ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО

систем автоматизированного проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
11443195.5014-011 90 01-ЛУ

Программно-аппаратные комплексы средств защиты информации от несанкционированного доступа **"АККОРД "**

Подсистема распределенного аудита и управления «Аккорд-РАУ»

Руководство администратора

11443195.5014-011 90 01

Листов ____

Литера 0_1

АННОТАЦИЯ.

Настоящий документ является руководством по управлению механизмами защиты подсистемы распределенного аудита и управления (ПРАУ) и предназначен для конкретизации задач и функций администратора безопасности информации (АБИ).

Для лучшего понимания и использования защитных механизмов ПРАУ рекомендуется предварительно ознакомиться с пакетом эксплуатационной документации на комплекс.

Применение защитных мер ПРАУ должно дополняться общими мерами предосторожности и физической безопасности ПЭВМ (АС).

Содержание

Введение

Автоматизированное рабочее место администратора безопасности информации (АРМ АБИ) на базе контроллера "Аккорд-АМДЗ", далее по тексту - комплекс "Аккорд", предназначен для оперативного наблюдения за работой пользователей, оперативного управления работой пользователей, централизованного сбора журналов регистрации работы комплекса "Аккорд", управления составом рабочих станций и серверов.

1 Содержание работы администратора безопасности информации

1.1 Планирование применения комплекса "Аккорд"

Планирование применения СЗИ "Аккорд" осуществляется на этапе общего планирования защиты. Содержание этого этапа заключается в составлении плана защиты. Обычно план защиты - это документ, в который входят данные о характере и составе обрабатываемой локальной сети информации, составе технических и программных средств, возможных угрозах системе и способах их возможной реализации, и соответственно описание выбранных методов и средств защиты от этих угроз.

Для настройки средств защиты комплекса "Аккорд" рекомендуется выявить и отразить в плане защиты следующие характеристики защищаемой системы:

- перечень задач, решаемых сотрудниками организации с использованием автоматизированной системы;
- полный перечень используемых при решении каждой конкретной задачи программ;
- полный перечень используемых при решении каждой задачи данных;
- подробный перечень имеющихся в защищаемой локальной сети технических средств (рабочих станций, серверов и т.д.) с указанием их состава, конфигурации и характеристик.
- перечень размещенных на каждой рабочей станции и сервере системных и прикладных программ, файлов и баз данных.
- перечень установленных на рабочих станциях и серверах программно-аппаратных средств защиты;
- списки пользователей системы с указанием решаемых ими задач из общего перечня задач и предоставляемых им полномочий по доступу к рабочим станциям и серверам сети.

Для более эффективного применения комплекса "Аккорд" и поддержания уровня защищенности необходимы:

- физическая охрана всех компонентов автоматизированной системы обработки информации, в т.ч. обеспечение мер по не извлечению контроллера комплекса;
- использование в автоматизированной системе технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в системе Государственной системы безопасности информации (ГСЗИ);
- периодическое тестирование средств защиты комплекса;
- разработка и ведение учетной и объектовой документации (инструкция администратора, инструкций пользователей, журнал учета идентификаторов и отчуждаемых носителей пользователей и др.). Все разработанные учетные и объектовые документы должны быть согласованы, утверждены у руководства и доведены до сотрудников (пользователей). Это необходимо для того, чтобы План защиты организации (предприятия, фирмы и т.д.) и действия АБИ (администратора БИ) получили юридическую основу.

1.2 Установка и настройка комплекса "Аккорд"

Администратор БИ организует установку комплекса и осуществляет контроль за качеством ее выполнения. Порядок установки и настройки комплекса содержится в "Руководстве по установке комплекса" (**11443195.5014-011 98 01**).

Для установки программного обеспечения необходимо наличие установочной дискеты и идентификатора TouchMemory типа DS1996. На рабочих станциях должен быть установлен комплекс "АККОРД-АМДЗ" с ПО разграничения доступа версии 1.35, 1.95 или NT/2000, на АРМ администратора должен быть установлен комплекс "АККОРД-АМДЗ" и загружен соответствующий драйвер (ПО разграничения доступа может быть установлено, но не является обязательным), а на сервере - комплекс «АККОРД-АМДЗ». Система функционирует в сетях Novell Netware V3.1X, V4.X (протоколы TCP/IP и IPX), V5.X(протокол IPX) и сетях Windows (протокол TCP/IP).

В процессе установки и настройки создается файла acnode.lst, в котором содержится список станций с параметрами:

- имя станции,
- номера сетевых карт с номерами сетей (ipx),
- открытый ключ станции.

В качестве средства транспортировки информации о станциях используется ТМ-идентификатор DS1996 (далее сетевой ТМ).

Установка осуществляется в несколько этапов:

- форматирование носителя информации (ТМ DS1996, или USB устройства ШИПКА), регистрация в носителе данных об АРМ АБИ;
- сбор данных о защищенных станциях и серверах ЛВС и регистрация этих данных на АРМ администратора безопасности информации;
- передача собранной информации с АРМ АБИ на все станции и сервера.

1.3 Эксплуатация комплекса

При эксплуатации комплекса администратор БИ решает следующие задачи:

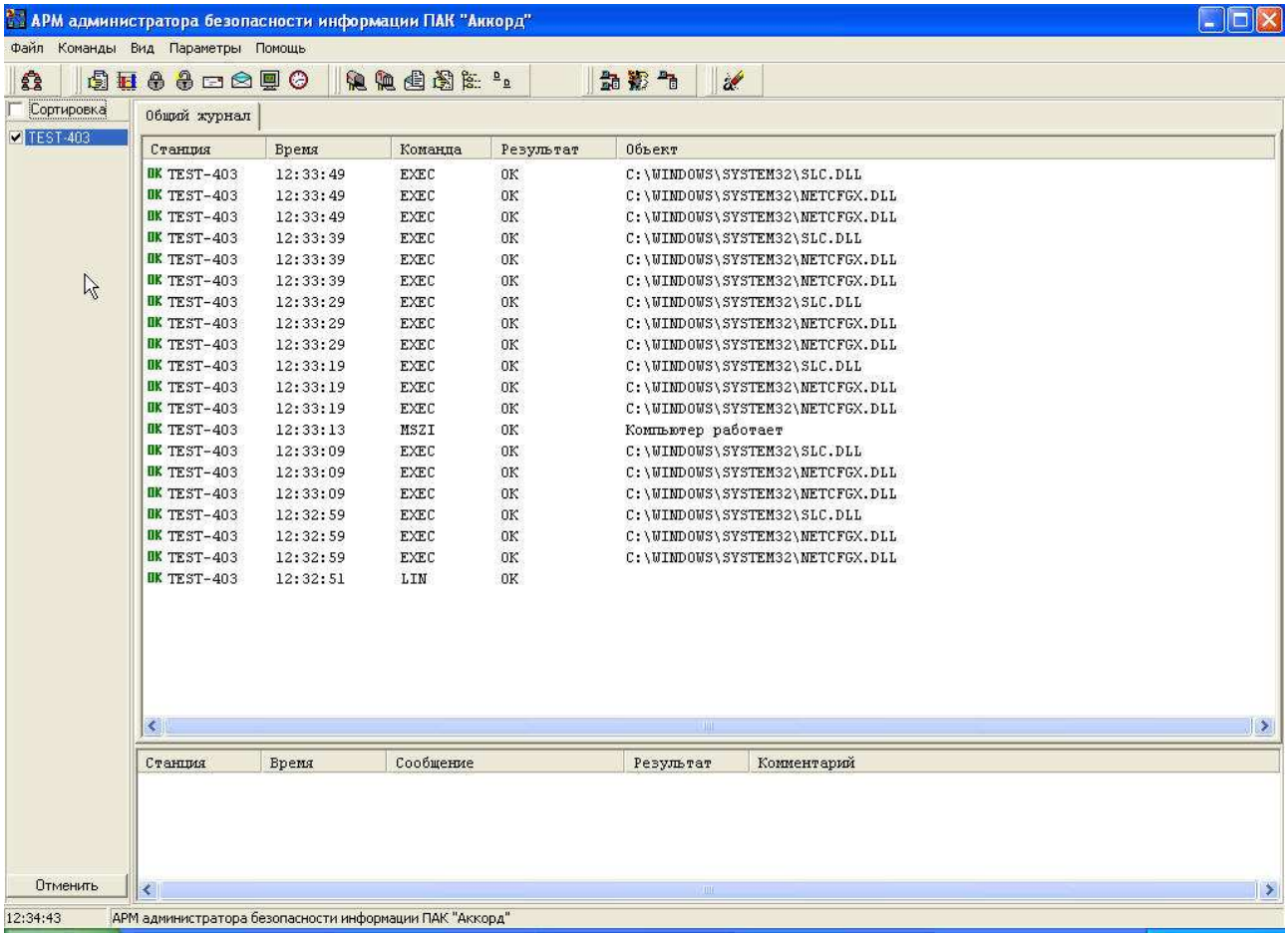
- поддерживает средства защиты в работоспособном состоянии и периодически контролирует корректность их работы;
- проводит изменения настроек средств защиты в соответствии с корректировками плана защиты, вызванными изменением состава пользователей, перечня решаемых задач и соответствующими изменениями функциональных обязанностей сотрудников;
- проводит оперативное наблюдение за работой пользователей;
- обеспечивает оперативное управление работой пользователей;
- осуществляет централизованный сбор и своевременный анализ журналов регистрации работы СЗИ "Аккорд";
- обеспечивает управление составом пользователей на рабочих станциях;
- обеспечивает управление составом рабочих станций и серверов.

Внимание !

Доступ к журналам и списку пользователей в контроллере АМДЗ имеет только администратор. Для выполнения операций получения журналов и редактирования пользователей идентификатор администратора, который предъявляется при запуске АРМ АБИ, должен быть зарегистрирован в контроллерах «Аккорд-АМДЗ» в группе «Администраторы» на всех рабочих станциях.

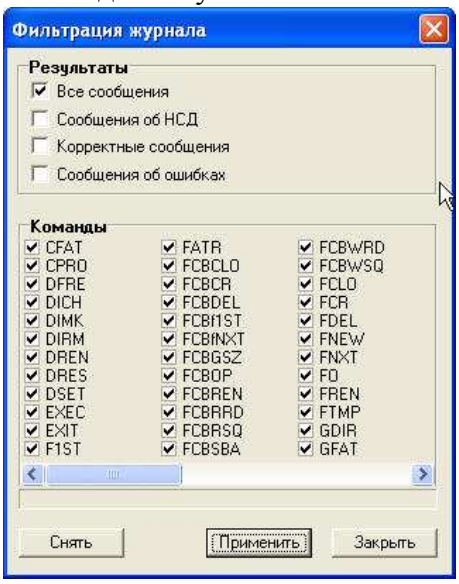
2 Эксплуатация автоматизированного рабочего места администратора безопасности информации (АРМ АБИ)

2.1. Общий вид АРМ администратора безопасности



Слева – список рабочих станций. Справа два окна: верхнее – общее окно журнала событий, происходящих на станциях; нижнее – окно сообщений от станций.

В окне «Общий журнал» можно установить фильтры для отбора поступающих сообщений. При нажатии правой кнопки мыши всплывает меню с пунктом «Фильтрация журнала». После выбора команды на экран выводится форма, позволяющая сделать необходимые установки.



Результаты: в журнал будут выводиться только сообщения с установленным результатом.

Команды: выбор команд (функций ОС). Сообщения о выполнении только выбранных команд будут выводиться на экран.

2.2. Общий вид панели управления

2.3. Меню команд

(1) Файл

Выход - завершение работы с программой**.**

(2) Команды

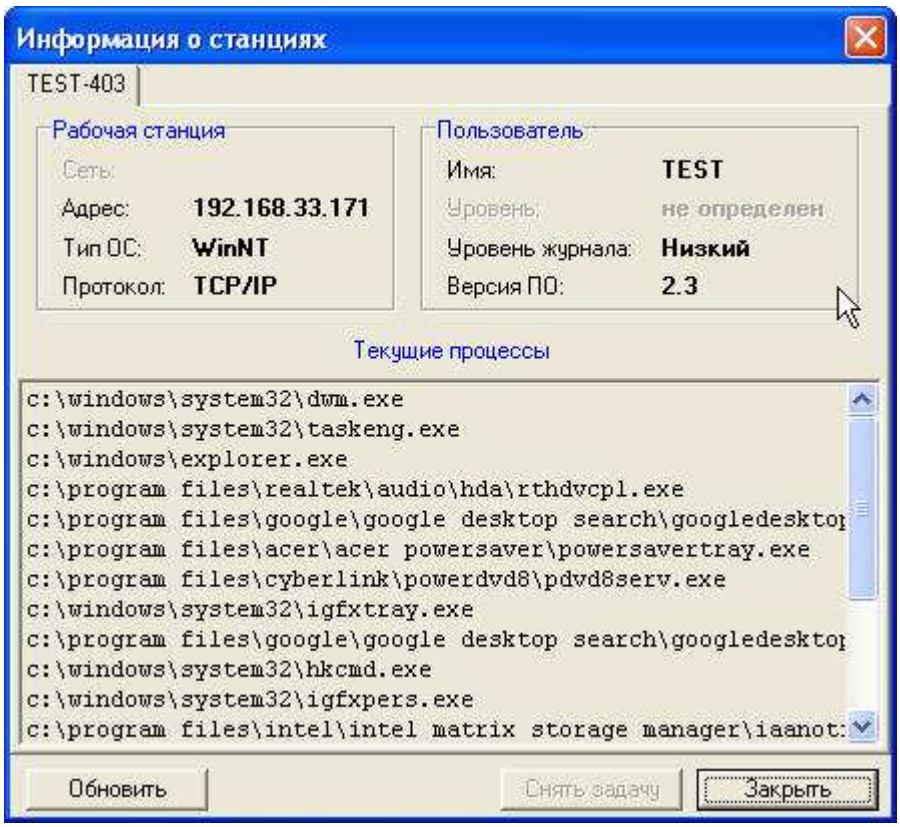
Команды, которые могут быть выполнены в процессе работы администратора безопасности информации на АРМ. Соответствуют кнопкам на панели управления.

Поиск клиентов в сети 

С помощью этой команды можно проверить сеть на наличие подключенных станций и найти новые.

Получить информацию о станциях 

Окно «Информация о станциях» имеет следующий вид:



Информация о рабочей станции:

Сеть - MAC адрес сетевой карты;
Адрес - адрес станции в сети (IP или NIC);
Тип ОС - тип операционной системы (Dos, Win95, WinNT);
Протокол - сетевой протокол (IPX или TCP/IP);

Информация о пользователе:

Имя - имя пользователя, работающего на выбранной станции или сообщение "No_Acrun !";

Уровень
Уровень журнала - уровень журнала, установленный у пользователя;
Версия ПО - версия ПО, установленного у пользователя.

Текущие процессы.

Список текущих задач и процессов на рабочей станции.

Обновить - обновить список Текущих процессов.
Снять задачу - завершить выполнение выбранной задачи на рабочей станции.
Закрыть - закрыть окно.

Установить уровень детальности журнала 

Отключить - не вести журнал событий;
Высокий - выводить все события, происходящие на станциях;
Средний - выводить основные события, происходящие на станциях;
Низкий - выводить главные события, происходящие на станциях.

При работе станции, происходят обращения к функциям операционной системы, которые заносятся в журнал событий данной станции. Отбор событий происходит в зависимости от выбранного уровня детальности журнала. При максимальном уровне журнала, записываются все обращения к файловым функциям ОС. При минимальном - только запуск программ и все попытки несанкционированного доступа.

События НСД (несанкционированного доступа) фиксируются при любом уровне детальности журнала

Заблокировать станции 

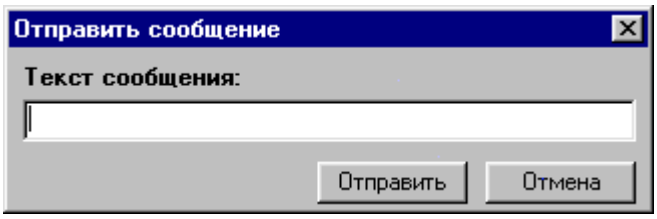
Включить хранитель экрана на выбранных станциях. После выполнения этой команды разблокировать станцию может только администратор с консоли, или непосредственно на рабочей станции своим идентификатором.

Разблокировать станции 

Выключить хранитель экрана на выбранных станциях.

Послать сообщение станциям 

С помощью этой команды можно написать и отправить сообщение операторам выбранных станций.



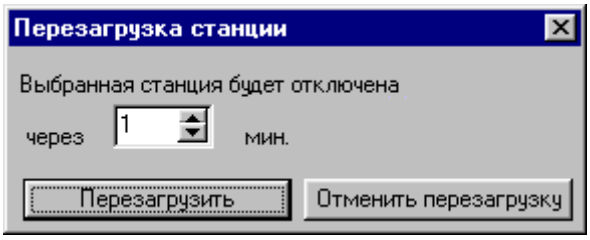
В этом окне администратор пишет сообщение, которое хочет отправить на выбранную станцию. После нажатия кнопки "*Отправить*" сообщение будет передано на станцию.

Получить экран станции 

Эта команда позволяет визуально наблюдать за работой пользователей. Администратор БИ получает копию графического экрана с выбранной станции.

Отключить станцию 

Данная команда выполняет перезагрузку выбранной станции через заданное время.



Если указано время 0 мин., то перезагрузка происходит немедленно.

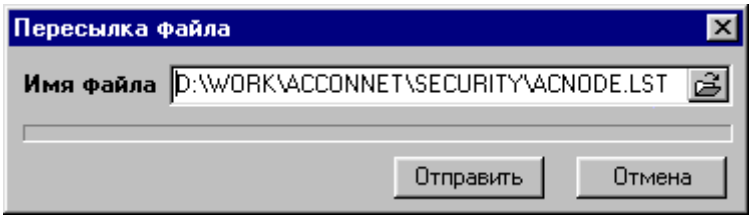
Перезагрузить - выполнить операцию.
Отменить перезагрузку - отменить перезагрузку выбранной станции.

Получить журналы от станций:

Эта команда позволяет переместить локальные журналы с выбранных станций на АРМ администратора, для проведения последующего их анализа. Для каждой станции создается отдельный подкаталог в папке CLIENT.LOG для хранения журналов.

Разослать список станций

Переслать обновлённый список станций всем станциям в сети.



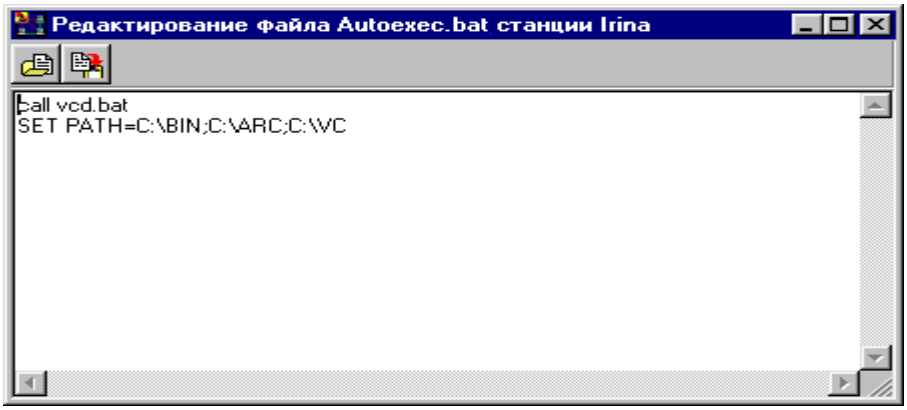
Имя файла - имя файла, в котором находится информация о станциях в сети.

Отправить - выполнить операцию.
Отмена - отменить пересылку файла.

Получение и редактирование файлов конфигураций станции

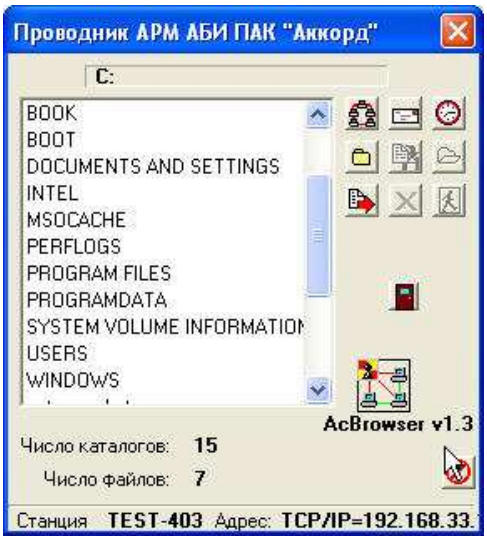
Здесь можно получить файлы конфигурации с выбранной станции.

К файлам конфигурации относятся - config.sys, config.dos, config.win, config.w40, autoexec.bat, autoexec.dos, autoexec.w40. После получения файла имеется возможность отредактировать его и заменить файлы конфигурации выбранной станции.



Проводник сети "Аккорд"

Вызов проводника сети  "Аккорд" для работы с дисками выбранной станции (сокращённый аналог проводника Windows).



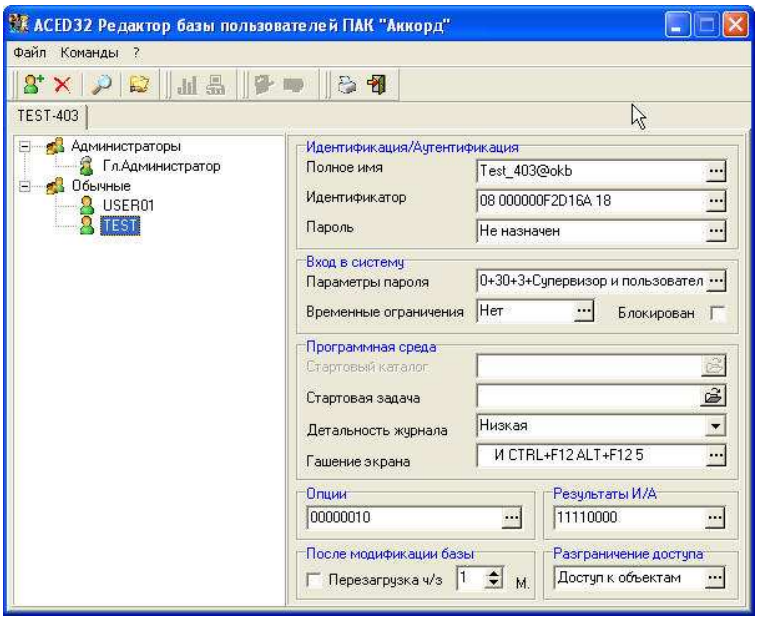
Программа позволяет:
- просматривать диски выбранной станции;
- копировать и удалять файлы;
- просматривать графические файлы в формате JPEG;
- посылать сообщения выбранной станции.
- получить удаленный доступ к рабочему столу станции.

Синхронизация баз пользователей 

Администратор имеет возможность синхронизировать базы пользователей. На каждой рабочей станции хранится база пользователей, в которой содержится список ПРД (правила разграничения доступа). Администратор может работать с базами пользователей на АРМ. Если база пользователей на выбранной станции отличается от файла, который находится на АРМе администратора, то при синхронизации происходит пересылка базы пользователей от администратора на рабочую станцию.

Редактирование базы пользователей 

Администратор может редактировать базы пользователей на АРМ. Измененные базы рассылаются пользователям после редактирования. После выбора этой команды открывается окно редактора ПРД, практически такого же, как в локальной версии. Единственное отличие – вместо пункта контроля целостности установка временного интервала перезагрузки станции после получения новой базы пользователей.



Очистка окон

- *"Очистка*  *окна вывода сообщений от станций"*, в результате которой удаляется информация из окна вывода сообщений от станций.
- *"Очистка окна вывода журнала от станций"*, в результате которой удаляется информация из окна вывода журналов от станций.

(3) Вид

Команды "Группы" и "Список" предназначены удобства работы с программой.

Группы - вывод списка зарегистрированных на АРМ АБИ станций в виде пиктограмм с их именами. В этом режиме работающее станции отображаются значком с синим экраном, а отключенные – рисунком с черным экраном.

Список - вывод включенных станций в виде списка с их именами и возможностью выбора интересующих станций.

Команда ***Журнал***

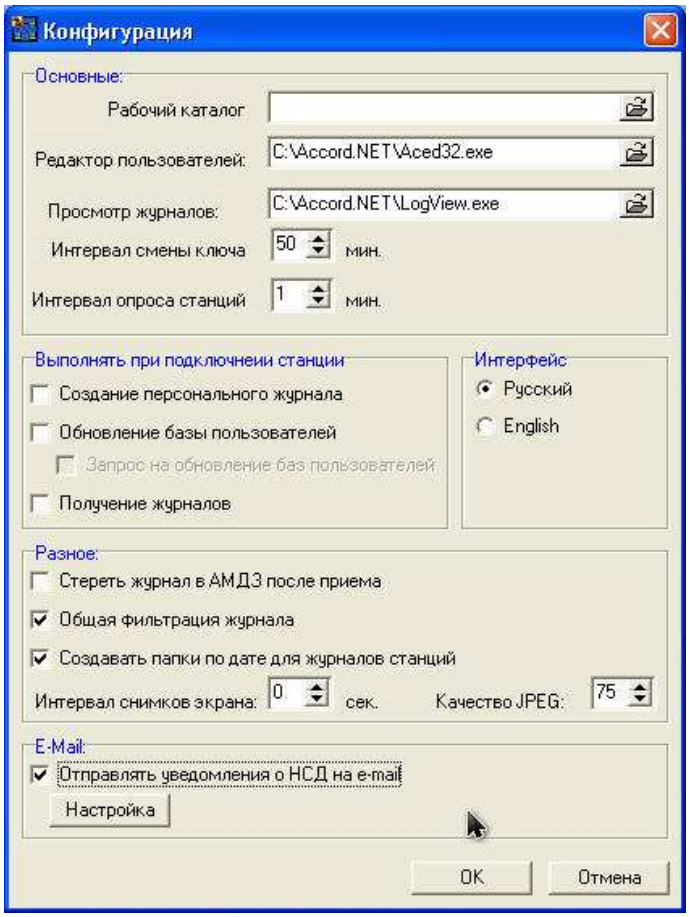
Во время работы каждого пользователя ведется журнал, в котором регистрируются действия, которые он совершает. Администратору безопасности информации рекомендуется в текущей работе использовать низкую детальность ведения журнала. Среднюю и высокую детальность следует использовать при изучении работы вновь используемых задач с целью определения особенностей задачи, а именно: создание новых постоянных и временных каталогов и файлов, используемых прерываний и т.д.

Общий - вывод событий, происходящих на станциях, в один «Общий журнал»

Персональный - вывод событий, приходящих на станциях, в персональные журналы.

(4) Параметры

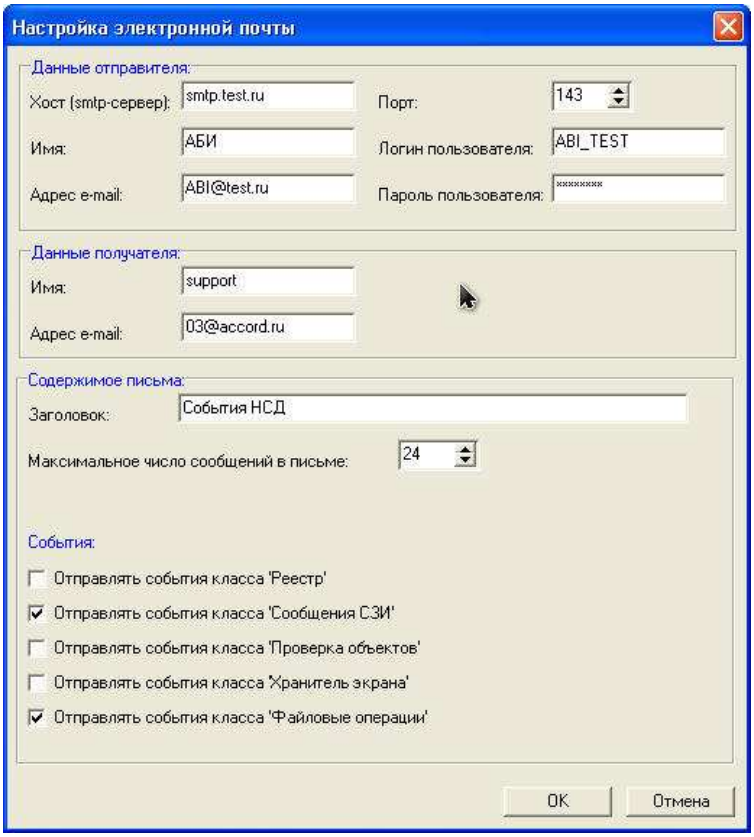
Конфигурация:



В этом окне можно изменить следующие параметры настройки АРМ:

1. *Рабочий каталог* - каталог, из которого запускается АРМ. Необходим для хранения временных файлов и файлов журнала со станций.
2. *Интервал смены ключа* - время, через которое изменяется сеансовый ключ шифрования.
3. *Интервал опроса станций* - время, через которое происходит автоматический поиск станций в сети.
4. *Редактор пользователей* – полное имя программы редактора пользователей ACED32.EXE.
5. *Просмотр журналов* – полное имя программы просмотра журналов LOGVIEW.EXE.
6. *Выполнять при подключении станции*

   Установка операций, которые нужно выполнить при подключении рабочей станции к АРМ АБИ
   - Создание персонального журнала – создавать ли персональный журнал при входе станции в сеть
   - Обновление базы пользователей – обновлять ли базу пользователей на рабочей станции при ее входе в сеть
   - Запрос на обновление баз пользователей – выдавать ли запрос на обновление баз пользователей при синхронизации.
   - Получение журналов
7. *Стереть журнал в АМДЗ после приема* – аппаратная часть комплекса (модуль доверенной загрузки «Аккорд АМДЗ») имеет внутреннюю память для регистрации событий, происходящих во время работы модуля до загрузки ОС. Команда «Получить журналы от станций» позволяет получать журналы из памяти АМДЗ, а данный параметр определяет режим копирования этих журналов (с очисткой памяти контроллера, или без).
8. *Отправлять уведомления о НСД на e-mail* – администратор может установить адрес электронной почты для отправки сообщений о несанкционированном доступе и параметры таких сообщений.



В качестве хоста можно указать имя smtp-сервера, или IP-адрес. Параметр «Максимальное число сообщений в письме» определяет режим накопления сообщений перед отправкой. Если установить значение 1, то письмо с уведомлением будет отправляться сразу. Установка другого числового значения определяет количество накопленных сообщений, которые будут отправлены в одном письме.

2.4. Сообщения программы

"No_Acrun !" - на станции не запущен монитор разграничения доступа.

"Драйвер клиента команду не обслуживает" - данная функция не реализована на выбранной станции.

Приложение 1

Список команд OS и их функциональные значения

№	Код	Операция
1	ACHE	Конец контроля целостности
2	ACHS	Начало контроля целостности
3	BIST	Буферизованный ввод строки
4	CFAT	Получить информацию о FAT текущего диска
5	CHEI	Завершение проверки целостности (вход)
6	CHEO	Завершение проверки целостности (выход)
7	CHKF	Контроль целостности файла
8	CHSI	Начало проверки целостности (вход)
9	CHSO	Начало проверки целостности (выход)
10	CI	Ввод с консоли без вывода
11	CINF	Ввод с консоли без вывода и фильтра
12	CNIO	Консольный I/O
13	CNTR	Получить/установить параметры страны
14	CPSP	Создать PSP
15	DFRE	Получить размер свободного места на диске
16	DGET	Получить текущий диск
17	DICH	Перейти в каталог
18	DIMK	Создать новый каталог
19	DINF	Получить информацию о диске
20	DIRM	Удалить каталог
21	DRES	Сброс диска
22	DSET	Установить текущий диск
23	DSPO	Вывод на дисплей
24	EMEM	Нарушение целостности ACRUN в памяти
25	EUED	ACED: Конец редактирования
26	EXCD	Получить код завершения программы
27	EXEC	Запустить программу
28	f1ST	Find1st через FCB
29	F1ST	Find1st
30	FACC	Запрет/разрешение файлового доступа
31	FATR	Установить/получить атрибуты файла
32	FCLO	Закрыть файл через FCB
33	FCLO	Закрыть файл
34	FCR	Создать файл через FCB
35	FCR	Создать файл
36	FDEL	Удалить файл через FCB
37	FDEL	Удалить файл
38	FGSZ	Получить размер файла через FCB
39	FNEW	Создать новый файл
40	FNXT	FindNext через FCB
41	FNXT	FindNext
42	FO	Открыть файл
43	FOC+	Открыть/создать файл 4.0+
44	FOP	Открыть файл через FCB
45	FRBR	Читать блок файла с произвольным доступом через FCB
46	FRD	Чтение из файла
47	FREN	Переименовать файл через FCB
48	FREN	Переименование/перемещение файла
49	FRRD	Чтение файла с произвольным доступом через FCB
50	FRSQ	Чтение последовательного файла через FCB
51	FSBA	Установить адрес блока файла с произвольным доступом через FCB
52	FSEK	Позиционирование в файле
53	FTIM	Запрос/установка даты/времени файла
54	FTMP	Создать уникальный временный файл
55	FWBR	Писать блок файла с произвольным доступом через FCB
56	FWR	Запись в файл

57	FWRD	Запись файла с произвольным доступом через FCB
58	FWSQ	Запись последовательного файла через FCB
59	GDIR	Получить текущий каталог
60	GDTA	Получить адрес DTA
61	GERR	Получить информацию об ошибке
62	GETD	Получить текущую дату
63	GETT	Получить текущее время
64	GFAT	Получить информацию о FAT
65	GPSP	Получить сегмент PSP
66	GVER	Получить версию ДОС
67	GVRF	Получить состояние флага ДОС Verify
68	HDUP	Дублировать Handle
69	HRED	Перенаправить Handle
70	IAUX	Ввод с AUX
71	ICHK	Проверка состояния ввода
72	ICLR	Ввод с очисткой
73	IDP	ИА Пароль получен
74	IDTM	ИА Дождались ТМ
75	ILOG	ИА Вход в систему
76	INL	Начало работы пользователя
77	IOCT	Функции IOCTL
78	IST	ИА Начало
79	IWP	ИА Ожидание пароля
80	IWTM	ИА Ожидание ТМ
81	KBDI	Ввод с клавиатуры
82	LOUT	Завершение работы пользователя
83	MEMA	Запросить блок памяти
84	MEMC	Изменить размер блока памяти
85	MEMF	Освободить блок памяти
86	NETM	Сеть: разное
87	NRDR	Перенаправление сетевого устройства
88	OAUX	Вывод на AUX
89	OPRI	Печать
90	PARS	Разбор имени файла
91	PRI	Печать
92	PRST	Печать строки
93	SBRK	Запросить/установить состояние флага Break
94	SETD	Установить текущую дату
95	SETT	Установить текущее время
96	SFDA	Получить адрес флага реентерабельности ДОС
97	STDA	Установить DTA
98	SUED	ACED: Начало редактирования
99	SVRF	Установка состояния флага Verify
100	SWTC	Set/Query Switchar (undocumented)
101	TERM	Завершение программы
102	TSR	Завершить и остаться резидентом
103	UWRK	Продолжение работы
104	VGET	Получить адрес вектора прерывания
105	VSET	Установить вектор прерывания