

ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО



систем автоматизированного
проектирования

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН

11443195.4012-006 03 -ЛУ

**Программно-аппаратный комплекс средств защиты
информации от НСД для ПЭВМ (РС)**

“Аккорд–АМДЗ”

(Аппаратный модуль доверенной загрузки)

РУКОВОДСТВО АДМИНИСТРАТОРА

11443195.4012-006 90 03

СОДЕРЖАНИЕ

1.	РАБОТА С ПРОГРАММОЙ.....	4
1.1	СПИСОК ПОЛЬЗОВАТЕЛЕЙ.....	5
1.2	ОБЩИЕ ПАРАМЕТРЫ ГРУППЫ “АДМИНИСТРАТОРЫ”.....	6
1.2.1	<i>Параметры пароля.</i>	6
1.2.2	<i>Доступ к устройствам.</i>	7
1.2.3	<i>Атрибуты доступа.</i>	8
1.2.4	<i>Результаты ИА.</i>	8
1.3	ОБЩИЕ ПАРАМЕТРЫ ГРУППЫ “ОБЫЧНЫЕ” (ПОЛЬЗОВАТЕЛИ).	9
1.3.1	<i>Режим блокировки.</i>	10
1.3.2	<i>Временные ограничения.</i>	10
1.3.3	<i>Загрузка ОС.</i>	10
1.4	РЕГИСТРАЦИЯ СУПЕРВИЗОРА (АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИИ).....	11
1.4.1	<i>Назначение персонального идентификатора.</i>	12
1.4.2	<i>Генерация секретного ключа.</i>	13
1.4.3	<i>Назначение пароля.</i>	14
1.5	РЕГИСТРАЦИЯ НОВОГО ПОЛЬЗОВАТЕЛЯ.....	16
1.6	УДАЛЕНИЕ ПОЛЬЗОВАТЕЛЯ ИЗ СПИСКА.....	16
1.7	РЕДАКТИРОВАНИЕ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЕЙ.....	16
1.8	ЭКСПОРТ/ИМПОРТ СПИСКА ПОЛЬЗОВАТЕЛЕЙ.....	16
1.9	КОНТРОЛЬ.....	18
1.9.1	<i>Контроль аппаратуры.</i>	18
1.9.2	<i>Контроль целостности служебных областей жестких дисков.</i>	19
1.9.3	<i>Контроль целостности файлов.</i>	19
1.9.4	<i>Контроль целостности реестра Windows.</i>	23
1.9.5	<i>Дополнительные функции меню «Контроль».</i>	24
1.10	СИСТЕМНЫЙ ЖУРНАЛ.....	26
1.11	СЕРВИС.....	27
2.	ВЫХОД ИЗ ПРОГРАММЫ.....	28

Назначение

Программа администратора системы защиты информации является частью комплекса "АККОРД-АМДЗ" и не требует установки какого-либо дополнительного ПО. С помощью этой программы администратор СЗИ может добавлять и удалять пользователей, назначать пользователям идентификаторы и пароли, контролировать аппаратную часть ПЭВМ, прикладные и системные файлы, получает доступ к системному журналу контроллера.

Термины.

Пользователь - субъект доступа к объектам (ресурсам) ПЭВМ.

Администратор - администратор службы безопасности информации.

Идентификатор - идентификатор Touch-memory DS-199X, смарт-карта eToken PRO, или ПСКЗИ ШИПКА.

Использовать идентификатор – подключить идентификатор к соответствующему контактному устройству.

Меню - окно с изображением кнопок с названиями команд. Перемещения по меню осуществляются с помощью мыши или клавишей <Tab>. Выбор команды - мышью (левая клавиша) или <Enter>, выход из меню - <Esc>, или командой в меню.

Окно ввода/вывода - служит для ввода и отображения буквенно-цифровой информации, а так же может выполнять функции меню. Содержит окно для ввода буквенно-цифровой информации, окна списков, кнопки команд, окна флагов. Ввод буквенно-цифровой информации должен заканчиваться <Enter>, или перемещением в другое окно, движение списка в окне - с помощью стрелок, или мышью. Перемещение по окнам и кнопкам команд, выбор команд и выход из окна - аналогично работе с меню.

Сообщения - информация, выводимая на дисплей, которая сообщает о действиях, требуемых от пользователя, о состоянии программы и о нормально завершенных действиях.

Ошибки - информация, выводимая на дисплей, указывающая на неправильность действий, сбой, аварии комплекса.

Пояснения - в описании некоторых команд даются пояснения и рекомендации администратору для использования этих команд. Пояснения выделены мелким шрифтом.

1. РАБОТА С ПРОГРАММОЙ.

Если в компьютер устанавливается новый контроллер АДЗ, то при загрузке выполняется инициализация и форматирование внутренней памяти. После завершения этой операции на экран выводится стартовое меню администратора (Рис. 1.). Поскольку в контроллере нет зарегистрированных пользователей, то в этом меню доступны для выбора только пункты "Администрирование" и "Выход в AcDOS".

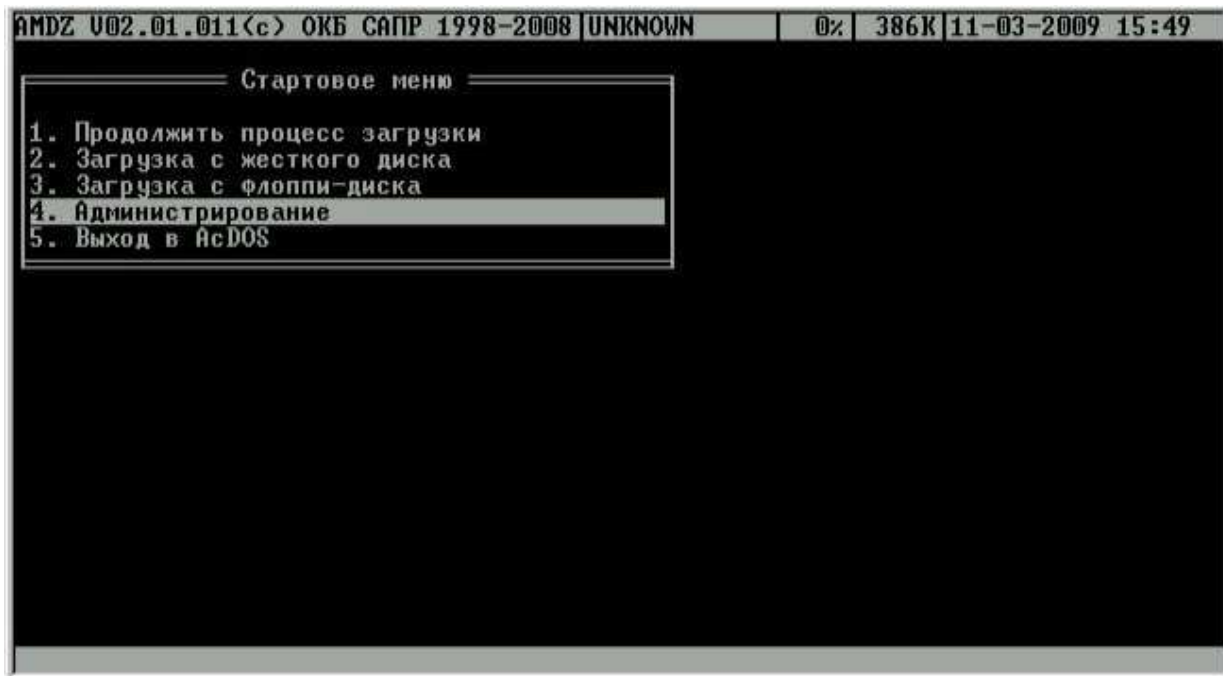


Рис. 1. Стартовое меню администратора.

“Выход в AcDOS” позволяет загрузить компьютер с использованием внутренней операционной системы контроллера (ACDOS). В дальнейших разработках предполагается включение в состав этой ОС средств диагностики контроллера и компьютера.

Клавишей <Enter> запустите программу администрирования. На экран выводится главное меню (Рис. 2.).



Рис. 2. Главное меню администратора.

Главное меню состоит из следующих полей:

- строка команд (левая половина верхней строки);
- информационная строка (правая половина верхней строки);
- статус (HELP) - нижняя строка;
- рабочее поле (все остальное пространство).

Строка команд позволяет вызвать следующие подпрограммы:

- <Польз> - работа со списком пользователей;
- <Контр> - работа со списками контроля целостности;
- <Журнал> - работа с внутренним журналом регистрации событий;
- <Сервис> - дополнительные настройки;
- <Помощь> - описание функций и сведения о продукте.

После начальной инициализации в строке команд недоступны пункты <Контр> и <Журнал>, т.к. в памяти контроллера не зарегистрировано ни одного пользователя (в верхней информационной строке имя текущего пользователя UNKNOWN, т.е. неизвестный). Поэтому первое действие, которое нужно выполнить - это регистрация пользователя с правами администратора.

1.1 Список пользователей.

В меню выберите команду <Польз.>. На экран выводится дерево списка пользователей (Рис. 3.).



Рис. 3. Список пользователей.

При инициализации контроллера создаются две зарезервированные группы пользователей – “Администраторы” и “Обычные”. Эти две группы нельзя ни переименовать, ни удалить. Для каждой из групп можно задать общие параметры, которые будут устанавливаться по умолчанию при создании пользователя в группе. Для каждого зарегистрированного пользователя можно изменить данные параметры при индивидуальной настройке. Такие же правила будут выполняться и для любой группы, созданной администратором. Для редактирования общих параметров группы пользователей необходимо клавишами “стрелка” или мышью установить курсор на строке заголовка группы и нажать <Enter>, или дважды щелкнуть левой кнопкой мыши.

1.2 Общие параметры группы “Администраторы”.

Для группы “Администраторы” установлены следующие общие параметры (Рис. 4.):

- параметры пароля;
- доступ к устройствам;
- атрибуты доступа;
- результаты ИА (Идентификации/Аутентификации пользователя).



Рис. 4. Общие параметры группы “Администраторы”.

1.2.1 Параметры пароля.

Для пользователя, у которого введен пароль, можно регулировать следующие параметры пароля (Рис. 5.):

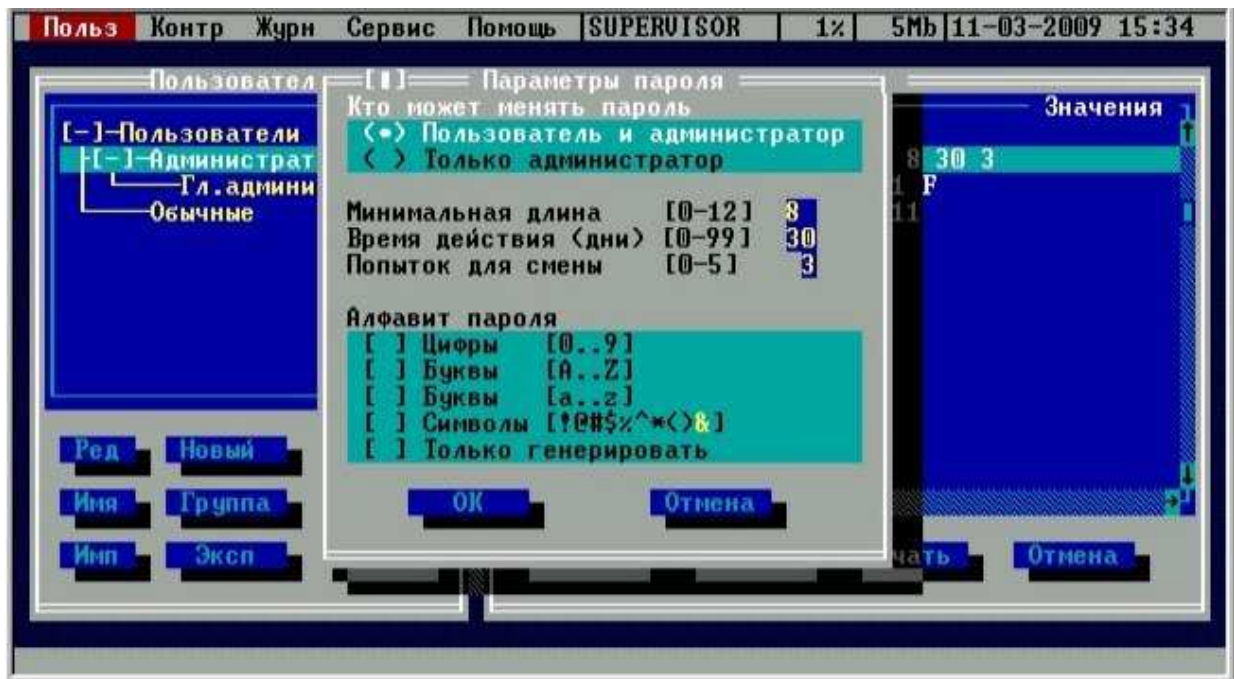


Рис. 5. Параметры пароля.

- "Кто может менять пароль" - установка этого параметра позволяет пользователю самому менять пароль после истечения времени действия, или смену пароля может осуществлять только администратор.
- "Минимальная длина" - параметр определяет количество символов, контролируемое при создании и смене пароля. Нельзя ввести пароль меньшей длины. Если предполагается для авторизации пользователя использовать только идентификатор, то этот параметр нужно установить в 0 (пароль задавать не обязательно). По умолчанию длина пароля установлена равной 8 символам, максимальное допустимое значение - 12 символов.
- "Время действия (дни)" - время действия пароля до смены в календарных днях: от 0 (смены пароля не требуется) до 99 дней.
- "Попыток для смены" - количество попыток смены пароля: от 0 (не ограничено) до 5. Этот параметр определяет допустимое число попыток смены пароля, если пользователю разрешено самому выполнять такую операцию. Если за отведенное число попыток пароль не сменен корректно, то работа данного пользователя блокируется, и для разблокировки и смены пароля потребуется вмешательство администратора (для выполнения смены пароля необходимо ввести старый пароль, а затем дважды - новый).
- «Алфавит пароля» - определяет набор символов, которые обязательно должны использоваться при вводе пароля. Например, если в алфавите заданы цифры и буквы, то нельзя ввести пароль, состоящий из одних цифр. При установке флага «Только генерировать» пароль будет генерироваться случайным образом из символов заданного алфавита при смене пароля пользователя.

Обратите внимание! Если пароль уже задан, то изменения его параметров вступят в силу только при смене пароля.

1.2.2 Доступ к устройствам.

Этот параметр действует только для контроллеров с установленными реле управления внешними (по отношению к плате контроллера) устройствами. Внутреннее ПО контроллера АМДЗ дает возможность управлять 3-мя независимыми гальванически развязанными контактными парами, с помощью которых можно блокировать доступ отдельных пользователей к внешним устройствам, например, к накопителю FDD, CD-ROM, HDD или USB-портам. При установке флага «Фиксировать» запрет действует не только на момент загрузки операционной системы, но и на весь сеанс работы пользователя.

Выберите пункт "Управление устройствами" и нажмите <Enter>. На экран выводится окно со списком устройств (Рис. 6.).



Рис. 6. Функция управления внешними устройствами.

С помощью клавиши <Пробел> в квадратных скобках можно установить или сбросить флаг разрешения работы устройства. Переход к пунктам <Запись> <Отмена> осуществляется клавишей <Tab> или мышью.

Внимание!

На управляемую контактную пару может быть заведен сигнал напряжением не более 5В и силой тока не более 300 Ма.

ОКБ САПР выпускает переходники-прерыватели для разных типов устройств. Подробная информация размещена на сайте компании (www.accord.ru) в разделе «Цены».

1.2.3 Атрибуты доступа.

При выборе параметра «Атрибуты доступа» открывается окно (Рис.7.) в котором Гл.администратор может установить набор функций администрирования, доступных «подчиненным» администраторам. Эти параметры лучше устанавливать индивидуально каждому администратору, а не в параметрах группы. Нужно заметить, что в правилах настройки СЗИ «Аккорд-АМДЗ» нет ограничений на число пользователей, зарегистрированных в той, или иной группе. Существует только лимит на общее количество записей (128) в базе данных пользователей. Запись – это данные о группе, или отдельном пользователе.

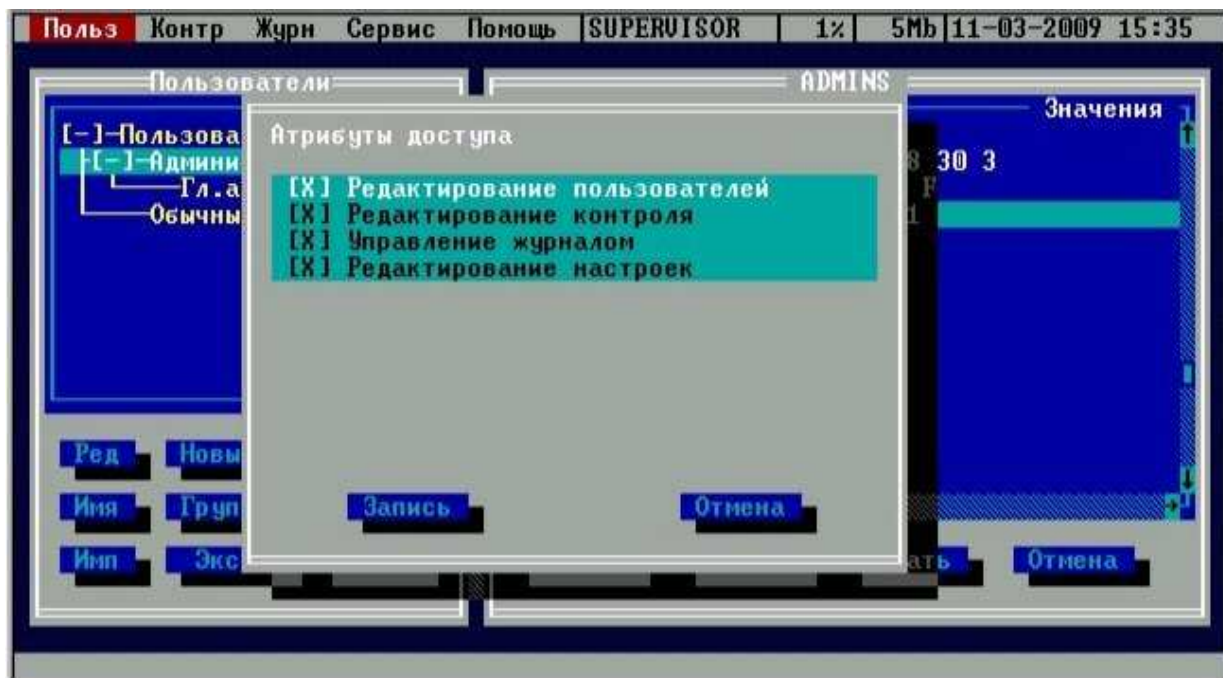


Рис. 7. Выбор атрибутов доступа администратора к функциям управления.

1.2.4 Результаты ИА.

В разделе “Результаты ИА” устанавливается, какая информация о пользователе, полученная в результате процесса Идентификации/Аутентификации, будет передаваться из контроллера в программную подсистему разграничения доступа (если таковая установлена на компьютере). Для успешного выполнения процедуры «Автологин», т.е. когда пользователь авторизуется на аппаратном уровне, а программная часть автоматически подгружает его профиль доступа, необходимо включить первые пять флагов «Результатов И/А». Установки по умолчанию (Рис. 8.) предполагают использование только контроллера АМДЗ.

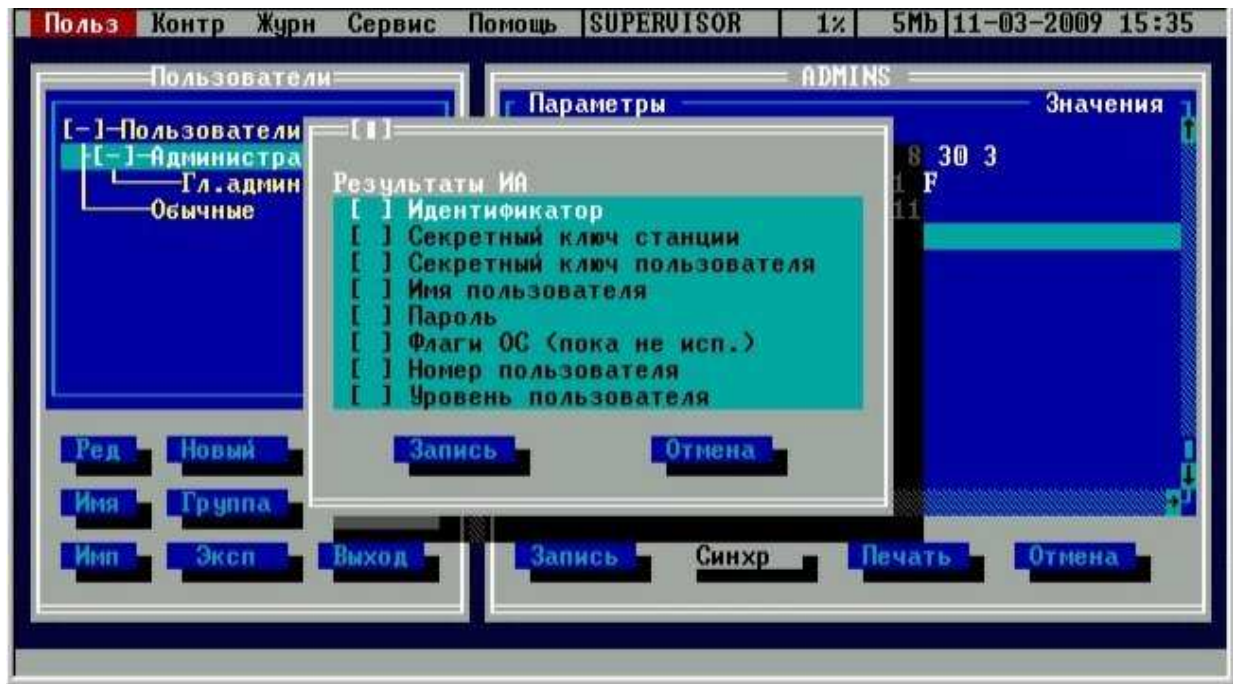


Рис. 8. Результаты ИА.

1.3 Общие параметры группы “Обычные” (пользователи).

Для группы “Обычные” (пользователи) установлены следующие общие параметры (Рис. 9.):

- параметры пароля;
- временные ограничения;
- режим «Блокирован»;
- загрузка ОС;
- доступ к устройствам;
- результаты ИА (Идентификации/Аутентификации пользователя).



Рис. 9. Общие параметры группы “Обычные пользователи”.

Настройки “Параметры пароля”, “Доступ к устройствам” и “Результаты ИА” такие же, как общие параметры группы “Администраторы”. Другие пункты рассмотрим подробнее.

1.3.1 Режим блокировки.

При установке флага «Блокирован» в состояние «Да» все параметры пользователя сохраняются в базе данных, но вход в систему и работа данного пользователя будут запрещены. Данный флаг можно использовать для временной блокировки пользователя. После того, как администратор снимет блокировку, работа пользователя восстановится со всеми установленными настройками. Для изменения состояния данного флага достаточно установить курсор в строку «Блокирован» и нажать клавишу <Enter>.

1.3.2 Временные ограничения.

Администратор может устанавливать для пользователя ограничения на вход в систему с точностью до 30 минут в любой день недели. Выберите пункт "Временные ограничения" и нажмите <Enter>. На экран выводится окно "Временные ограничения" (Рис. 10.).

Клавишами «стрелка» можно перемещаться по матрице времени входа в систему. Клавиша <Пробел> меняет знак + на – и обратно, т.е. разрешает или запрещает загрузку компьютера данному пользователю в данный временной интервал.

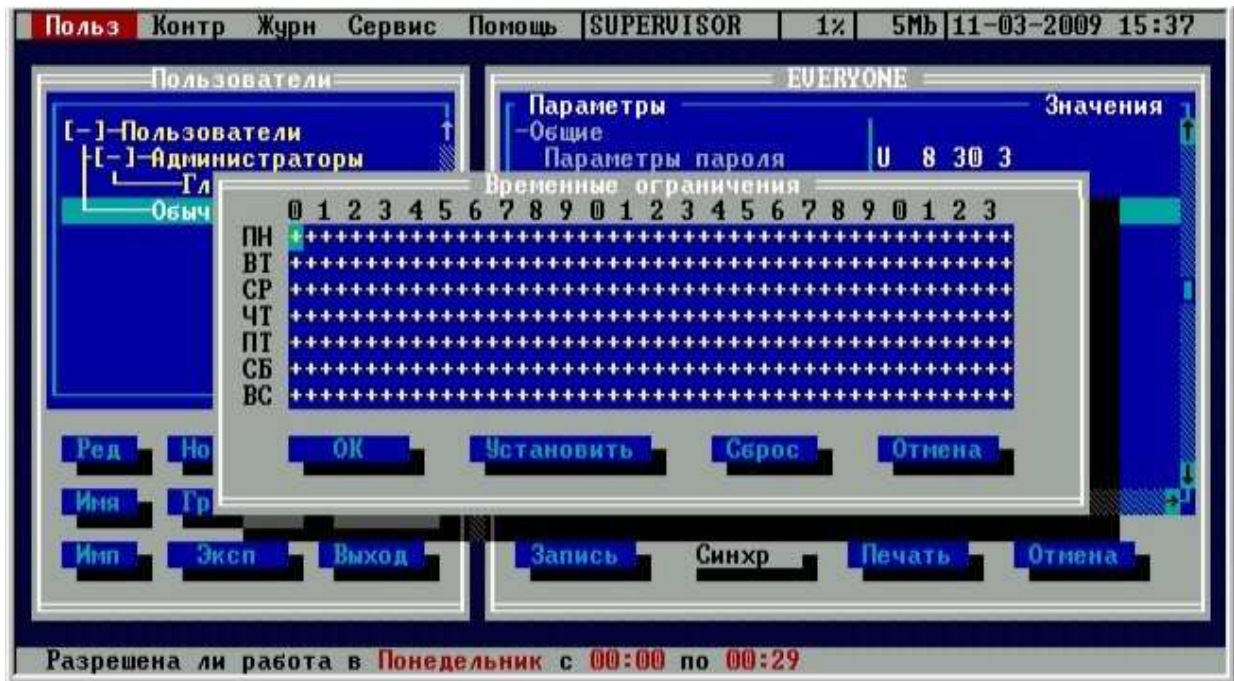


Рис. 10. Временные ограничения на загрузку компьютера.

1.3.3 Загрузка ОС.

В контроллере «Аккорд-АМДЗ» предусмотрена возможность управления режимом загрузки Windows 95/98 и загрузкой различных конфигураций ПО с использованием меню в файле CONFIG.SYS.

Выберите пункт "Загрузка ОС" и нажмите <Enter>. На экран выводится окно со списком возможных вариантов загрузки Windows 95, меню выполнения CONFIG.SYS для Windows 95 и MSDOS (если она установлена) (Рис. 11.). С помощью клавиши <Пробел> в квадратных скобках можно установить или сбросить флаг разрешения выбора того или иного сценария загрузки. Клавиша <F6> служит для перемещения курсора от одного окна к другому. Отмеченные флагом пункты меню становятся доступными пользователю для выбора в процессе загрузки ОС путем нажатия на клавишу с номером пункта. Клавиши со стрелками блокируются на момент загрузки, как на основной, так и на дополнительной (цифровой) клавиатуре.



Рис. 11. Управление загрузкой ОС.

Внимание!

Для успешной работы данной опции под Windows 95/98 в файле MSDOS.SYS в разделе [Options] должна быть прописана строка BootMenu=1.

1.4 Регистрация супервизора (администратора безопасности информации).

При инициализации контроллера в базе данных создается учетная запись “Гл. администратор”, но поля этой записи не заполнены. Для регистрации администратора системы выберите строку <Гл. администратор>, нажмите <Enter>. На экран выводится окно ввода-вывода "Параметры пользователя" (Рис. 12.).



Рис. 12. Регистрация пользователя «Гл.Администратор».

1.4.1 Назначение персонального идентификатора.

Выберите строку <Идентификатор> (Рис. 12.). На экран выводится информация о зарегистрированном идентификаторе. При первой установке контроллера никаких данных об идентификаторе нет (Рис. 13.). Выберите команду <Новый>. На запрос идентификатора (Рис. 14.) прикоснитесь идентификатором к съемнику. Для отмены текущей операции, выберите команду <Отмена>.

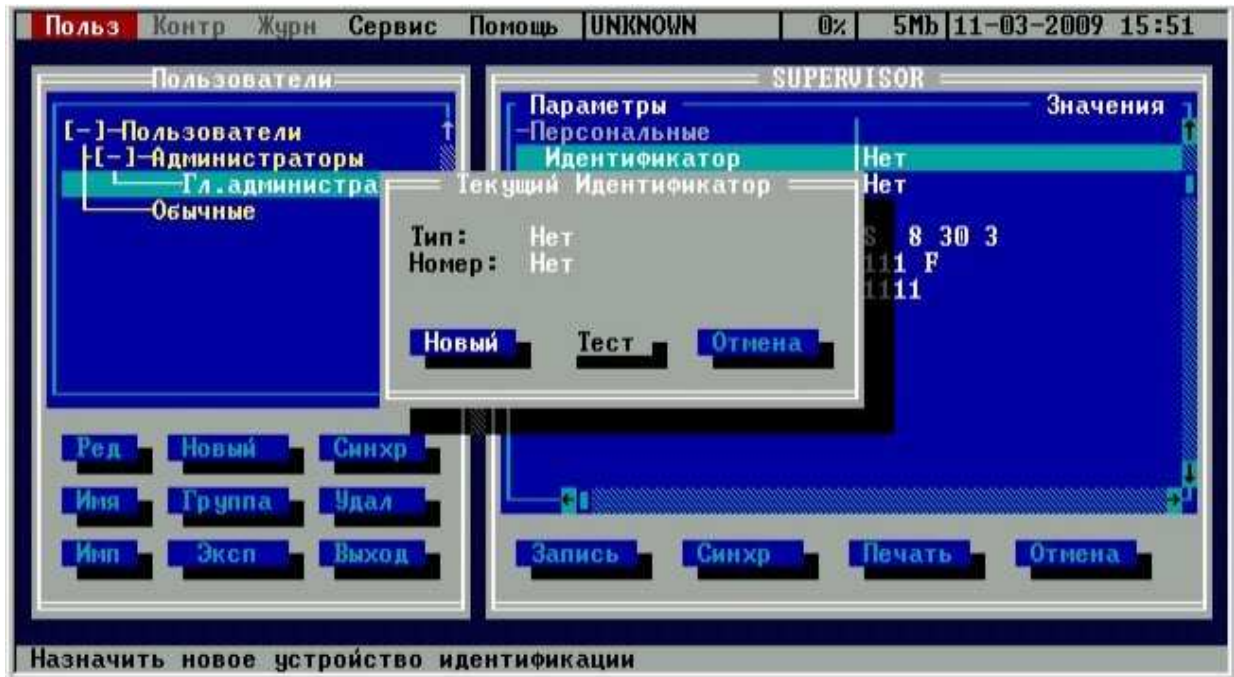


Рис. 13. Информация об идентификаторе.

Примечание: В том случае, когда в качестве персонального идентификатора используется ПСКЗИ ШИПКА, на запрос идентификатора следует подключать устройство ШИПКА к USB-порту контроллера АМДЗ. Если в качестве идентификатора используется смарт-карта eToken PRO, то следует вставить карту в считыватель.

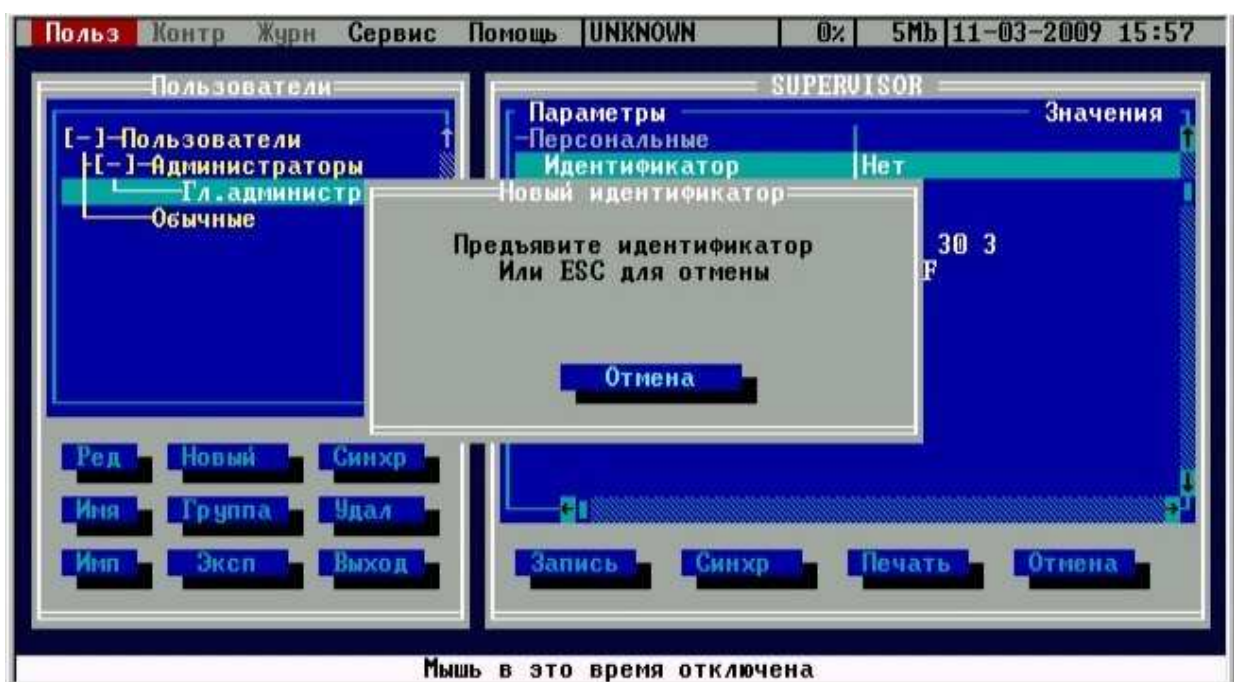


Рис. 14. Запрос идентификатора.

1.4.2 Генерация секретного ключа.

После использования идентификатора на экране появляется меню генерации секретного ключа (Рис. 15.), который уникален для каждого пользователя и записывается во внутреннюю память регистрируемого идентификатора. Этот секретный ключ используется в мониторе правил разграничения доступа ACRUN, который позволяет каждому пользователю создать изолированную программную среду (ИПС) и персональный набор файлов, контролируемых на целостность. Кроме того, этот параметр позволяет надежно защищать данные о пользователе в энергонезависимой памяти контроллера, т.к. в качестве уникального признака используется результирующая хеш-функция от номера идентификатора, пароля и секретного ключа.

Внимание! Идентификатор, в котором не записан секретный ключ, воспринимается как недопустимый в процессе идентификации-аутентификации пользователя, даже если его номер высвечивается в строке "Идентификатор".

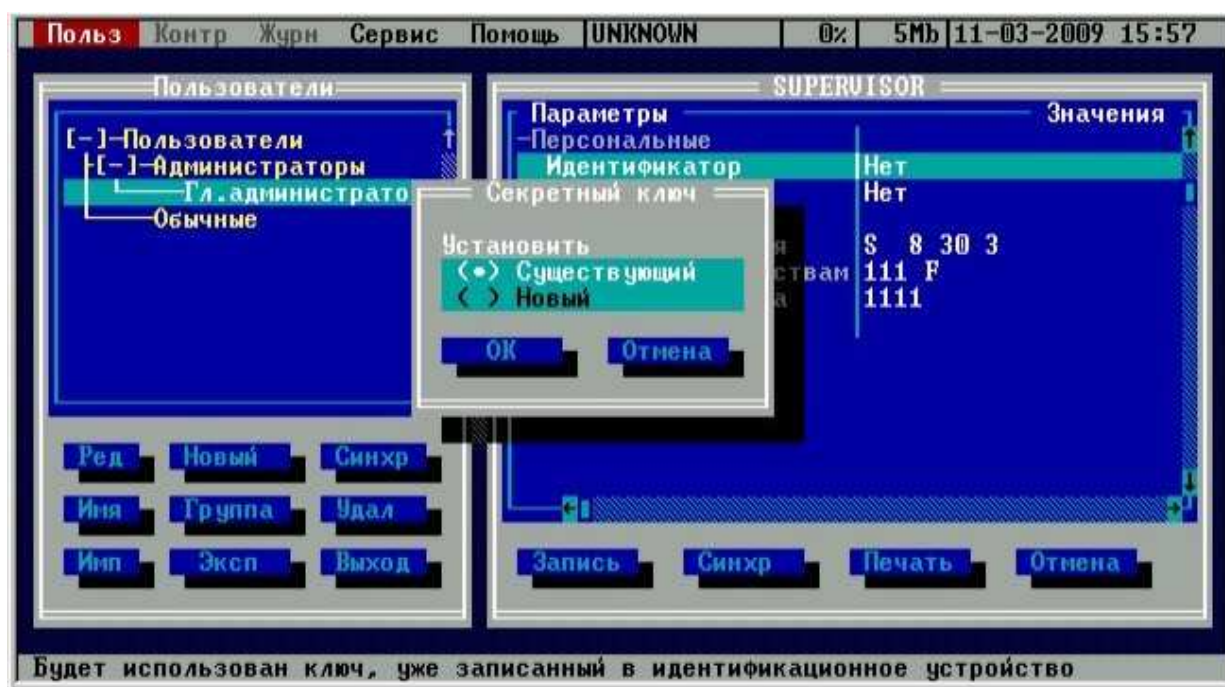


Рис. 15. Генерация секретного ключа пользователя.

Выберите опцию <Новый> и <ОК>. На запрос идентификатора подключите идентификатор к контактному устройству.

Примечание: секретный ключ может быть уже записан в идентификаторе в следующих случаях:

- при перерегистрации пользователя;
- при регистрации одного пользователя на нескольких компьютерах с установленной системой "Аккорд".

Генерировать секретный ключ следует **только при первой регистрации**, т.к. каждая новая генерация затирает предыдущее значение ключа, и идентификатор не будет читаться на других компьютерах.

В этом случае выберите опцию <Существующий> и <ОК>. На запрос идентификатора подключите идентификатор к контактному устройству.

1.4.3 Назначение пароля.

В окне "Параметры пользователя" (Рис. 12.) выберите строку "Пароль" и нажмите <Enter>. На экран выводится окно ввода пароля (Рис. 16.). Введите новый пароль. Повторите ввод пароля во второй строке. Пароль может состоять из букв, цифр и специальных символов. Вводимые символы на экране отображаются точками. При несовпадении введенных последовательностей выводится сообщение об ошибке. В этом случае операцию придется повторить. Символы могут вводиться как в верхнем, так и в нижнем регистре. Будьте внимательны! Длина пароля должна быть не меньше параметра, установленного в строке "Минимальная длина" в разделе "Параметры пароля". Если длина введенного пароля меньше, выводится сообщение об ошибке. Не допускается ввод в качестве пароля последовательностей типа: '123456' или 'qwerty'. При вводе подобных последовательностей символов выдается сообщение об ошибке.

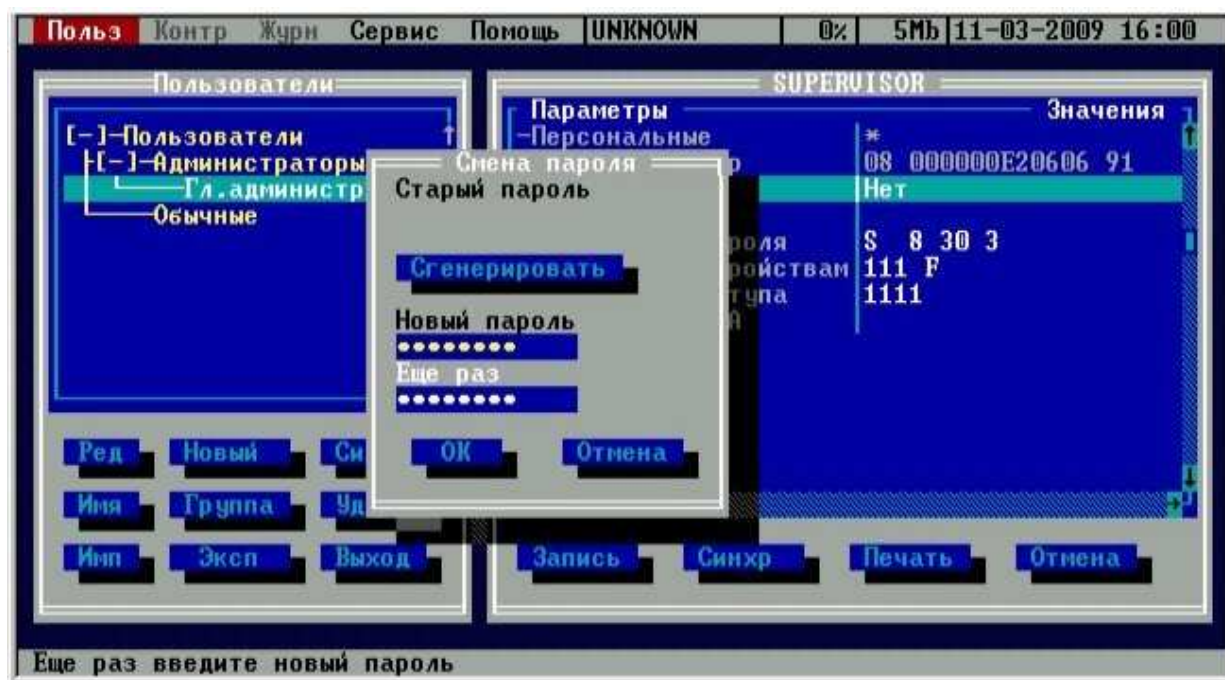


Рис. 16. Окно ввода пароля.

Внимание! Если пользователю не назначается пароль, то в строке "Минимальная длина" в разделе "Параметры пароля" следует установить длину пароля 0, иначе при записи данных о пользователе (по клавише F2) выводится сообщение об ошибке.

Можно выбрать процедуру генерации пароля случайным образом (кнопка «Сгенерировать»). В этом случае пароль генерируется таким образом, чтобы в нем обязательно присутствовал хотя бы один символ из набора, заданного в параметре «Алфавит пароля» (Рис. 17.). После генерации новый пароль выводится в строке «Новый пароль» и пользователь должен его ввести с клавиатуры в поле «Ещё раз».

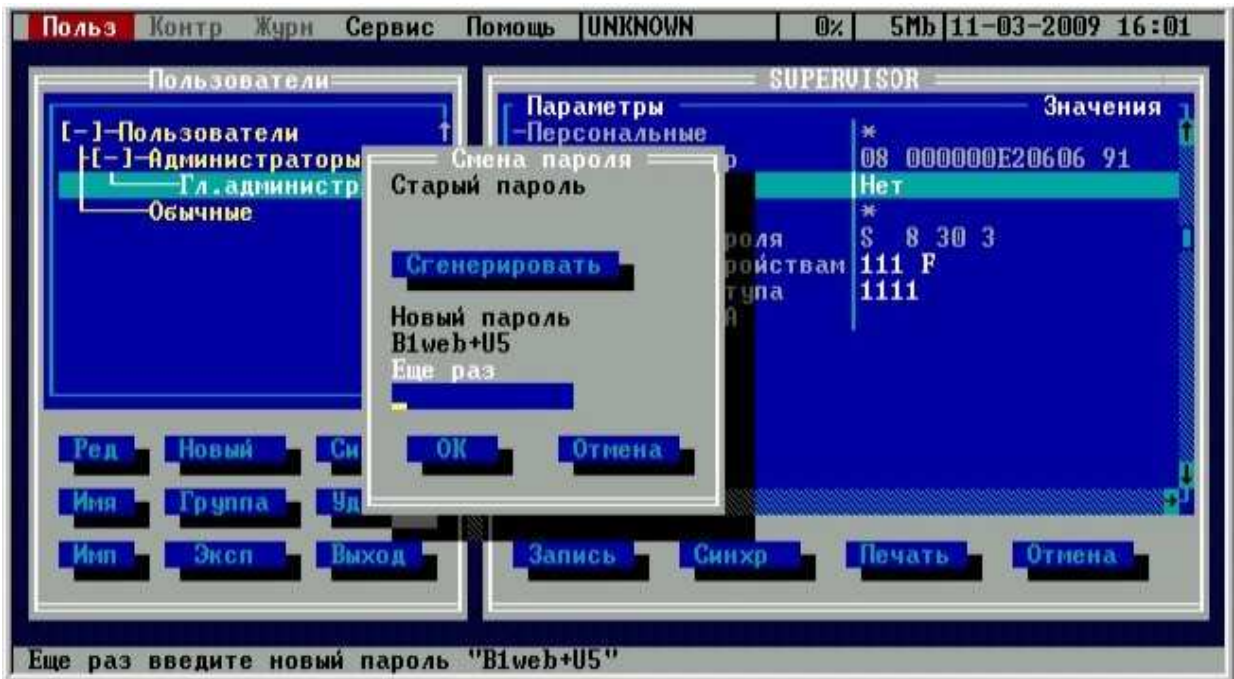


Рис. 17. Случайная генерация пароля.

Для сохранения параметров пользователя «Гл.Администратор» и выхода в окне «Параметры пользователя» выберите команду <Запись> (клавиша <F2>).

После сохранения параметров пользователя «Гл.Администратор» нужно выйти из процедуры редактирования списка пользователей по клавише <Esc> и повторным нажатием этой клавиши из программы администрирования. Выполняется рестарт внутреннего ПО контроллера, и на экран выводится запрос идентификатора и пароля пользователя. После предъявления идентификатора и ввода пароля пользователя «Гл.Администратор» появляется меню, в котором уже доступны все пункты, в частности выбор вариантов загрузки ОС (Рис. 18.).

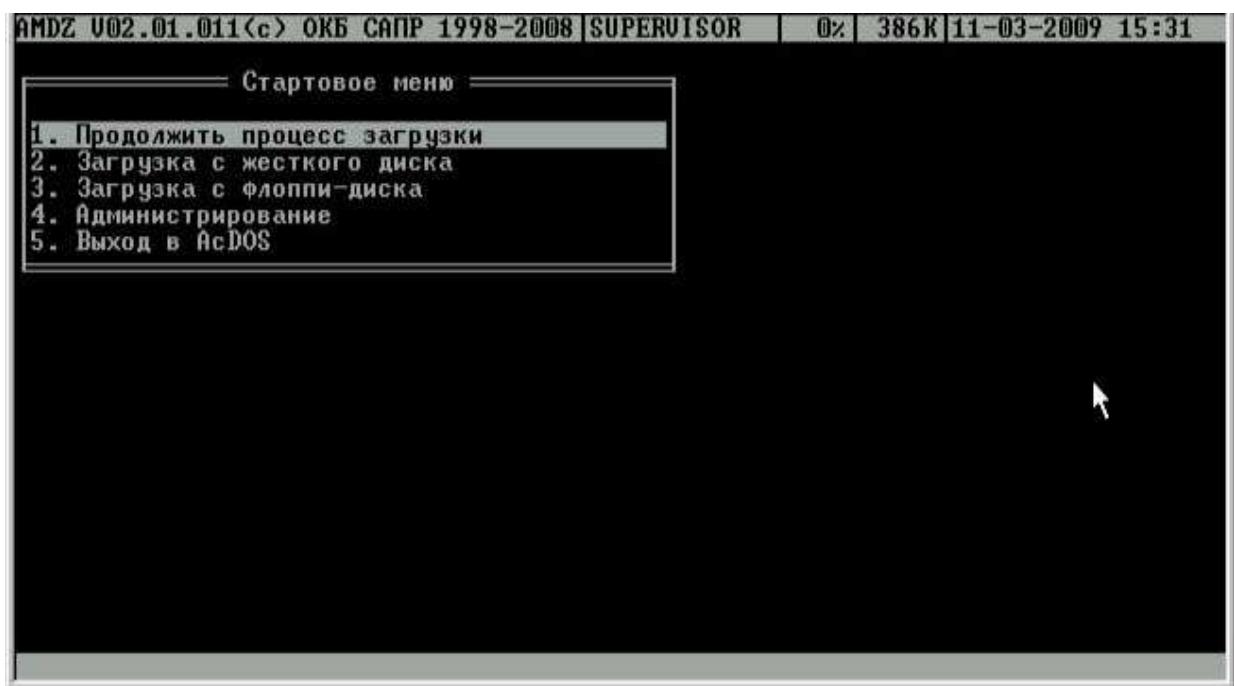


Рис. 18. Меню администратора после регистрации и успешной аутентификации.

Теперь в режиме «Администрирование» доступны все функции.

1.5 Регистрация нового пользователя.

Установите в списке пользователей курсор на заголовке группы “Обычные”. Выберите команду <Новый>, или нажмите клавишу <Insert>. На экран выводится окно ввода имени пользователя. Введите имя нового пользователя. Администратор должен присвоить каждому пользователю уникальное в данной вычислительной среде (отдельный компьютер или локальная сеть) имя. Рекомендуется использовать в качестве имени фамилию пользователя. На экран выводится окно ввода-вывода “Параметры пользователя”. Зарегистрируйте идентификатор и пароль пользователя. При вводе нового пользователя общие параметры, установленные для группы, присваиваются ему по умолчанию, но в окне “Параметры пользователя” их можно изменить. Если администратор безопасности изменяет общие параметры группы, то установить их для всех пользователей группы можно по команде <Синхр.> (Синхронизировать).

1.6 Удаление пользователя из списка.

В подменю списка пользователей (Рис. 3.) выберите и пометьте имена пользователей, предназначенных для удаления из списка. Нажмите клавишу , подтвердите удаление.

1.7 Редактирование параметров пользователей.

В этом режиме администратор производит изменение параметров доступа пользователя к объектам СЗИ. В подменю списка пользователей (Рис. 3.) выберите имя пользователя, параметры которого необходимо отредактировать, нажмите клавишу <Enter>. На экран выводится окно (Рис. 19.). Произведите изменения в окне ввода/вывода “Параметры пользователя”.



Рис. 19. Редактирование параметров пользователя

1.8 Экспорт/импорт списка пользователей.

Список пользователей можно скопировать на внешний носитель, а в случае необходимости, загрузить эту копию с внешнего носителя. В качестве внешнего носителя можно использовать ТМ-идентификатор DS-1996, или флоппи-диск.

При выборе кнопки "Эксп."(экспорт) выводится окно выбора типа внешнего носителя.



Рис. 20. Выбор носителя для экспорта базы пользователей.

Если в качестве носителя выбран диск, то потребуется ввести имя файла.



Рис. 21. Ввод имени файла резервной копии.

Расширение (тип файла) задано по умолчанию, менять его не нужно. После нажатия кнопки "Ok", выполняется копирование списка пользователей на внешний носитель.

Для считывания списка с внешнего носителя нужно нажать кнопку "Имп"(импорт) в окне списка пользователей, выбрать тип носителя (при выборе дискеты необходимо ввести имя файла). На экран выводится окно – предупреждение. Для подтверждения выполнения операции необходимо выбрать и нажать кнопку "Ok".

1.9 Контроль.

В этом режиме администратор контролирует состав и параметры аппаратной части ПЭВМ и может выбирать файлы для контроля их целостности.

В главном меню выберите команду <Контроль>. На экран выводится подменю контроля, состоящее из основных пунктов:

- <Аппаратура>
- <Диски>
- <Файлы>
- <Реестры Windows>.

1.9.1 Контроль аппаратуры.

В подменю выберите команду <Аппаратура> и нажмите <Enter>. На экран выводится окно контроля аппаратуры (Рис. 22.).

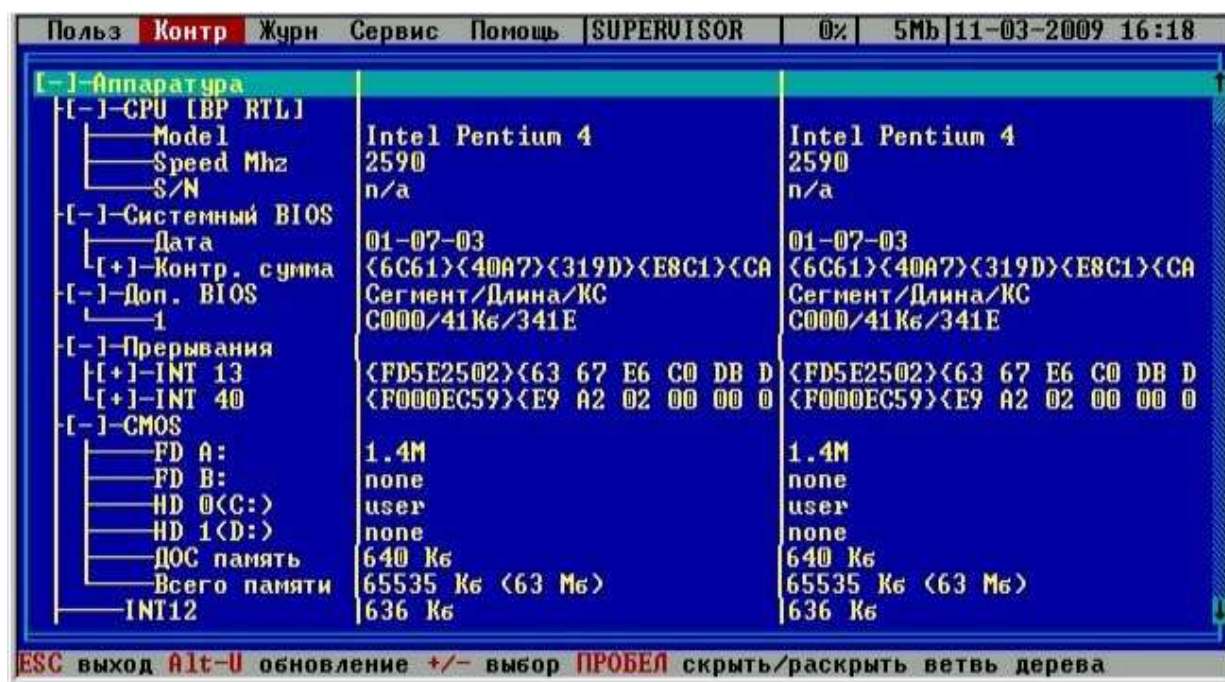


Рис. 22. Окно контроля аппаратной части компьютера.

В левой колонке выводится список контролируемых устройств, в средней - состояние устройств и контрольные суммы, записанные в энергонезависимой памяти контроллера, а в правой - текущее состояние аппаратуры и контрольных сумм. Скролирование окна производится клавишами <Page Up> и <Page Down> или мышью в правой полосе прокрутки. Если данные совпадают, то они высвечиваются в обеих колонках одинаковым цветом. При несовпадении данные в колонках высвечиваются разными цветами. В этом случае запустите операцию обновления комбинацией клавиш <Alt>+<U>. Для включения устройства в список контролируемых необходимо установить на него курсор и нажать клавишу <Insert>. Для снятия отметки используется клавиша . Клавиша <Пробел> раскрывает/сворачивает дерево параметров в контролируемой группе. Выход из режима контроля аппаратуры осуществляется клавишей <Esc>.

После регистрации в СЗИ "АККОРД" хотя бы одного пользователя контроль аппаратуры производится при каждой загрузке компьютера после идентификации/аутентификации пользователя. Если обнаруживается несовпадение параметров конфигурации, записанных в памяти контроллера и текущих параметров системы, то выдается сообщение на красном фоне "Разберитесь с ошибками" и загрузка компьютера блокируется для обычного пользователя, или выводится стартовое меню, если идентифицирован администратор.

Может встречаться ситуация, когда после перезагрузки Аккорд сообщает, что есть ошибки в контрольной сумме BIOS и доп. BIOS, хотя никаких изменений в настройках BIOS не выполнялось. В процедуре контроля аппаратуры видны ошибки, контрольные суммы не совпадают. Администратор обновляет данные, но после перезагрузки все повторяется: снова сообщение об ошибке контроля аппаратуры.

В данном случае в компьютере достаточно «интеллектуальная» материнская плата, или устройство с расширенным собственным BIOS. При каждой перезагрузке, или выключении они записывают информацию в определенные области своих BIOS. Бессмысленно каждый раз пересчитывать контрольные суммы того, что меняется при перезагрузке. Нужно исключить меняющиеся параметры из списка контролируемых объектов клавишей <->, или и пересчитать КС (комбинация клавиш Alt-U).

1.9.2 Контроль целостности служебных областей жестких дисков.

В подменю <Контроль> выберите команду <Диски> и нажмите <Enter>. На экран выводится окно контроля служебных областей дисков (Рис. 23.). Поддерживаются файловые системы следующих типов: FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSD.

В окне контроля выводится дерево всех дисков, установленных на данном компьютере с указанием файловой системы каждого диска. Перемещение по дереву выполняется стрелками, или клавишами <Page Up> и <Page Down>. Для включения области диска в список контролируемых объектов необходимо установить на него курсор и нажать клавишу <Insert>. Для снятия отметки используется клавиша . В список контролируемых можно вносить служебные области с любых дисков, установленных в компьютере, независимо от файловой системы. Для пересчета и записи в память контроллера хэш-функций контролируемых областей используется комбинация клавиш <Alt>+<U> (обновление).

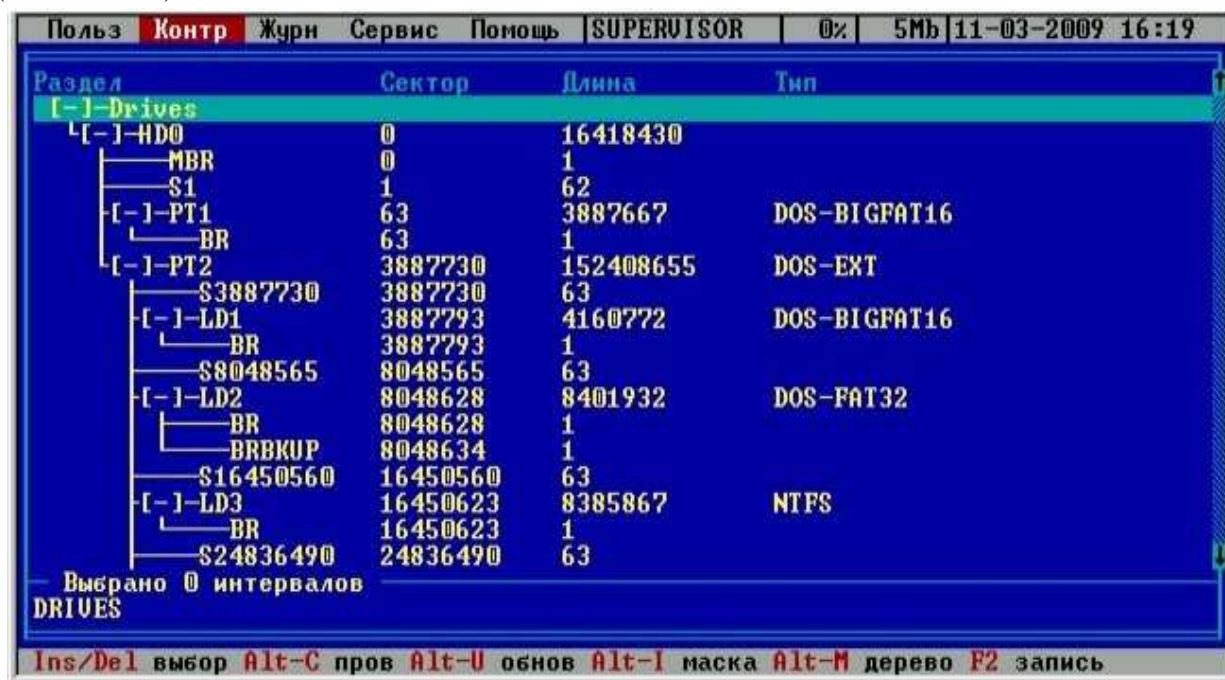


Рис. 23. Окно контроля служебных областей диска.

1.9.3 Контроль целостности файлов.

В подменю <Контроль> выберите команду <Файлы> и нажмите <Enter>. На экран выводится окно контроля файлов (Рис. 24.). СЗИ "Аккорд-АМДЗ" обеспечивает контроль целостности программ и данных до загрузки ОС, защиту от внедрения разрушающих программных воздействий (ППВ). Поддерживаются файловые системы следующих типов: FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSD, Ext2/3 FS, Sol86FS, QNXFS, MINIX.

В окне контроля файлов выводится список всех дисков установленных в системе с указанием файловой системы каждого диска. Перемещаться по списку можно клавишами <Стрелка вниз>, <Стрелка вверх>. Клавиша <Пробел> раскрывает/сворачивает дерево

каталогов на диске, или подкаталогов в каталоге. Перемещение по дереву выполняется стрелками или клавишами <Page Up> и <Page Down>. Для включения файла в список контролируемых необходимо установить на него курсор и нажать клавишу <Insert>. Для снятия отметки используется клавиша <Delete>. В список контролируемых можно вносить файлы с любых дисков, установленных в компьютере, независимо от файловой системы.

Для пересчета хэш-функций файлов используется комбинация клавиш <Alt>+<U> (обновление), для расчета хэш-функций и сравнения с данными, записанными в контроллере (для выявления измененных файлов) используется комбинация клавиш <Alt>+<C> (проверка).

Комбинация клавиш <Alt>+<M> изменяет представление на экране файлов в виде списка, либо в виде дерева.

Хэш-функция контролируемых файлов, пересчитывается при каждой загрузке компьютера с установленным контроллером "Аккорд-АМДЗ" и сравнивается с эталонным значением, записанным в памяти контроллера. Если обнаруживается несовпадение, то выдается сообщение на красном фоне "Разберитесь с ошибками" с указанием в нижней строке состояния на каком этапе выявлена ошибка ("Контроль аппаратуры" или "Контроль файлов") и загрузка компьютера блокируется для обычного пользователя, или выводится стартовое меню, если идентифицирован администратор. Администратор, запустив программу администрирования, может выполнить операцию проверки в разделе <Контроль>/<Файлы> и выявить измененные файлы.



Рис. 24. Окно контроля целостности файлов.

Примечание. Если в каталоге находятся файлы, внесенные в список контролируемых, то этот каталог нельзя свернуть клавишей <Пробел> при отображении каталогов в виде дерева.

Количество файлов, которые можно установить на контроль, зависит от операционной системы и от длины пути к каталогу, где находятся файлы. Среднее количество составляет 1200- 1500 файлов.

Для выбора файлов из папки по типу (расширению) отметьте нужный каталог с помощью мыши (левая кнопка). При нажатии на клавишу <Пробел> открывается окно дерево файлов в данном каталоге. После нажатия комбинации клавиш <Alt>+<I> выводится окно задания фильтра расширения (Рис. 25).

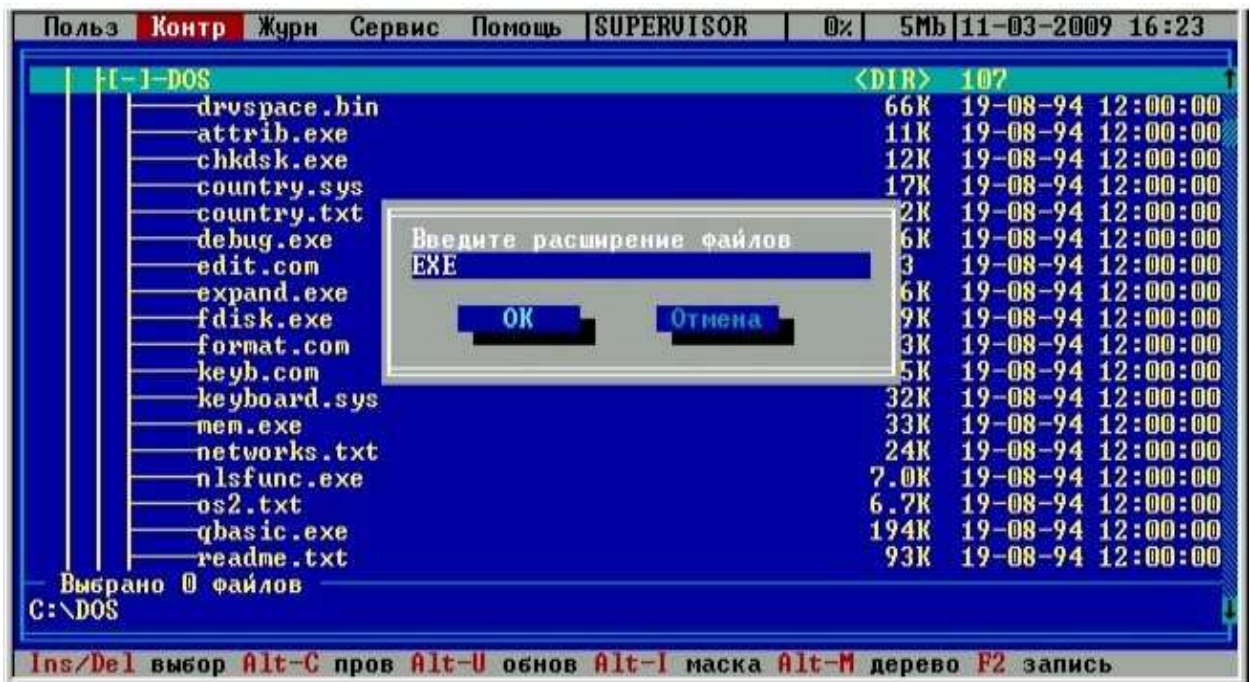


Рис. 25. Задание фильтра для выбора типа контролируемых файлов.

Фильтр можно ввести с клавиатуры в формате xxx, где xxx – расширение файла. При нажатии кнопки «ОК» или клавиши <Enter>, все файлы, удовлетворяющие заданному фильтру, будут помечены (Рис. 26). Кнопка «Отмена» или клавиша <Esc> отменяет операцию «Добавить по фильтру».



Рис. 26. Файлы, удовлетворяющие условию, отмечены для контроля.

ВНИМАНИЕ! Для отмеченных файлов расчет контрольных сумм выполняется только после комбинации клавиш <Alt>+<U> (обновление).

Еще один специфический объект контроля – это контейнер. Для формирования контейнера нужно выделить объект (в качестве объекта может выступать корневой каталог логического раздела жесткого диска, или отдельный каталог) и нажать клавишу <Insert>. После этого выводится окно выбора параметров контейнера (Рис. 27).

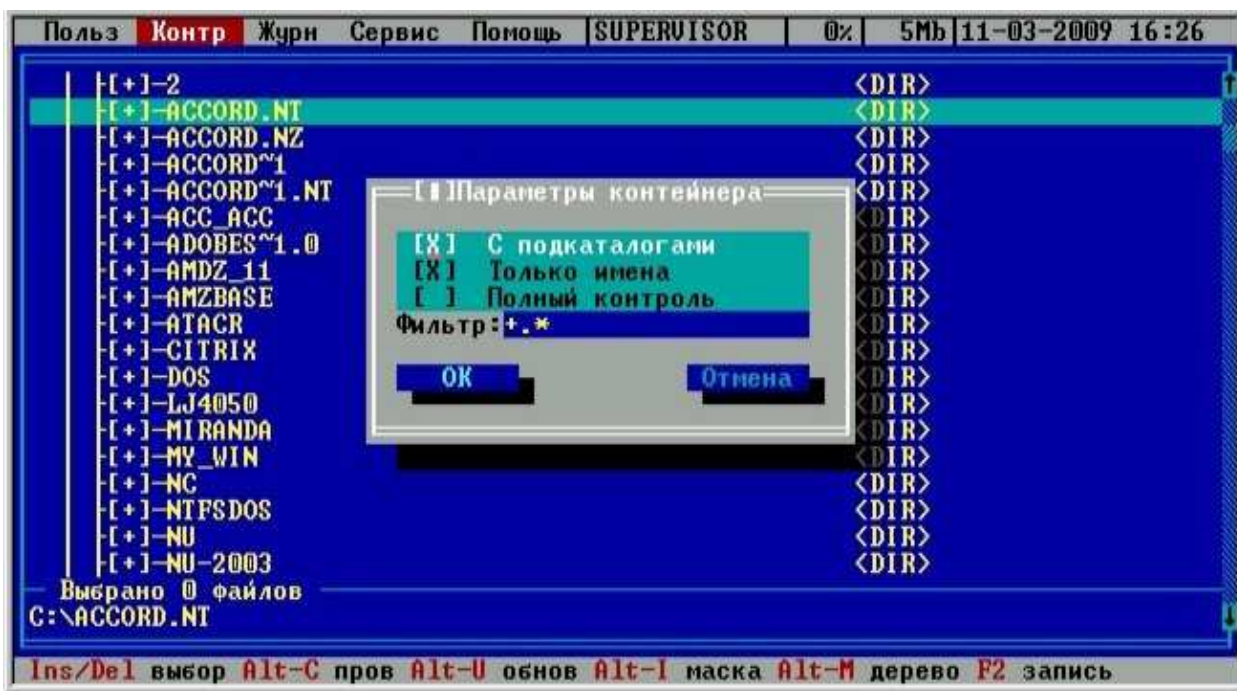


Рис. 27. Выбор параметров контейнера.

Фильтр расширений файлов может содержать одну запись «+.*», в этом случае контролируются все файлы. А можно ввести несколько расширений через точку с запятой, например, +.EXE;+.DLL;+.BAT. Процедура контроля будет существенно отличаться от обычного списка файлов.

Флаг «С подкаталогами» действует стандартно. Если включить флаг «Только имена», то контрольная сумма рассчитывается для содержимого объекта, т.е. для имен файлов в этом каталоге. Контрольная сумма содержимого самих файлов не вычисляется. В списке контролируемых объектов сохраняется одна запись с результирующей хэш-функцией. Нарушение целостности выявится при изменении состава контролируемых объектов, т.е. при удалении существующих, или добавлении новых файлов, или папок. Такая процедура контроля может успешно использоваться, если установлен режим автоматического обновления компонентов ПО из доверенного источника, а состав файлов не меняется.

Флаг «Полный контроль» добавляет следующий уровень контроля, т.е. рассчитывается хэш-функция содержимого каталога и содержимого файлов. В контейнере хранится полный список файлов с контрольной суммой для каждого объекта. При обнаружении нарушений в журнал записывается имя контейнера и имя файла, у которого не совпадает контрольная сумма с эталонным значением.

Пользоваться возможностями контроля целостности контейнера объектов следует по принципу «разумной достаточности». Можно, например, установить полный контроль на папку Windows, но следует понимать, что время расчета хэш-функции нескольких тысяч файлов будет значительным, да к тому же пользователь не сможет нормально работать на таком «защищенном» компьютере. Операционная система при работе создает некоторое количество временных файлов и при каждом новом сеансе будет выявлено нарушение целостности.

В то же время контроль целостности контейнера объектов может быть очень эффективным, когда нужно проконтролировать целостность и неизменность набора данных, необходимых для выполнения технологического процесса обработки информации. Процедура контроля будет выявлять не только изменение контрольных сумм отдельных

объектов, но также изменение состава ПО, т.е. появление новых файлов, которые изначально не предусмотрены для выполнения тех, или иных операций.

Полностью очистить список контролируемых объектов можно комбинацией клавиш <Ctrl>+<Delete>.

После добавления файлов в список и расчета контрольных сумм по <Alt>+<U> обязательно нажмите клавишу <F2> для записи обновленного списка в память контроллера.

1.9.4 Контроль целостности реестра Windows.

Данная функция позволяет контролировать целостность разделов реестра Windows 95/98 и Windows NT/2000/XP/Vista.

В подменю <Контроль> выберите команду <Реестры Windows> и нажмите <Enter>. На экран выводится окно списка контролируемых реестров. В начальный момент список пуст. Для добавления записей в список нажмите клавишу «Insert». Появится окно со списком логических разделов жесткого диска данного компьютера. Следует выбрать тот раздел, в котором установлена ОС, нажать <Пробел>. Появится дерево каталогов данного раздела. Стрелками установить курсор на каталог, в который установлена Windows, нажать <Enter> (Рис. 28).



Рис. 28. Выбор папки с установленной операционной системой.

В списке контролируемых реестров появится строчка с информацией о версии ОС. Теперь можно клавишей <Enter> раскрыть список разделов реестра (Рис. 29).



Рис. 29. Дерево разделов и ключей реестра.

Процедуры перемещения по списку, выбора, расчета контрольных сумм, проверки и сохранения аналогичны разделу «Контроль файлов».

1.9.5 Дополнительные функции меню «Контроль»

В меню «Контроль» в отдельной секции доступны несколько дополнительных функций: «Экспорт», «Импорт», «Мастер».

Процедуры Экспорта/Импорта аналогичны тем, которые используются в списке пользователей, а вот функция «Мастер» требует отдельных пояснений.

Мастер контроля целостности – это возможность установить на контроль наиболее важные с точки зрения безопасности компоненты различных операционных систем. При выборе этой команды на экране появляется окно, в котором администратор может указать тип установленной ОС (Рис. 30).

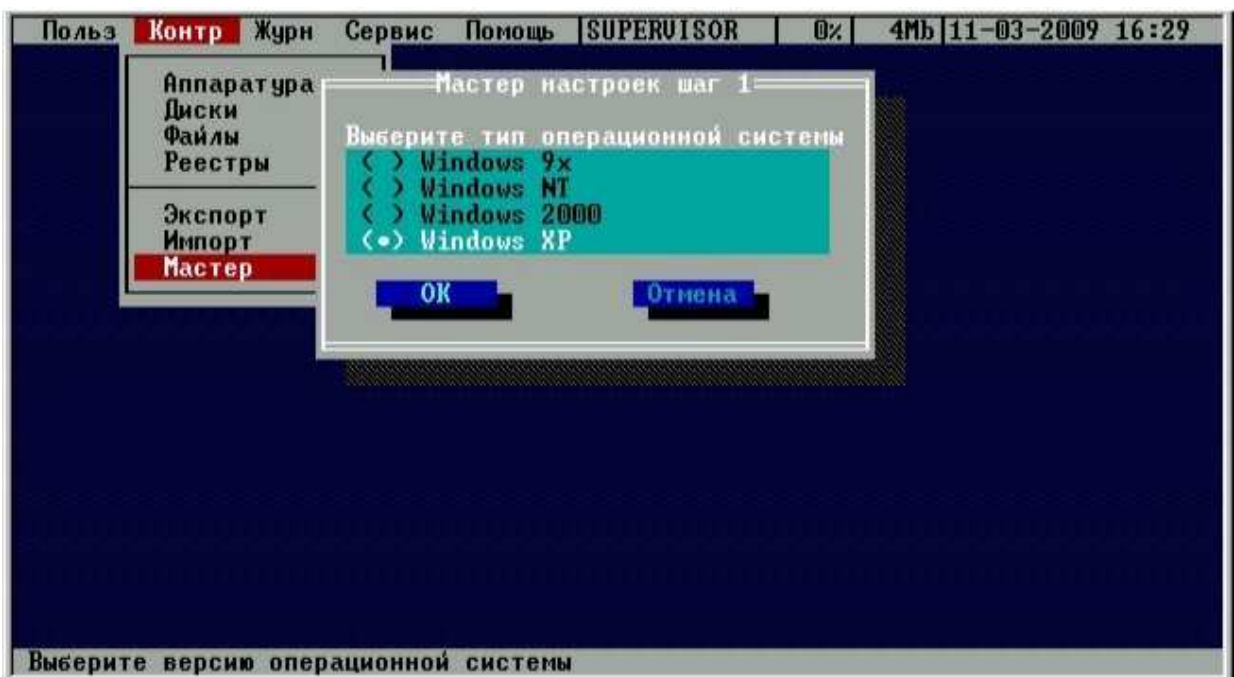


Рис. 30. Выбор типа ОС в «Мастере» контроля целостности.

Следующий шаг – указание каталога, в котором установлена операционная система (Рис. 31). Процедура аналогична выбору каталогов в разделе контроля файлов. Перемещаться по списку можно клавишами <Стрелка вниз>, <Стрелка вверх>. Клавиша <Пробел> раскрывает дерево каталогов на диске. Выбор каталога по клавише <Enter>.



Рис. 31. Выбор каталога с установленной ОС.

После этого «Мастер» выполняет анализ ключей системного реестра и поиск соответствующих файлов на жестком диске. В результате формируется общий список контролируемых объектов с контрольными суммами. Часть этих объектов выбирается на основании анализа реестра (установленные системные драйверы и приложения, стартующие при загрузке ОС), а часть из заранее сформированных шаблонов, в которые включены наиболее критичные приложения для каждой версии ОС Windows (Рис. 32).

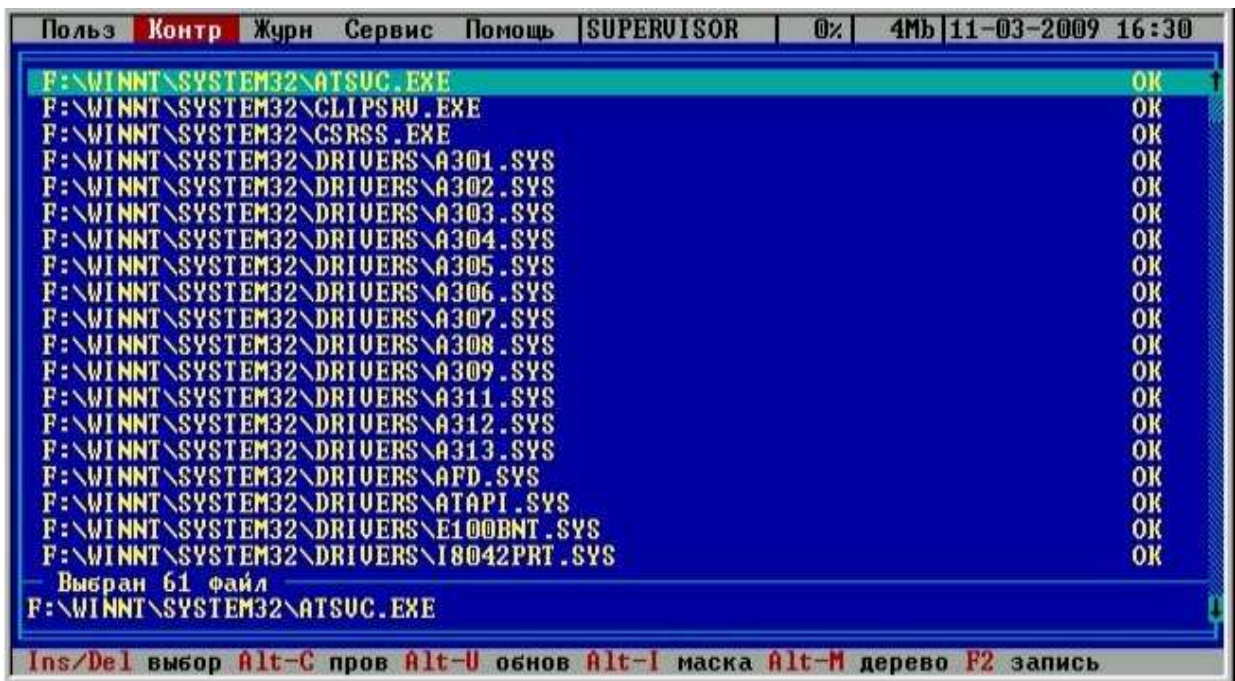


Рис. 32. Результат работы «Мастера» контроля целостности.

1.10 Системный журнал.

В энергонезависимой памяти контроллера АМДЗ ведется системный журнал. В журнал заносится информация о сеансах работы пользователей с указанием номера идентификатора и все попытки несанкционированного доступа к компьютеру.

В главном меню выберите команду <Журнал> и нажмите <Enter>. На экран выводится окно системного журнала (Рис. 33).



Рис. 33. Системный журнал контроллера.

В левой колонке выводится дата и время начала сеанса работы, а для остальных событий этого сеанса выводится только время в виде смещения от начала работы. Во второй колонке выводится наименование выполненной операции. В третьей - серийный номер идентификатора. В четвертой - результат операции. Расшифровка наименований и результатов операций дана в Приложении. В самой верхней строке экрана после имени пользователя выводится процент заполнения области памяти контроллера, отведенной под системный журнал. Если процент заполнения журнала превышает 85%, то при загрузке компьютера выдается предупреждение, но загрузка продолжается. Если процент заполнения журнала превышает 95%, то загрузка для пользователя блокируется и требуется вмешательство администратора. В окне просмотра журнала администратор по клавише <F2> может скопировать содержимое журнала в файл на гибкий диск, или ТМ-идентификатор DS1996. После этого можно стереть содержимое журнала с помощью клавиши <Delete>.

Выход из режима просмотра журнала по клавише <Esc>.

1.11 Сервис

В подменю “Сервис” пункт “*Ключ станции*” зарезервирован для использования в подсистеме распределенного аудита и управления «Аккорд-РАУ», и изменять параметры в этом пункте не рекомендуется.

Пункт “*Установки*” позволяет изменять некоторые параметры (Рис. 34):

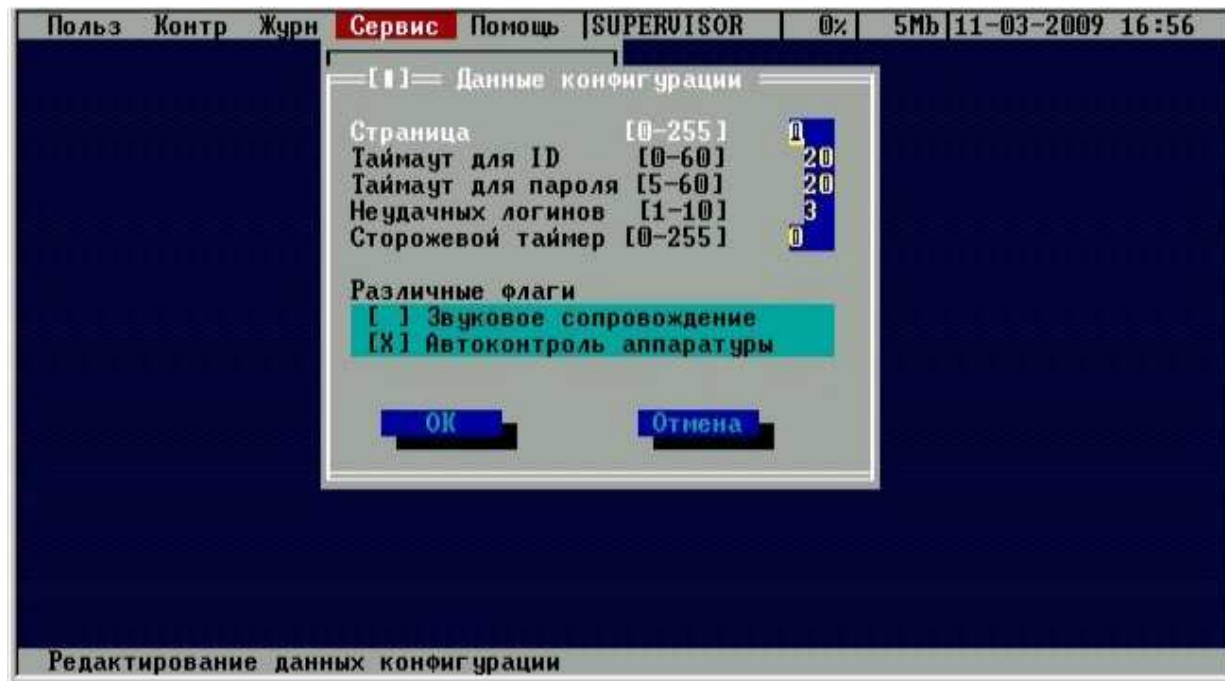


Рис. 34. Окно установок параметров конфигурации.

“**Страница**” – определяет, с какой страницы внутренней памяти персонального идентификатора располагается служебная информация СЗИ «Аккорд». Данный параметр изменять не рекомендуется. Изменение допускается, если используется ПО других производителей, которое осуществляет запись/чтение в идентификатор именно в 0-1 страницу памяти. Номер страницы должен быть четным. Идентификатор DS 1992 имеет четыре страницы памяти. Идентификаторы DS 1996 и ПСКЗИ ШИПКА имеют 256 страниц памяти.

ВНИМАНИЕ! После изменения этого параметра обязательно нужно перерегистрировать все идентификаторы пользователей с генерацией нового секретного ключа.

“**Таймаут для ID**” и “**Таймаут для пароля**” определяют интервал времени, отведенный для процедур начальной идентификации и аутентификации соответственно.

“**Сторожевой таймер**” используется только в контроллерах АМДЗ с внутренним таймером и реле управления питанием материнской платы. Этот параметр позволяет администратору установить интервал времени в секундах, необходимый для инициализации процессора, установленного на плате контроллера. Этот временной интервал определяется экспериментальным путем (на разных компьютерах он может отличаться). Если за установленный промежуток времени процессор не стартует, то срабатывает управляющее реле и один провод в шлейфе питания материнской платы, который заведен на это реле, прерывается. Этот механизм позволяет противостоять попыткам несанкционированного доступа к компьютеру с помощью выключения отдельных слотов PCI шины через настройки системного BIOS и тем самым прервать нормальную работу АМДЗ.

“Звуковое сопровождение” – включение данного флага означает, что процедура начальной идентификации/аутентификации будет сопровождаться звуковыми сигналами.

“Автоконтроль аппаратуры” определяет, что при каждом включении компьютера будет выполняться поиск новых устройств, а потом уже процедура контроля аппаратуры.

Пункт “Установки RTC” применяется только в том случае, когда на плате контроллера АМДЗ установлен таймер реального времени. При выборе этого пункта открывается окно настроек таймера (Рис. 35).

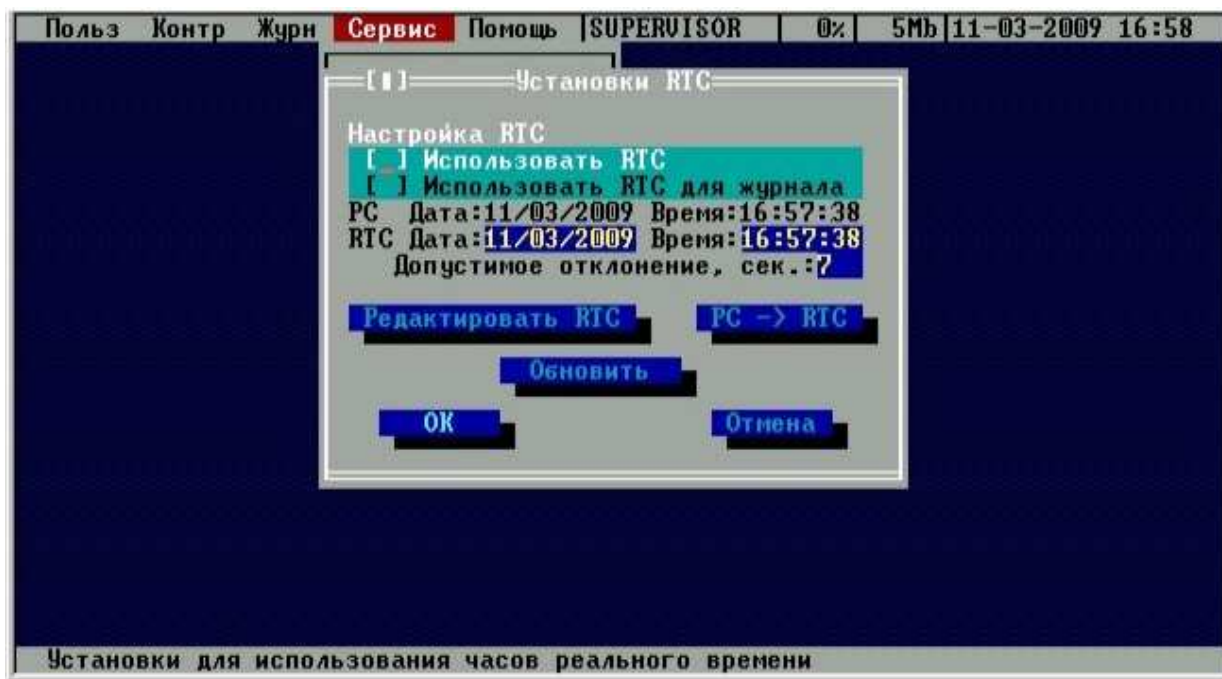


Рис. 35. Окно установок параметров таймера.

Администратор может синхронизировать внутренний таймер контроллера «Аккорд» с таймером компьютера и установить интервал допустимого отклонения. Расхождение времени больше установленного интервала определяется как попытка НСД. Этот режим может использоваться на АРМ, в которых несанкционированное изменение времени приводит к искажению информации.

Пункт меню “*Старт ACRUN*” позволяет изменять режим старта монитора безопасности подсистемы разграничения доступа из состава СПО «Аккорд NT/2000» v. 3.0. При выборе этого пункта открывается окно, в котором только один изменяемый параметр – «Не запускать ACRUN». Если администратор устанавливает флаг в этом пункте, то в процессе дальнейшей загрузки ОС монитор безопасности при наличии этого флага не стартует. Данные о включенном параметре «Не запускать ACRUN» сохраняются в памяти процессора только на один сеанс работы, т.е. по умолчанию при старте компьютера этот флаг выключен. Данная опция корректно работает только с теми релизами СПО «Аккорд NT/2000» v. 3.0, которые выпущены после января 2010 года.

2. ВЫХОД ИЗ ПРОГРАММЫ.

Выход из программы администрирования выполняется по клавише <Esc>, когда Вы находитесь в главном меню. После этого на экране снова появляется стартовое меню администратора (Рис.18.). Администратор может выбрать вариант загрузки или перезагрузить компьютер. При корректном входе в систему идентификатором пользователя меню не выводится, а выполняется загрузка установленной операционной системы с жесткого диска. Загрузка с любых сменных носителей для пользователя запрещена.

Приложение 1.

Наименование и результат операций в системном журнале.

Сокращение	Название операции
НС	Начало сеанса
ИА	Идентификация/аутентификация
КА	Контроль аппаратуры
КФ	Контроль файлов
КС	Контроль сектора
КИ	Контроль INI файла
КР	Контроль реестра
ЖС	Создание журнала
РД	Изменение полномочий пользователя
Сокращение	Результат операции
ОК	Успешное завершение
ULST	Создание списка пользователей
ИД	Незарегистрированный идентификатор
ТИД	Истекло время предъявления идентификатора
IPSW	Неправильный пароль
TPSW	Истекло время ввода пароля
NFIL	Файл не существует.
Stah	Изменился размер файла.
sTah	Изменилась дата создания файла.
stAh	Изменились атрибуты файла.
staH	Изменилась контрольная сумма.
STah	Изменились размер, дата создания файла.
StAh	Изменились размер, атрибуты файла.
StaH	Изменились размер, контрольная сумма файла.
sTAh	Изменились дата создания, атрибуты файла.
sTaH	Изменились дата создания, контрольная сумма.
stAH	Изменились атрибуты, контрольная сумма.
STAh	Изменились размер, дата создания, атрибуты файла.
StAH	Изменились размер, атрибуты, контрольная сумма файла.
STaH	Изменились размер, дата, контрольная сумма файла.
sTAN	Изменились дата, атрибуты, контрольная сумма файла.
STAN	Изменились размер, дата, атрибуты, контрольная сумма файла.
TIMR	Запрещённое время
IDE	Изменилась контрольная сумма, жесткий магнитный диск
CMOS	Изменилась контрольная сумма, данные CMOS
CPU	Изменилась контрольная сумма, процессор
PCI	Изменилась контрольная сумма, PCI устройство
MEM	Изменилась контрольная сумма, оперативная память
ПСЗД	Создание пользователя
ПУДП	Удаление пользователя
ППЕР	Переименование пользователя
ППРД	Изменение прав пользователя
ГСЗД	Создание группы
ГУДЛ	Удаление группы
ГПЕР	Переименование группы
ГПРД	Изменение прав группы
ОКРС	Успешное изменения пароля пользователя