировать каталог с журналами на АРМ управляющего персонала;
- во вкладке «Журналы» нажать кнопку <Импорт> (рисунок 65);

• далее в появившемся окне выбрать необходимый каталог и нажать кнопку <Применить>.

4 Сообщения программных средств комплекса и порядок действий по ним

При работе на CBT, оснащенном 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)	TM-идентификатор был неправильно прислонен к съемнику информации.	Снова приложить ТМ- идентификатор к съемнику информации после появле- ния соответствующего за- проса.		
«Это не сетевой ТМ»	Прислонен неверный ТМ- идентификатор	Прислонить правильный ТМ- идентификатор		
«В данное время вход в систему запрещен»	Для данного пользователя не разре- шен вход в систему в данное время	Вызвать Администратора ИБ и уточнить разрешенное время работы		
«Ваш пароль просрочен. Обратитесь к Администра- тору для смены» (на крас- ном фоне)	Окончилось время жизни пароля. Закончились все попытки смены па- роля.	Вызвать Администратора ИБ. Изменить параметры паро- ля.		
«Доступ не разрешен!» (на красном фоне)	Не зарегистрированный идентифика- тор. Не правильно введен пароль. В данное время работают временные ограничения.	Обратиться к Администрато- ру ИБ для регистрации. По- вторить процедуры иденти- фикации / аутентификации.		
«Требуется Администра- тор» (на красном фоне) «Разберитесь с ошибками» (на оранжевом фоне)	Несовпадение контрольных и текущих параметров аппаратной и программ- ной частей системы.	Вызвать Администратора ИБ. Выявить и устранить причи- ны изменения параметров.		
«Такую комбинацию сим- волов недопустимо исполь- зовать в качестве пароля»	Это сообщение появляется в случае, если пользователь вводит комбина- цию символов, которую легко подоб- рать (например, qwerty).	Ввести более сложную ком- бинацию 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 па- роля.		
В идентификаторе нет сво- бодных страниц для запи- си»	Объем идентификатора DS1996 по- зволяет 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 неза- регистрированные станции, то следует добавить список на АРМ АБИ и после очистки памяти ТМ провести регист- рацию остальных рабочих станций.		

5 Сообщения программных средств подконтрольных объектов

Сообщения на экране	Описание сообщений			
События работы с реестром				
RegOpenKey	Открыть ключ реестра			
RegCloseKey	Закрыть ключ реестра			
RegCreateKey	Создать ключ реестра			
RegDeleteKey	Удалить ключ реестра			
RegEnumKey	Перечисление ключей реестра			
RegSetValue	Установить значение параметра ключа			
RegQueryValue	Прочитать значение параметра ключа			
RegDeleteValue	Удалить параметр ключа			
RegCreateValue	Создать параметр ключа			
RegEnumValue	Перечисление параметров ключа			
События работы с	СО СКрин-сейвером			
SSOnTime	ScreenSaver включен по времени			
SSOnKey	ScreenSaver включен используя горячие клавиши			
SSOnRemote	ScreenSaver включен внешней программой			
SSOffTM	ScreenSaver выключен с помощью ТМ			
SSOffRemote	ScreenSaver выключен с АРМ АБИ			
SOffTMRemote	ScreenSaver выключен с помощью ТМ АБИ			
SSTimeOff	Выключен временной контроль ScreenSaver-a			
SSTimeOn	Включен временной контроль ScreenSaver-a			
SSBadTM	Попытка разблокировать чужим ТМ			
События конт	оля объектов			
StartCheck	Начало проверки списка объектов			
EndCheck	Завершение проверки списка объектов			
StartUpdate	Начало обновления списка объектов			
EndUpdate	Завершение обновления списка объектов			
TotalHash	Хэш списка объектов			
TotalEDS	Подпись списка объектов			
GetPrivateKey	Получение секретного ключа			
FileCheck	Проверка объекта			
События -	гипа «PM»			
Term00	Прекращение работы программы			
SetDate	Установить дату			
SetTime	Установить время			
MkDir	Создать каталог			
RmDir	Удалить каталог			
ChDir	Изменить текущий каталог			
RenameDir	Переименовать каталог			
CreateFile	Создать файл			
OpenFileR	Открыть файл на чтение			
OpenFileW	Открыть файл на запись			
OpenFileRW	Открыть файл на чтение/запись			
CloseFile	Закрыть файл			
DeleteFile	Удалить файл			
ChMod	Установить атрибуты файла			
Exec	Запуск программы			
Exit	Выход из программы			
FindFirst	Найти первый файл			
FindNext	Найти следующий файл			
RenameFile	Переименовать файл			
Traverse	Проверка существования пути			

6 Перечень принятых сокращений

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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

	Номера листов (страниц)				Вхоляций				
Из м.	И3- Ме- Нен- НЫХ	заме- нен- ных	новых	Аннули- рованных	Всего лис- тов (стр.) в документе	№ докумен- та	Входящий № сопрово- дительного документа	Под- пись	Дата
					· · · · · · · · · · · · · · · · · · ·				
					· · · · · · · · · · · · · · · · · · ·				
			İ						
					1				
					1				
					1				
					1				
					1				
					1				
					1				
					1				
					1				
					1				
			l						
		,							

СОГЛАСОВАНО

Наименование	Должность	Фамилия, имя,	Подпись	Дата
организации.	исполнителя	отчество		
прелприятия				
продприлил				