ОКБ АПР
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

Программно-аппаратный комплекс защиты информации от НСД для ПЭВМ (PC)
«Аккорд-АМДЗ»
(Аппаратный модуль доверенной загрузки)

Руководство администратора

11443195.4012.006 90 04

Листов 48

Москва
2014

АННОТАЦИЯ

Настоящий документ является руководством администратора программно-аппаратного комплекса средств защиты информации от НСД – аппаратного модуля доверенной загрузки – «Аккорд-АМДЗ», далее по тексту «Аккорд-АМДЗ», и предназначен для лиц, планирующих и организующих защиту информации с их использованием в системах и средствах информатизации на базе ПЭВМ.

В документе приведены основные функции и особенности эксплуатации комплексов СЗИ НСД «Аккорд-АМДЗ», работающих на основе контроллеров Аккорд-5MX, Аккорд-5.5, Аккорд-5.5e, Аккорд-5.5MP, Аккорд-5.5ME.

Перед установкой и эксплуатацией комплексов СЗИ НСД «Аккорд-АМДЗ» необходимо внимательно ознакомиться с комплектом эксплуатационной документации на комплекс, а также принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных средств комплексов должно дополняться общими мерами технической безопасности.

СОДЕРЖАНИЕ

ПРИНЯТЫЕ ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

Администратор БИ (или АБИ) – администратор безопасности информации, привилегированный пользователь – должностное лицо, имеющее особый статус и абсолютные полномочия (супервизора). Администратор БИ планирует защиту информации на предприятии (учреждении, фирме и т.д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует установку комплекса в СВТ, эксплуатацию и контроль правильности использования СВТ с внедренным комплексом «Аккорд», в том числе, учет выданных идентификаторов, осуществляет периодическое тестирование средств защиты комплекса

Доверенная загрузка – загрузка ОС только после проведения контрольных процедур идентификации/аутентификации пользователей, проверки целостности технических и программных средств СВТ с использованием алгоритма пошагового контроля целостности.

Идентификатор – персональный идентификатор пользователя – микропроцессорное устройство DS1992 – DS1996 («Touch memory», далее по тексту – ТМ-идентификатор) или устройство ПСКЗИ ШИПКА.

Пользователь – субъект доступа к объектам (ресурсам) СВТ.

Объект доступа – под объектом доступа понимается один из перечисленных ресурсов СВТ: диск, каталог, файл, процесс (задача).

Меню – окно с изображением кнопок с названиями команд.

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.

Ошибки – информация, выводимая на дисплей, указывающая на неправильность действий, сбои, аварии комплекса.

Пояснения – замечания в описании некоторых команд, содержащие рекомендации администратору БИ по порядку использования этих команд. Пояснения выделены мелким шрифтом.

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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АМДЗ	Аппаратный модуль доверенной загрузки
АБИ	Администратор безопасности информации
АС	Автоматизированная система
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПК	Персональный компьютер
ПО	Программное обеспечение
ПРД	Правила (политики) разграничения доступа
ПСКЗИ	Персональное средство криптографической защиты информации
ПЭВМ	Персональная электронно-вычислительная машина
РС	Рабочая станция
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
ТУ	Технические условия
ЭНП	Энергонезависимая память

1. Общие сведения

1.1. Назначение комплекса

Комплекс СЗИ НСД «Аккорд-АМДЗ» представляет собой аппаратный модуль доверенной загрузки (АМДЗ) для IBM-совместимых ПК – серверов и рабочих станций локальной сети, обеспечивающий защиту устройств и информационных ресурсов от НСД, идентификацию, аутентификацию пользователей, регистрацию их действий, контроль целостности файлов и областей HDD (в том числе и системных) при многопользовательском режиме их эксплуатации.

Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера – до загрузки операционной системы, и обеспечивает доверенную загрузку[1] ОС, использующих одну из поддерживаемых файловых систем. Это, в частности, ОС типа MS-DOS, ОС семейства Windows, QNX, OS/2, UNIX, LINUX, BSD и др.

Все модификации комплекса поддерживают файловые системы FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX.

Комплекс представляет собой совокупность технических и программных средств, предназначенных для выполнения основных функций защиты от НСД ПЭВМ (АС) на основе:

- применения персональных идентификаторов пользователей;
- парольного механизма;
- блокировки загрузки операционной системы со съемных носителей информации;
- контроля целостности технических средств и программных средств (файлов общего, прикладного ПО и данных) ПЭВМ (АС);
- обеспечения режима доверенной загрузки установленных на ПЭВМ (АС) операционных систем, использующих любую из поддерживаемых комплексом файловых систем.

Комплекс СЗИ НСД для ПЭВМ (РС) «Аккорд-АМДЗ» обеспечивает:

- защиту ресурсов ПЭВМ (РС) от лиц, не допущенных к работе на ней, на основе идентификации пользователей ПЭВМ (РС) по персональным идентификаторам до загрузки операционной системы (ОС);
- аутентификацию пользователей ПЭВМ (РС) по паролю длиной до 12 символов, вводимому с клавиатуры с защитой от раскрытия пароля - до загрузки операционной системы (ОС);

[1)] подробнее см. раздел «Принятые термины, обозначения и сокращения» настоящего документа

– блокировку загрузки с отчуждаемых носителей (FDD, CD/DVD-ROM, ZIP, USB-накопителей и др.);

– контроль целостности технических, программных средств, условно-постоянной информации ПЭВМ (PC) до загрузки ОС, с реализацией пошагового алгоритма контроля;

– доверенную загрузку системного и прикладного ПО при одновременной установке на дисках или в логических разделах диска ПЭВМ (PC) нескольких ОС;

– регистрацию на ПЭВМ (PC) до 126 пользователей;

– регистрацию контролируемых событий в системном журнале, размещенном в энергонезависимой памяти контроллера;

– возможность физической коммутации управляющих сигналов периферийных устройств, в зависимости от уровня полномочий пользователя, позволяющей управлять вводом/выводом информации на отчуждаемые физические носители и устройства обработки данных;

– администрирование встроенного ПО комплекса (регистрацию пользователей и персональных идентификаторов, назначение файлов для контроля целостности, контроль аппаратной части ПЭВМ (PC), просмотр системного журнала);

– регистрацию, сбор, хранение и выдачу данных о событиях, происходящих в ПЭВМ (PC) в части системы защиты от несанкционированного доступа в ЛВС.

Идентификация и аутентификация пользователей, контроль целостности технических и программных средств ПЭВМ (PC) выполняются контроллером комплекса до загрузки операционной системы, установленной в ПЭВМ (PC).

Комплекс обеспечивает выполнение основных функций защиты от НСД как в составе локальной ПЭВМ, так и на рабочих станциях ЛВС в составе комплексной системы защиты от НСД ЛВС, в том числе, настройку, контроль функционирования и управление комплексом.

Комплекс СЗИ НСД «Аккорд-АМДЗ» разработан ОКБ САПР на основании лицензий ФСТЭК и ФСБ РФ. Комплекс производится на аттестованном производстве.

1.2. Состав комплекса

Комплекс СЗИ НСД «Аккорд-АМДЗ» включает в себя программные и аппаратные средства.

1.2.1. Аппаратные средства

Аппаратные средства комплекса СЗИ НСД «Аккорд-АМДЗ» (ТУ 4012-006-11443195-97 04) включают в себя:

– ***одноплатный контроллер*** - представляет собой карту расширения (expansion card), устанавливаемую в свободный слот материнской платы ПЭВМ (PC). Контроллер изготовлен по современной технологии многослойных печатных плат с покрытием химическим золотом с использованием наиболее современной элементной базы, является универсальным, не требует замены при смене используемого типа операционной системы (ОС). В контроллере комплекса аппаратно реализована работа с каналом Touch Memory, что обеспечивает надежную работу с идентификаторами DS-199x на всех типах ПЭВМ (PC). На контроллеры серии 5.5 по заказу может устанавливаться процессор с USB-хостом и разъем mini-USB, что позволяет использовать в качестве идентификатора ПСКЗИ ШИПКА.

– ***съемник информации с контактном устройством***, обеспечивающий интерфейс между контроллером комплекса и персональным идентификатором пользователя.

– ***персональный идентификатор пользователя*** – микропроцессорное устройство DS 199x («Touch memory»), или USB-устройство ПСКЗИ ШИПКА. Каждый идентификатор обладает уникальным номером (48 бит), который формируется технологически. Объем памяти, доступной для записи и чтения зависит от типа идентификатора. Подробнее о порядке использования персональных идентификаторов см. п. «Идентификаторы» «Руководства по установке» (11443195.4012-006 98), входящего в комплект поставки комплекса.

Количество и тип идентификаторов, модификация контроллера и контактного устройства оговаривается при поставке комплекса и указываются в Формуляре (11443195.4012-006 ФО).

1.2.2. Программные средства

В состав программных средств, размещенных в энергонезависимой памяти контроллера комплекса, входят:

1) BIOS контроллера комплекса «Аккорд-АМДЗ»;

2) программное обеспечение АМДЗ в составе следующих функциональных модулей:

– средства идентификации пользователей;

– средства аутентификации пользователей;

– средства контроля целостности технических средств ПЭВМ (PC);

– средства контроля целостности системных областей жесткого диска;

– средства контроля целостности программных средств;

– средства контроля целостности отдельных ветвей реестра (для ОС семейства Windows);

– средства аудита (работа с журналом регистрации событий);

– средства администрирования комплекса.

Доступ к средствам администрирования и аудита комплекса предоставляется только администратору БИ.

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.

1.3. Технические условия применения комплекса

Все модификации комплекса «Аккорд-АМДЗ»:

- могут использоваться в составе ПЭВМ с центральным процессором архитектуры x86 (IA-32) или x86-64 (AMD64), с объемом динамической оперативной памяти (RAM) не менее 128 Мб, при наличии свободного разъема на материнской плате ПЭВМ, соответствующего типу специализированного контроллера АМДЗ;
- обеспечивают многопользовательский режим эксплуатации ПЭВМ с возможностью регистрации до 126 пользователей на одной ПЭВМ;
- предполагают наличие на ПЭВМ любой из ОС, использующей поддерживаемую комплексом файловую систему.

При модификации внутреннего ПО замена контроллера не требуется. При этом обеспечивается поддержка спецрежима (технологического режима контроллера, подробнее см. «Руководство по установке» 11443195.4012-006 98) программирования без снижения уровня защиты.

Технические средства защищаемой ПЭВМ не должны содержать аппаратно-программных механизмов, ориентированных на целенаправленное нарушение правильности функционирования комплекса. . В составе ПЭВМ (РС), в котором установлен комплекс СЗИ НСД, должны отсутствовать средства, позволяющие за счет воздействия со стороны пользователей на штатные органы управления ПЭВМ (РС) воспрепятствовать передаче управления комплексу стандартной процедурой ROM Scan.

1.4. Организационные меры, необходимые для применения комплекса

Для эффективного применения средств защиты комплекса и поддержания необходимого уровня защищенности ПЭВМ (АС) и информационных ресурсов требуется:

- наличие администратора безопасности информации (супервизора; далее по тексту – Администратор БИ) – привилегированного пользователя, имеющего особый статус и абсолютные полномочия. Администратор БИ планирует защиту информации на предприятии (учреждении, фирме и т.д.), определяет права доступа пользователям в соответствии с утвержденным Планом защиты, организует установку комплекса в СВТ(РС), эксплуатацию и контроль правильности использования СВТ(РС) с внедренным комплексом «Аккорд», в том числе, учет выданных идентификаторов, осуществляет 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 СБИ (администратора БИ) получили юридическую основу;
- физическая охрана СВТ (АС) и ее средств, в том числе проведение мероприятий по недопущению изъятия контроллера Комплекса;
- использование в СВТ (АС) технических и программных средств, сертифицированных как в Системе ГОСТ Р, так и в Государственной системе защиты информации (ГСЗИ);
- периодическое тестирование средств защиты комплекса.

2. Установка и настройка комплекса

Установка и настройка комплекса СЗИ НСД «Аккорд-АМДЗ» осуществляется администратором безопасности информации и включает в себя:

1) Установку платы контроллера в свободный слот ПЭВМ и подсоединение контактного устройства (съемника информации) – см. «Руководство по установке» (11443195.4012-006 98).

2) Регистрацию администратора БИ (супервизора), в том числе, настройку комплекса в соответствии с конфигурацией технических средств ПЭВМ (подробнее см. «Руководство по установке» и подраздел 3.5 настоящего руководства).

3) Регистрацию пользователей и настройку защитных средств комплекса (подробнее см. соответствующие подразделы раздела 3 настоящего руководства).

3. Работа с программой

3.1. Общие сведения

Если в компьютер устанавливается новый контроллер «Аккорд-АМДЗ», то при загрузке выполняется инициализация и форматирование внутренней памяти. После завершения этой операции на экран выводится стартовое меню администратора (рисунок 1).

Поскольку в контроллере нет зарегистрированных пользователей, то в этом меню доступны для выбора только пункты «Администрирование» и «Выход в AcDOS».

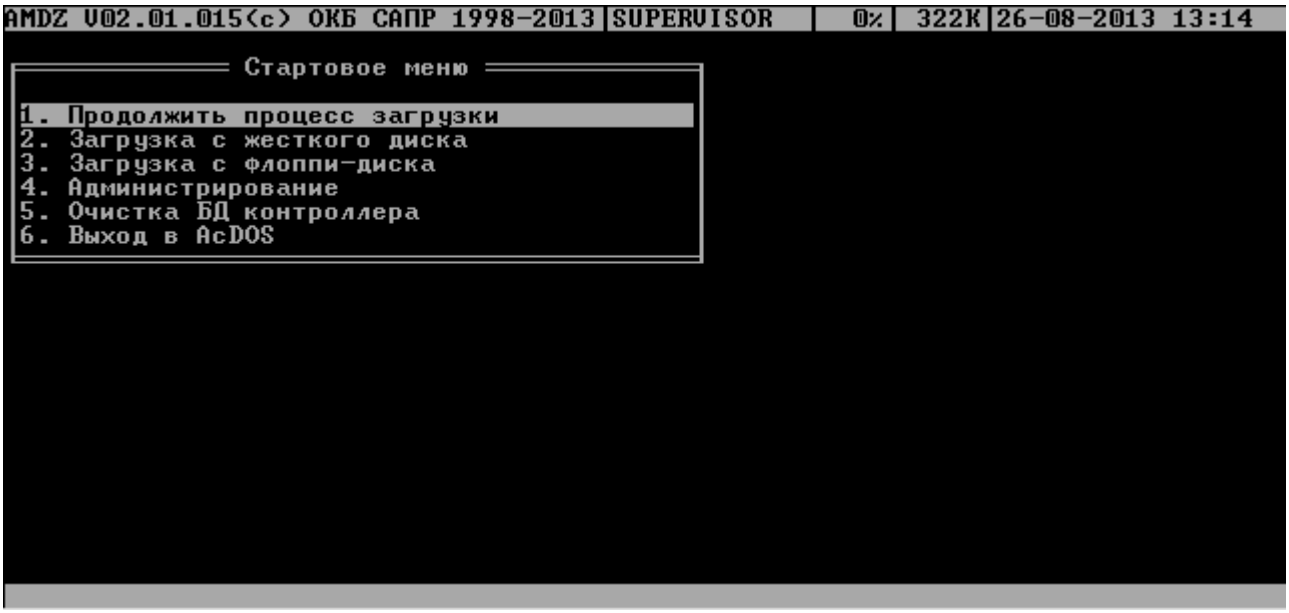

Рисунок 1 - Стартовое меню администратора

«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 (рисунок 2).

Рисунок 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.

3.2. Список пользователей

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

Рисунок 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 выполнятся 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.

3.3. Общие параметры группы «Администраторы»

Для группы «Администраторы» установлены следующие общие параметры (рисунок 4):

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

Рисунок 4 - Общие параметры группы «Администраторы»

3.3.1. Параметры пароля

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

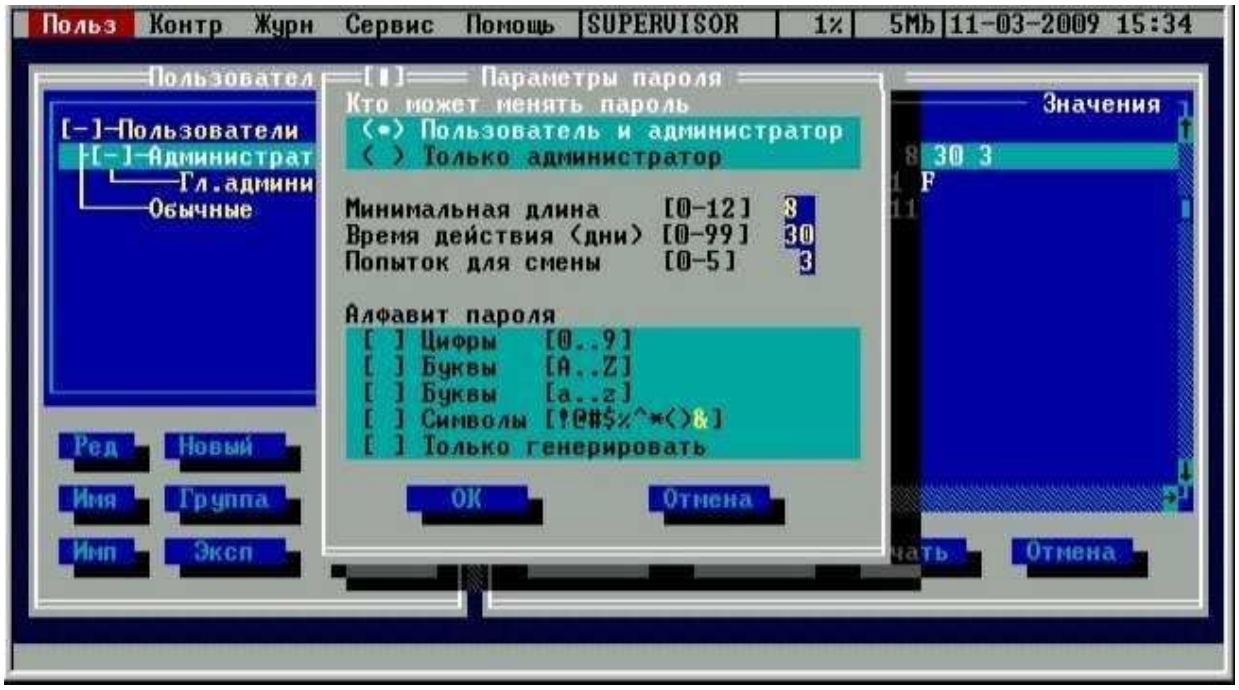

Рисунок 5 - Параметры пароля

– «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 366 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 задать и подтвердить новый пароль).

– «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.

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

3.3.2. 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 (рисунок 6).

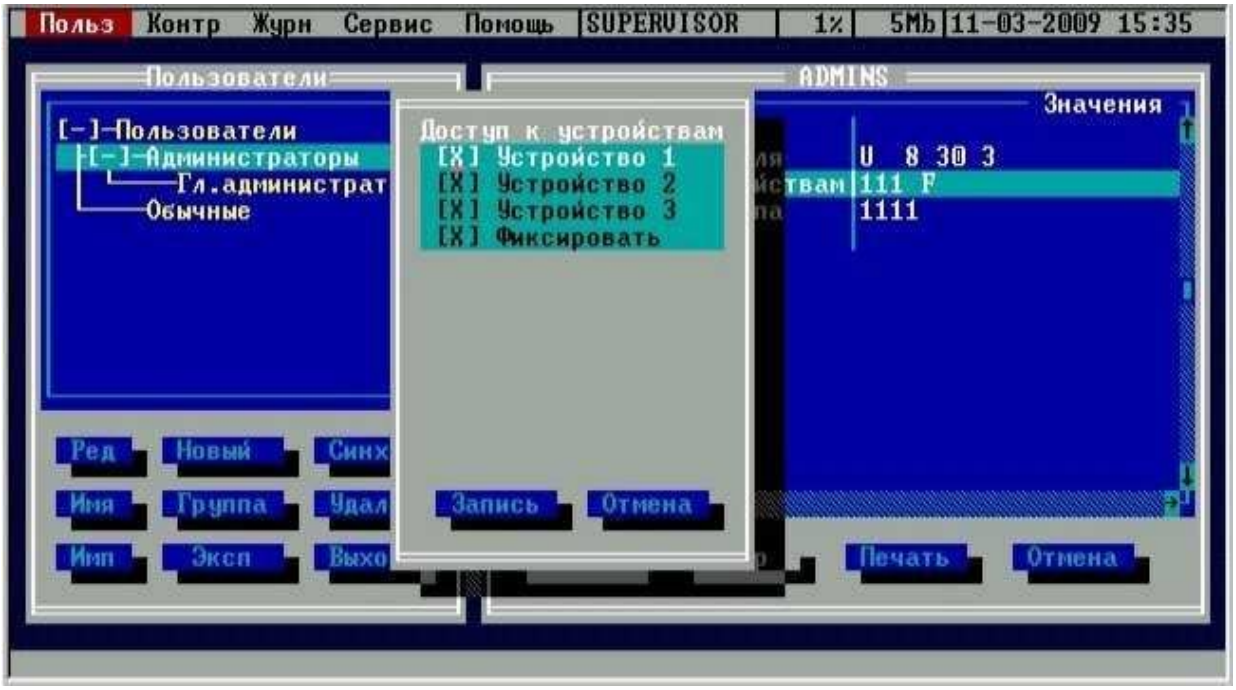

Рисунок 6 - Функция управления внешними устройствами

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».

3.3.3. Атрибуты доступа

При выборе параметра «Атрибуты доступа» открывается окно (рисунок 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.

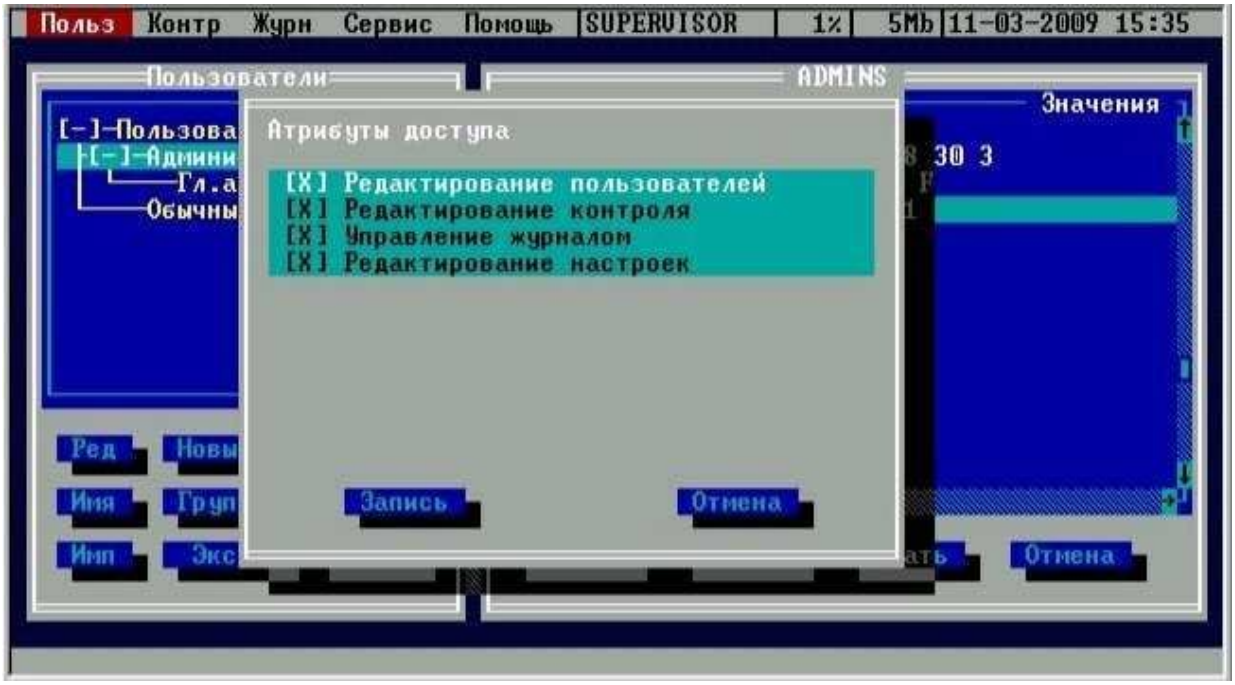

Рисунок 7 - Выбор атрибутов доступа администратора к функциям управления

3.3.4. 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 (рисунок 8) предполагают использование только контроллера АМДЗ.

Рисунок 8 - Результаты ИА

3.4. Общие параметры группы «Обычные» (пользователи)

Для группы «Обычные» (пользователи) установлены следующие общие параметры (рисунок 9):

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

Рисунок 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.

3.4.1. 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>.

3.4.2. 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» (рисунок 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.

Рисунок 10 - Временные ограничения на загрузку компьютера

3.4.3. 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) (рисунок 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.

Рисунок 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.

3.5. Регистрация супервизора (администратора безопасности информации)

При инициализации контроллера в базе данных создается учетная запись Главного Администратора – «Гл. администратор» – которому будут полностью доступны все функции администрирования. Но при этом поля этой записи не заполнены.

ВНИМАНИЕ! При первом старте контроллера прежде всего необходимо установить параметры учетной записи для пользователя «Гл.Администратор» и только после этого перейти к процедуре регистрации всех остальных пользователей.

Для ввода параметров учетной записи администратора системы следует выбрать строку <Гл. администратор>, нажать <Enter>. На экран выводится окно ввода-вывода «Параметры пользователя» (рисунок 12), в котором далее следует выполнить процедуру назначения идентификатора (см. пункт 3.5.1).

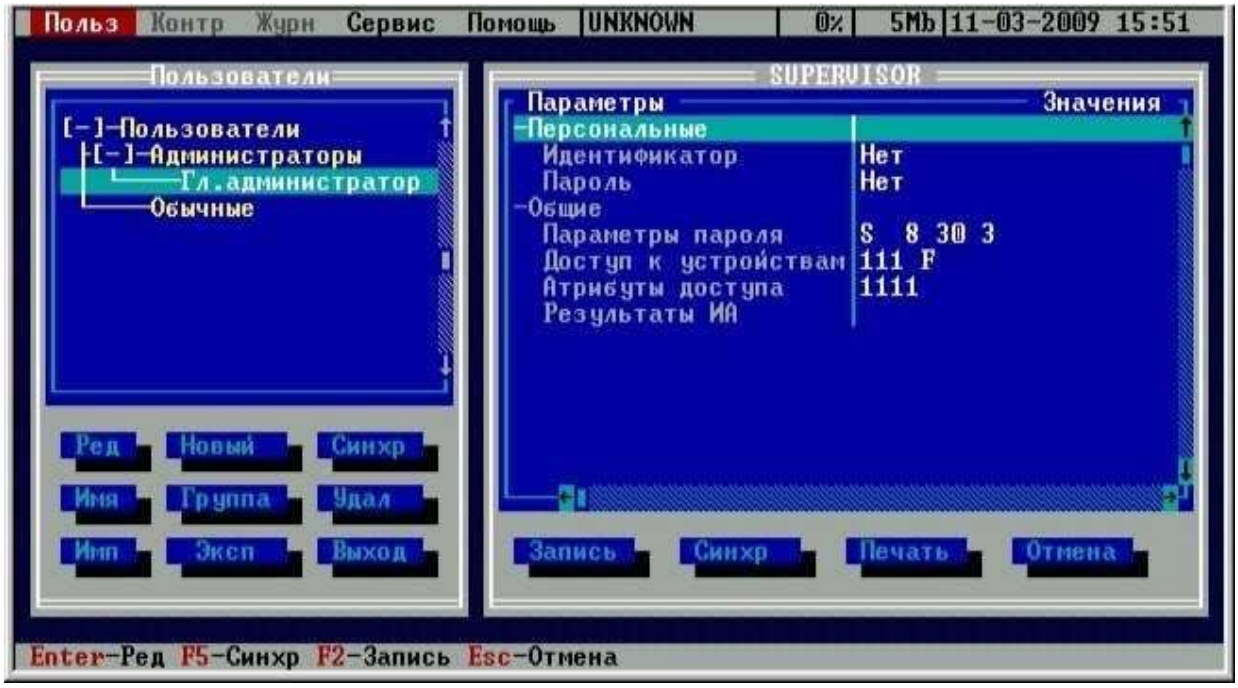

Рисунок 12 - Регистрация пользователя «Гл.Администратор»

3.5.1. Назначение персонального идентификатора

Для начала выполнения процедуры регистрации персонального идентификатора в окне параметров пользователя следует выбрать строку <Идентификатор> (рисунок 12). На экран выводится информация о текущем идентификаторе (рисунок 13).

При первой установке контроллера никаких данных об идентификаторе нет (рисунок 13). Выберите команду <Новый>.

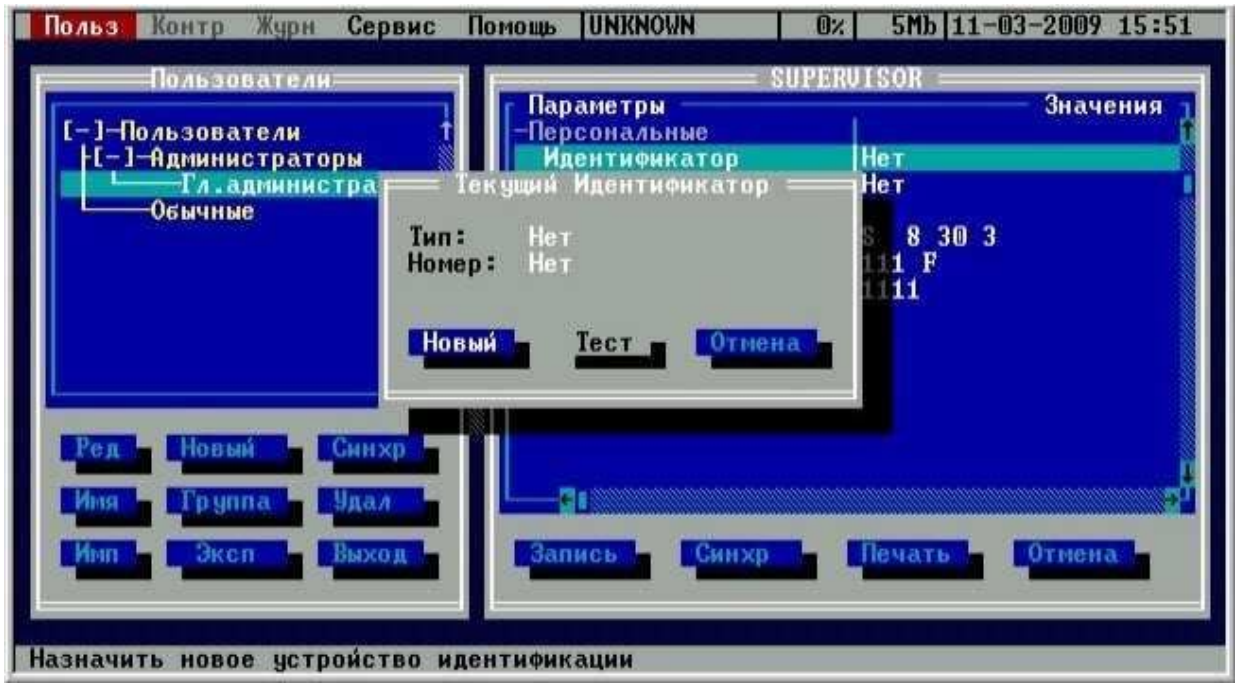

Рисунок 13 - Информация об идентификаторе

На запрос идентификатора (рисунок 14) прикоснитесь идентификатором к съемнику. Для отмены текущей операции выберите команду <Отмена>.

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, следует вставить карту в считыватель.*

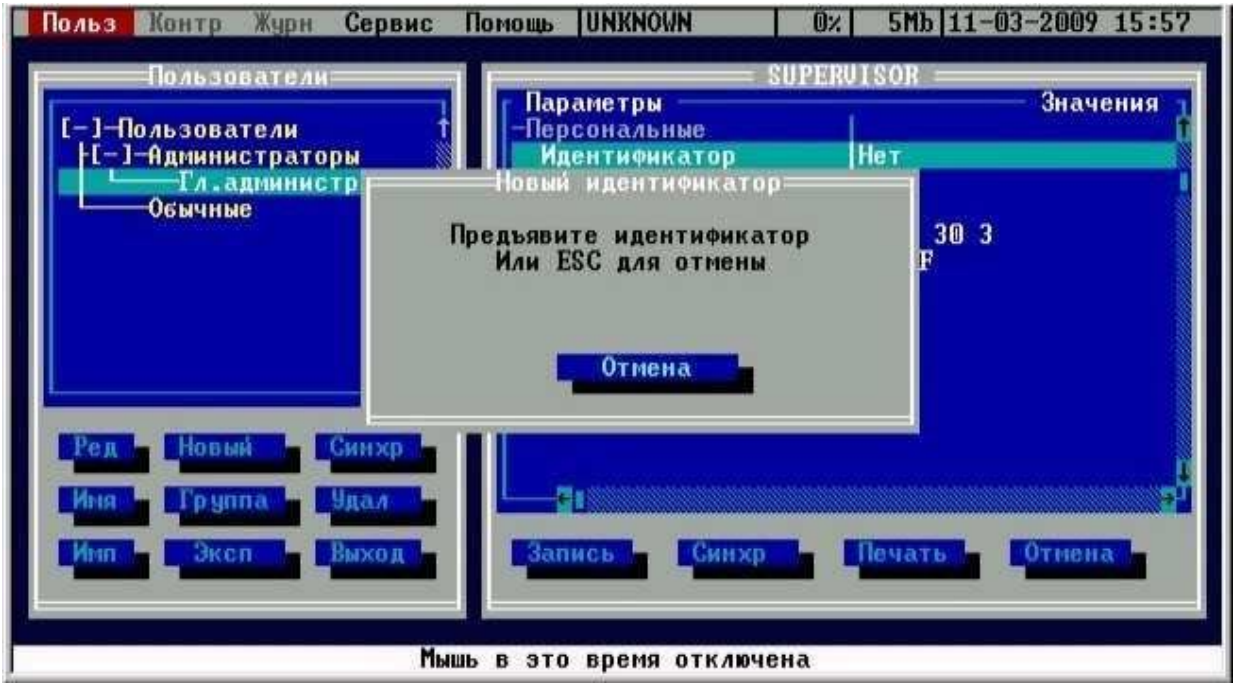

Рисунок 14 - Запрос идентификатора

После предъявления идентификатора на экране появляется окно, в котором требуется указать, какой секретный ключ будет использоваться (рисунок 15).

Секретный ключ 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! Генерировать секретный ключ следует только ***при первой регистрации***, т.к. при каждой генерации перезаписывается предыдущий ключ, и идентификатор не будет читаться на других компьютерах.

При работе с одним и тем же идентификатором на нескольких комплексах «Аккорд» в процессе каждой последующей регистрации идентификатора следует использовать существующий секретный ключ (сгенерированный в процессе первой регистрации идентификатора).

Выберите опцию <Новый> и нажмите кнопку <OK>. На запрос идентификатора подключите идентификатор к контактному устройству.

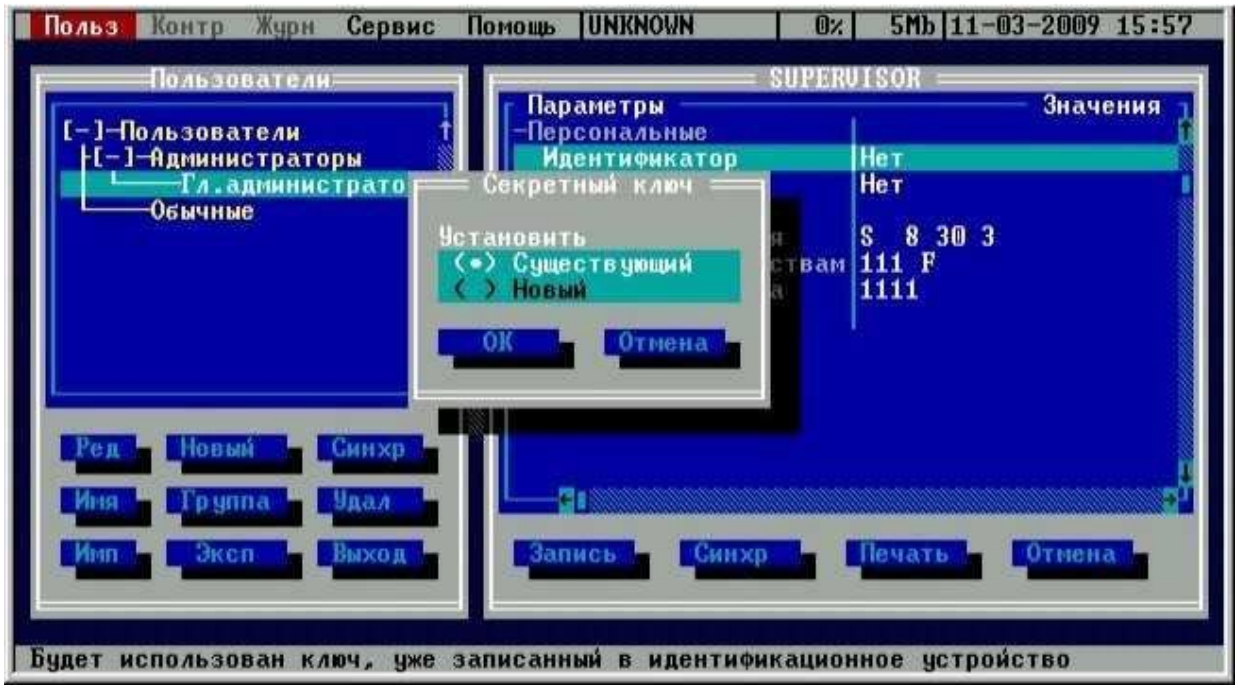

Рисунок 15 - Генерация секретного ключа пользователя

После успешного выполнения процедуры назначения идентификатора следует перейти к процедуре назначения пароля (см. пункт 3.5.2).

3.5.2. Назначение пароля

В окне «Параметры пользователя» (рисунок 12) выберите строку «Пароль» и нажмите <Enter>. На экран выводится окно ввода пароля (рисунок 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.

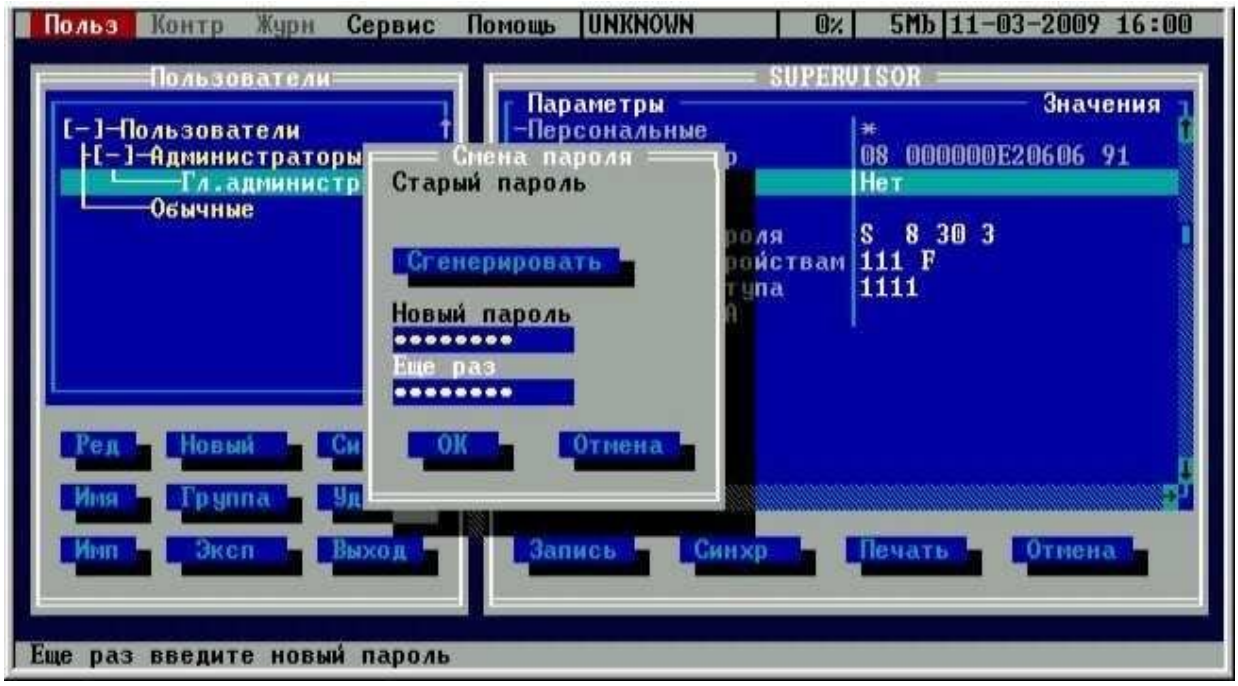

Рисунок 16 - Окно ввода пароля

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» (рисунок 17). После генерации новый пароль выводится в строке «Новый пароль» и пользователь должен его ввести с клавиатуры в поле «Ещё раз».

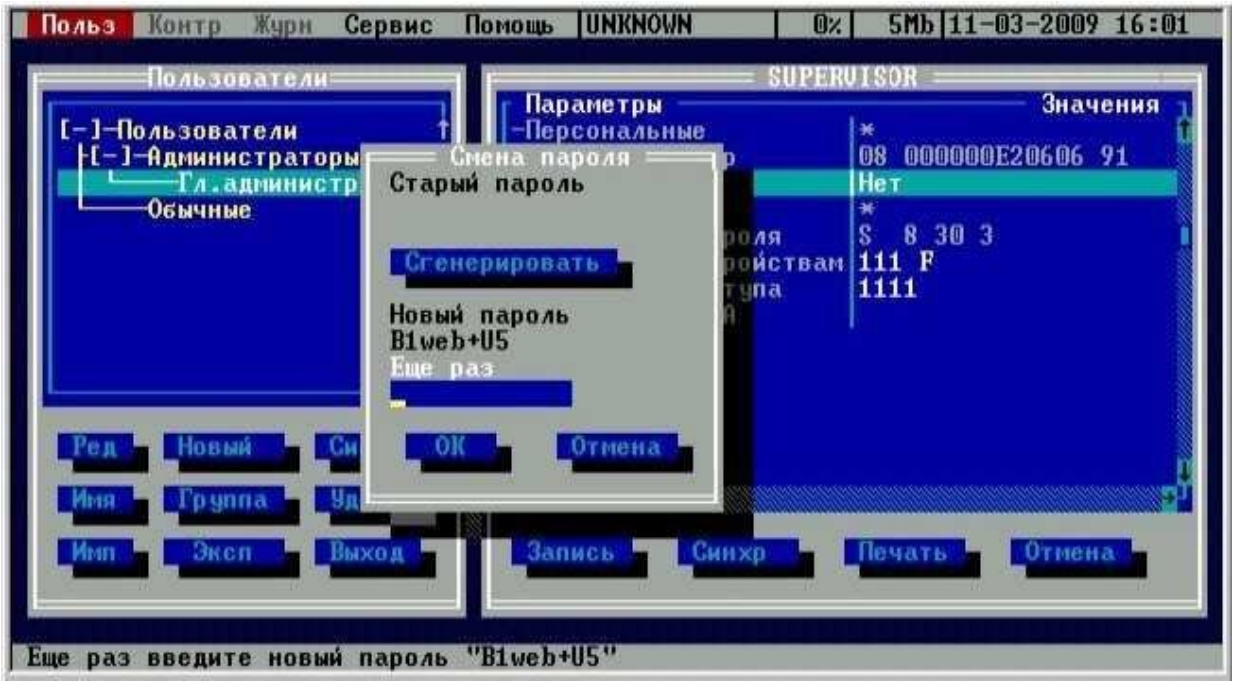

Рисунок 17 - Случайная генерация пароля

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 стартовое меню администратора, в котором уже доступны все пункты, в частности выбор вариантов загрузки ОС (рисунок 1).

Для дальнейшей настройки комплекса выберите пункт меню «Администрирование».

3.6. 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).

ВНИМАНИЕ! Если контроллер АМДЗ используется в составе комплекса «Аккорд NT/2000» v. 3.0, «Аккорд-Win32» или «Аккорд-Win64», то регистрацию пользователя следует выполнять только ПОСЛЕ установки СПО на жесткий диск и считывания из идентификатора с красным стикером ключевого файла лицензии.

3.7. Удаление пользователя из списка

В подменю списка пользователей (рисунок 3) выберите и пометьте имя пользователя, предназначенного для удаления из списка. Нажмите клавишу <Del>, подтвердите удаление. Пользователя <Гл.Администратор> нельзя удалить из списка.

3.8. Редактирование параметров пользователей

В этом режиме администратор производит изменение параметров доступа пользователя к объектам СЗИ. В подменю списка пользователей (рисунок 3) выберите имя пользователя, параметры которого необходимо отредактировать, нажмите клавишу <Enter>. На экран выводится окно (рисунок 18). Произведите изменения в окне ввода/вывода «Параметры пользователя».

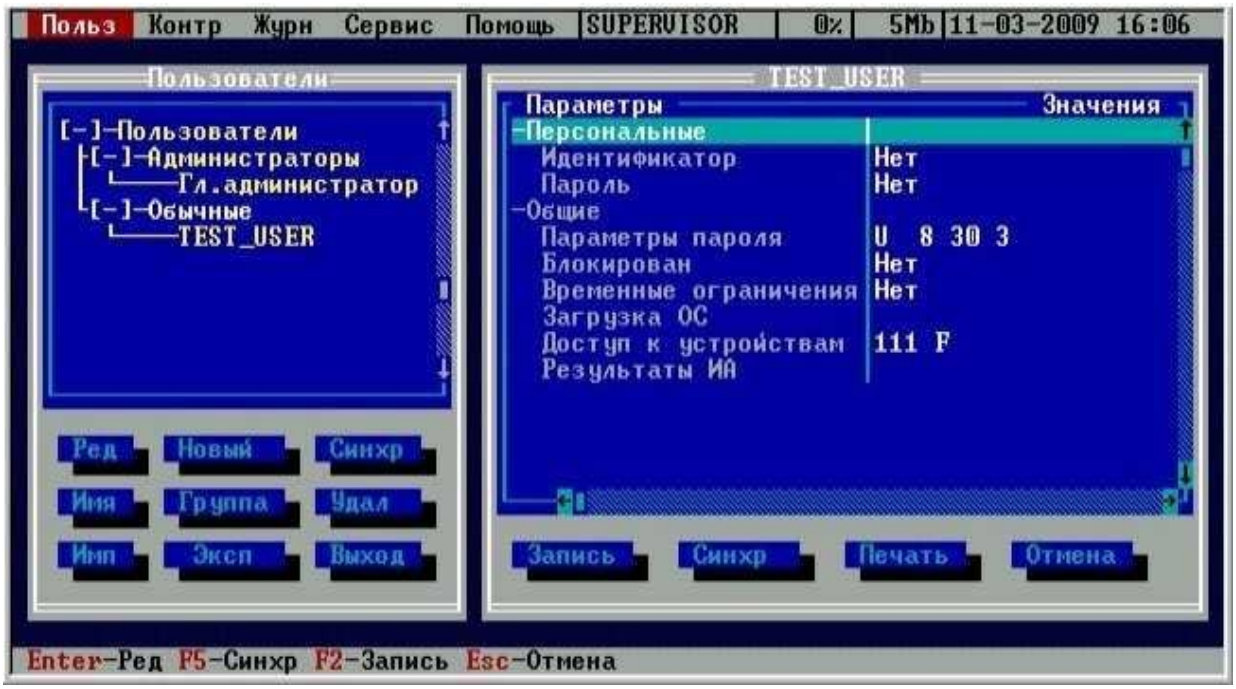

Рисунок 18 - Редактирование параметров пользователя

3.9. Создание новой группы пользователей

Для выполнения процедуры создания новой группы пользователей необходимо в пункте меню <Пользователи> выбрать строку «Пользователи», выбрать команду «Новый» и нажать <Enter>.

На экран выводится окно ввода имени группы, в котором необходимо задать имя новой группы. Администратор должен присвоить каждой группе

уникальное в данной вычислительной среде имя. При вводе новой группы пользователей общие параметры присваиваются ей по умолчанию, но их всегда можно изменить путем выполнения операций, описанных в подразделе 3.4.

После задания необходимых параметров новой группы необходимо нажать кнопку <Запись> – новая группа появится в списке групп в правой части окна.

3.10. Удаление группы пользователей

Для выполнения процедуры удаления группы пользователей необходимо в меню <Польз.> выбрать строку с соответствующей группой, нажать кнопку <Удал.> и в появившемся далее окне подтвердить выполнение операции удаления группы.

3.11. Экспорт/импорт списка пользователей

3.11.1. Общие сведения

Список пользователей можно скопировать на внешний носитель, а в случае необходимости, загрузить эту копию с внешнего носителя. В качестве внешнего носителя можно использовать TM-идентификатор DS-1996, флоппи-диск или USB-накопитель (обычные «флэшки»; в случае использования их для выполнения процедур экспорта/импорта списка пользователей, нуждаются в специальной подготовке – подробнее см. 3.11.2).

3.11.2. Подготовка USB-накопителей для выполнения процедур экспорта/импорта списка пользователей

Для выполнения процедур экспорта/импорта списка пользователей необходимо использовать специально подготовленные USB-накопители – с записанным на них файлом образа amdz_fdd.img. Для этого необходимо выполнить следующие действия (на примере использования утилиты «Win32DiskImager»).

1) Загрузить ПЭВМ, выполнить вход в операционную систему.

2) Скачать с сайта ОКБ САПР http://www.accord.ru/ файл образа amdz_fdd.img.

3) Запустить утилиту Win32DiskImager с правами администратора (рисунок 19).

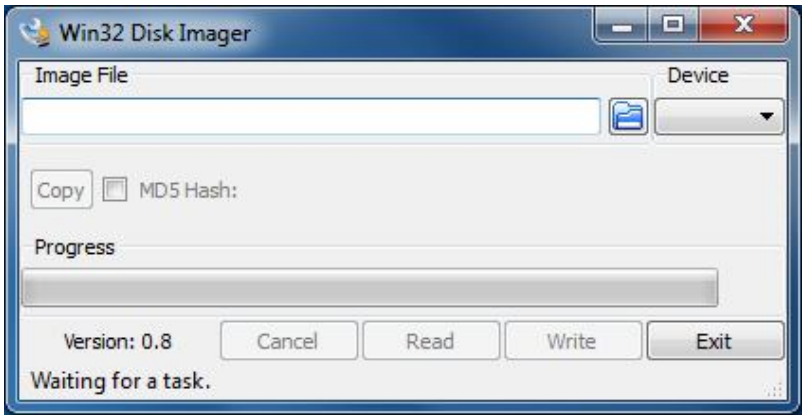

Рисунок 19 - Главное окно утилиты Win32DiskImager

4) Подключить флэшку к USB-порту компьютера.

5) Нажать на иконку папки справа от поля Image File и выбрать файл образа amdz_fdd.img (рисунок 20).

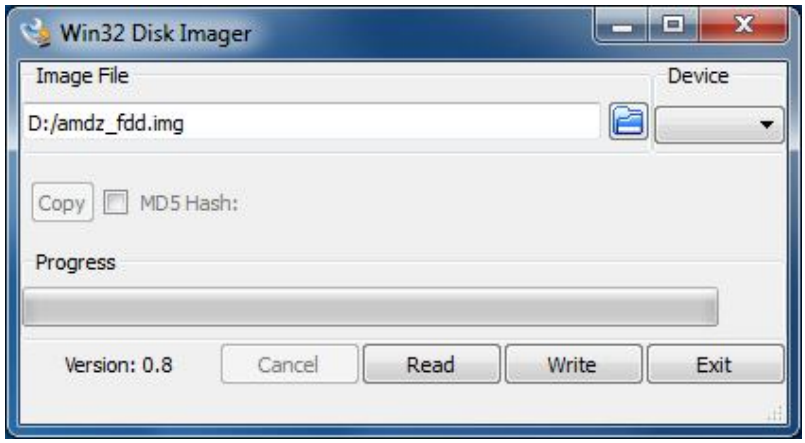

Рисунок 20 - Выбор образа

6) В поле Device выбрать нужный USB-накопитель (рисунок 21).

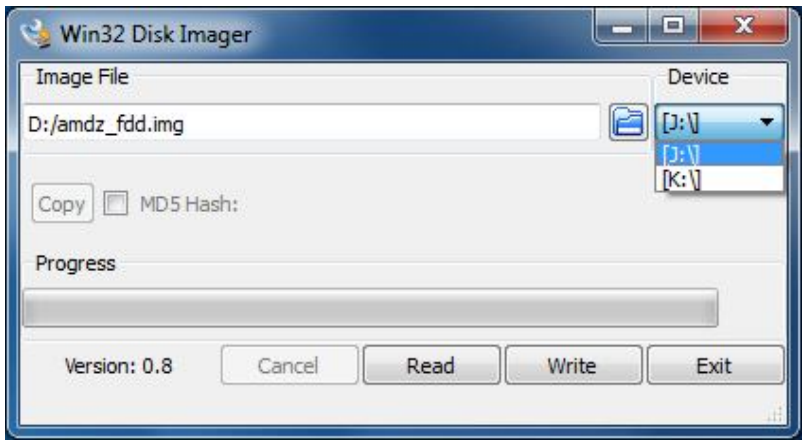

Рисунок 21 - Выбор USB-накопителя

7) Нажать кнопку <Write>.

После успешного выполнения описанной последовательности действий флэшку можно использовать для выполнения процедур экспорта/импорта списка пользователей (подробнее см. 3.11.3).

ВНИМАНИЕ! Используйте подготовленные USB-накопители только для выполнения процедур экспорта/импорта списка пользователей. Использование таких USB-накопителей для иных целей может привести к потере информации о списке пользователей «Аккорд-АМДЗ».

3.11.3. Экспорт/импорт списка пользователей

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

Рисунок 22 - Выбор носителя для экспорта базы пользователей

Если в качестве носителя используется специально подготовленный USB-носитель (подробнее см. 3.11.2), следует выбирать пункт «Флоппи-диск».

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

Рисунок 23 - 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>.

3.12. 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>.

3.12.1. Контроль аппаратуры

В подменю выберите команду <Аппаратура> и нажмите <Enter>. На экран выводится окно контроля аппаратуры (рисунок 24).

Рисунок 24 - 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. Прокрутка 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 <Del>. 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 <Del> и пересчитать КС (комбинация клавиш Alt-U).

3.12.2. Контроль целостности служебных областей жестких дисков

В подменю <Контроль> выберите команду <Диски> и нажмите <Enter>. На экран выводится окно контроля служебных областей дисков (рисунок 25). Поддерживаются файловые системы следующих типов: FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSD, Ext2FS, Sol86FS, QNXFS, MINIX.

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 <Del>. 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).

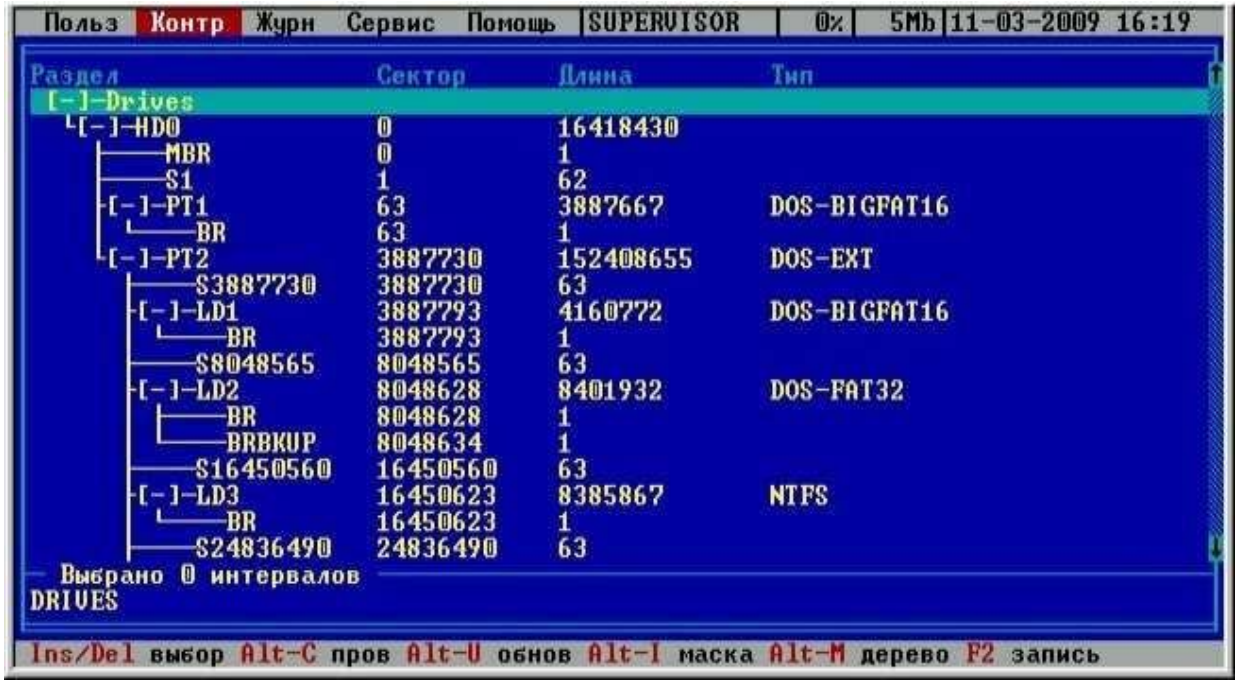

Рисунок 25 - Окно контроля служебных областей диска

3.12.3. Контроль целостности файлов

В подменю <Контроль> выберите команду <Файлы> и нажмите <Enter>. На экран выводится окно контроля файлов (рисунок 26). СЗИ «Аккорд-АМДЗ»

обеспечивает контроль целостности программ и данных до загрузки ОС, защиту от внедрения разрушающих программных воздействий (РПВ). Поддерживаются файловые системы следующих типов: FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSD, Ext2FS, 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.

Рисунок 26 - 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 дерево файлов в данном каталоге. После нажатия комбинации клавиш <Alt>+<I> выводится окно задания фильтра расширения (рисунок 27).

Рисунок 27 - 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 (рисунок 28). Кнопка «Отмена» или клавиша <Esc> отменяет операцию «Добавить по фильтру».

Рисунок 28 - 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 (рисунок 29).

Рисунок 29 - 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.

3.12.4. Контроль целостности реестра Windows

Данная функция позволяет контролировать целостность разделов реестра Windows 95/98 и Windows NT/2000/XP/Vista/2008/7.

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> (рисунок 30).

Рисунок 30 - 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 (рисунок 31).

Рисунок 31 - Дерево разделов и ключей реестра

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

3.12.5. 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 (рисунок 32).

Примечание. *При выборе типа ОС для Windows 2003 следует указывать «Windows XP», для Windows 2008 - «Windows 7».*

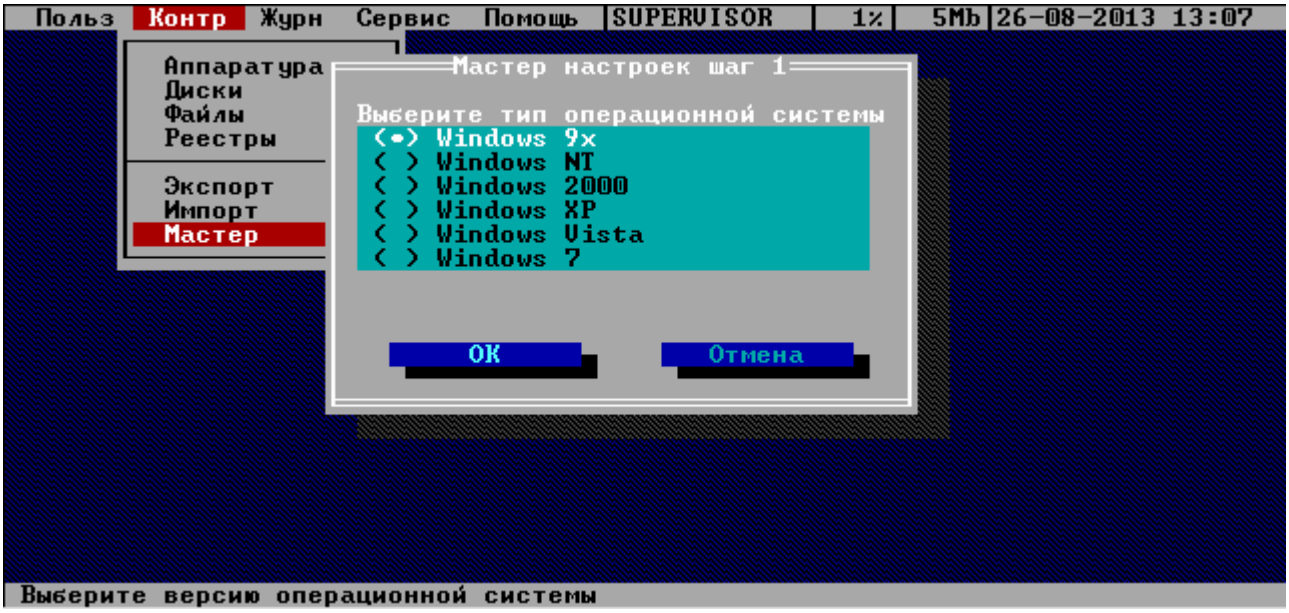

Рисунок 32 - Выбор типа ОС в «Мастере» контроля целостности

Следующий шаг – указание каталога, в котором установлена операционная система (рисунок 33). 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>.

Рисунок 33 - 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 (рисунок 34).

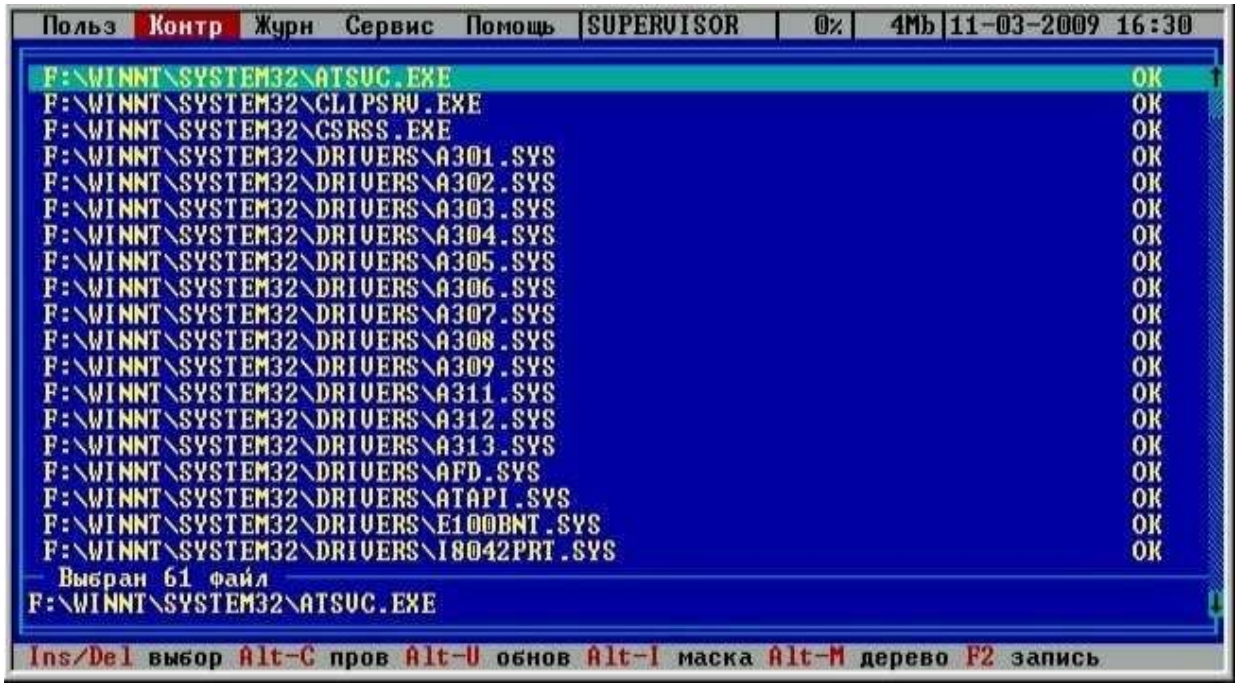

Рисунок 34 - Результат работы «Мастера» контроля целостности

3.13. 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 (рисунок 35).

Рисунок 35 - 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 1. В самой верхней строке экрана после имени пользователя выводится процент заполнения области памяти контроллера, отведенной под системный журнал. Если процент заполнение журнала превышает 85%, то при загрузке компьютера выдается предупреждение, но загрузка продолжается. Если процент заполнение 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 TM-идентификатор DS1996. После этого можно стереть содержимое журнала с помощью клавиши <Delete>.

Выход из режима просмотра журнала по клавише <Esc>.

3.14. 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 (рисунок 36):

Рисунок 36 - 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 (рисунок 37).

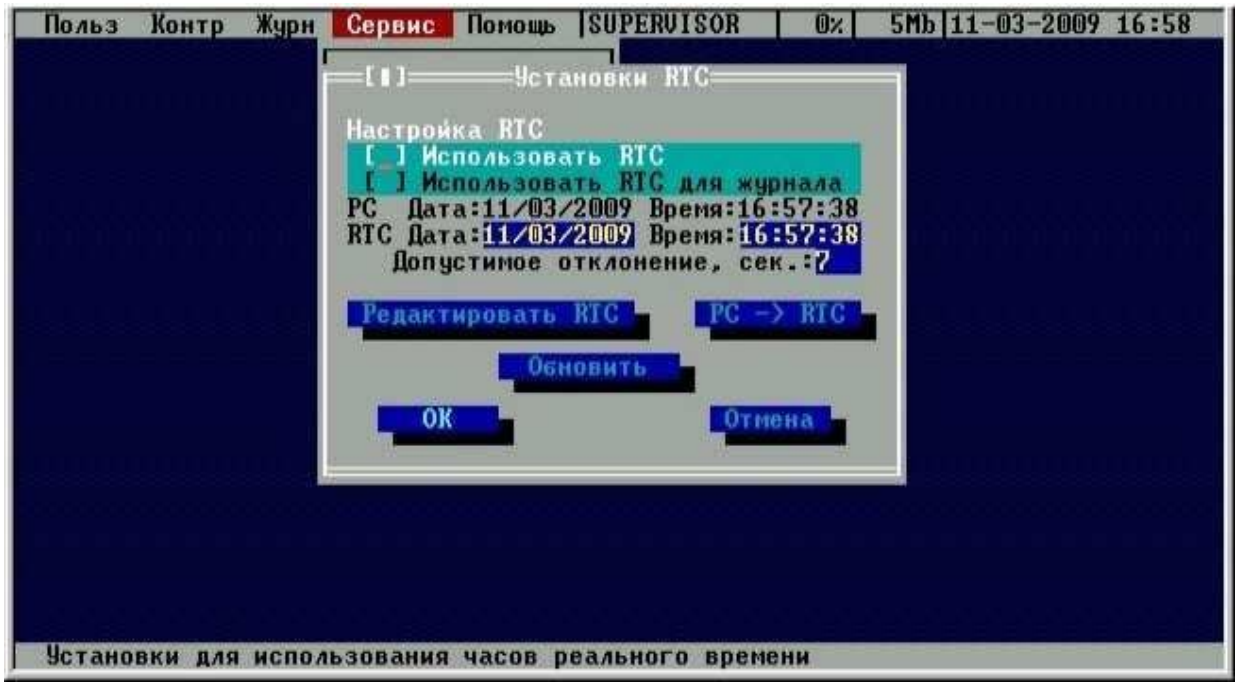

Рисунок 37 - Окно установок параметров таймера

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». 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, «Аккорд-Win32» и «Аккорд-Win64», которые выпущены после января 2010 года.

3.15. Форматирование баз данных контроллера

Данный пункт стартового меню администратора позволяет очистить все внутренние базы данных без перевода контроллера в технологический режим, т.е. провести повторную инициализацию контроллера без вскрытия корпуса компьютера. Эта функция доступна во внутреннем ПО контроллера начиная с версии 02.01.014 и выше.

При выполнении данной команды очищаются база пользователей, списки контролируемых объектов, журнал регистрации событий. Установки сбрасываются в значение «по умолчанию».

Данная функция может быть полезной при промышленной сборке компьютеров с предустановленной СЗИ, или при централизованной установке комплекса «Аккорд» с последующей отправкой компьютера в филиалы в разных регионах. После установки контроллера АМДЗ следует проверить работоспособность компьютера, а для этого необходимо зарегистрировать идентификатор Администратора и ввести пароль. Специалисту, который выполняет проверку, придется для каждого компьютера регистрировать отдельный идентификатор и в дальнейшем сообщать назначенный пароль непосредственному пользователю данного идентификатора. Для упрощения процедуры проверки можно выполнить регистрацию одного собственного идентификатора, а после проверки запустить процедуру очистки баз данных из меню администратора.

Также данная функция будет полезной при передаче компьютера в другое подразделение, где есть собственный администратор БИ и совсем иной состав пользователей.

Для выполнения процедуры форматирования базы данных Главному Администратору следует в окне стартового меню администратора выбрать пункт «Очистка БД контроллера» (рисунок 1).

При утере идентификатора администратора или при передаче компьютера в другое подразделение, где есть собственный администратор БИ и иной состав пользователей, вместо процедуры форматирования баз данных контроллера, вызываемой из стартового меню администратора, следует выполнять процедуру аппаратной очистки баз данных (подробнее см. раздел 5).

4. 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 (рисунок 1). 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.

5. Аппаратная очистка баз данных контроллера

ВНИМАНИЕ! Если контроллер АМДЗ используется в составе комплекса «Аккорд NT/2000» v. 3.0, «Аккорд-Win32» или «Аккорд-Win64», то пользоваться функцией очистки баз данных можно ТОЛЬКО ПОСЛЕ ОТКЛЮЧЕНИЯ монитора безопасности в программе настройки комплекса!

Для того чтобы выполнить операцию очистки баз данных контроллера, необходимо:

1. Выключить компьютер и вынуть плату контроллера из разъема системной шины.
2. Перевести контроллер в технологический режим (подробнее см. пункт «Режимы доступа к аппаратным ресурсам платы контроллера» «Руководства по установке» (11443195.4012-006 98)).
3. Вставить плату в компьютер.
4. Загрузить компьютер в ОС MS-DOS (никаких менеджеров памяти (QEMM, EMM386 и т.п.) быть не должно!).

Примечание: *Загрузиться в MS-DOS можно с дискеты, flash-накопителя или CD. Загрузочную дискету MS-DOS можно создать с помощью Windows XP при выборе параметров форматирования дискеты. Образ загрузочной дискеты с набором утилит для очистки базы данных для последней версии ПО можно также получить на сайте ОКБ САПР (утилита записи образа на дискету включена в архив). Кроме того, все CD с дистрибутивом ПО "Аккорд NT/2000" v.3.0 являются загрузочными. Диски версии 2.0 выпускаются загрузочными начиная с rev.2.30.*

5. Запустить ip(xx).exe, где xx - модель контроллера. В настоящее время выпускаются контроллеры серии 5mx и 5.5. Контроллеры серии 5 не выпускаются, но поддерживаются.

Примечание: *Если версия встроенного ПО в контроллере отличается от версии на CD, или в архиве с сайта, то очистка может завершиться неудачно. Фатальных последствий для контроллера это не влечет. В этом случае следует загрузить с сайта ОКБ САПР(www.accord.ru) архив с соответствующей версией встроенного ПО (раздел «Предыдущие версии») и использовать программу ipxx.exe из состава этого архива.*

6. Выключить компьютер, вернуть контроллер в рабочий режим (подробнее см. пункт «Режимы доступа к аппаратным ресурсам платы контроллера» «Руководства по установке» (11443195.4012-006 98)).
7. Установить контроллер в компьютер.

6. Техническая поддержка

В случае необходимости консультации ЗАО «ОКБ САПР» предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 18-00 (по московскому времени) обращаться по телефонам: +7 (499) 235-78-17,

+7 (926) 235-89-17, +7 (926) 762-17-72 или по адресу электронной почты help@okbsapr.ru. Наш адрес в Интернете http://www.okbsapr.ru/.

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
OK	Успешное завершение
ULST	Создание списка пользователей
IID	Незарегистрированный идентификатор
TID	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.
sTAH	Изменились дата, атрибуты, контрольная сумма файла.
STAH	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