ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

«Аккорд-АМДЗ»

(Аппаратный модуль доверенной загрузки)

Руководство администратора

11443195.4012.038 90

Листов 54

Москва

2015

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-5.5(e), Аккорд-LE, Аккорд-GX, Аккорд-GXM, Аккорд-GXMH.

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
СКЦ	Список (списки) контроля целостности
СУЦУ	Система удаленного централизованного управления

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, Ext4, ReiserFS, MINIX, QNX4, QNX6.

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 (РС) 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 (РС) нескольких ОС;
- регистрацию на ПЭВМ (РС) до 126 пользователей (для моделей на базе специализированных контроллеров «Аккорд-5.5(e)») и до 1022 пользователей на одной ПЭВМ (для моделей на базе специализированных контроллеров семейства «Аккорд-LE/GX»);
- 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 (для моделей на базе специализированных контроллеров «Аккорд-5.5(e)»);
- администрирование встроенного ПО комплекса (регистрацию пользователей и персональных идентификаторов, назначение файлов для контроля целостности, контроль аппаратной части ПЭВМ (РС), просмотр системного журнала);
- регистрацию, сбор, хранение и выдачу данных о событиях, происходящих в ПЭВМ (РС) в части системы защиты от несанкционированного доступа.

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

При модификации системного ПО замена контроллера не требуется. При этом обеспечивается поддержка спецрежима программирования контроллера без снижения уровня защиты.

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 4012-038-11443195-2011) 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 переходе к другим типам ОС.
- ***съемник информации с контактным устройством***, обеспечивающий интерфейс между контроллером комплекса и персональным идентификатором пользователя.
- ***персональный идентификатор пользователя*** – микропроцессорное устройство DS 199x («Touch memory»), или USB-устройство ПСКЗИ ШИПКА; в качестве персональных идентификаторов поддерживаются также смарт-карты и USB-ключи. Каждый идентификатор обладает уникальным номером, который формируется технологически и подделать который практически невозможно. Объем памяти, доступной для записи и чтения зависит от типа идентификатора. Подробнее о поддерживаемых типах и порядке использования персональных идентификаторов см. п. «Идентификаторы» «Руководства по установке» (11443195.4012.006 98/11443195.4012.038 98), входящего в комплект поставки комплекса.

Количество и тип идентификаторов, модификация контроллера и контактного устройства оговариваются при поставке комплекса и указываются в Формуляре (11443195.4012.038 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. Условия применения комплекса

Для установки комплекса «Аккорд-АМДЗ» требуется следующий минимальный состав технических и программных средств:

- ПЭВМ типа IBM PC, сервер или рабочая станция, основанная на процессоре с архитектурой x86 (IA-32) или x86-64 (AMD64), функционирующая под управлением операционной системы, поддерживающей любую из файловых систем, приведенных в подразделе 1.1 настоящего руководства;
- наличие свободного слота PCI/PCI-X/PCI-Express/miniPCI-Express (в соответствии с типом специализированного контроллера) на материнской плате ПЭВМ.

Технические средства защищаемой ПЭВМ (РС) 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 98/11443195.4012.038 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 3.2 настоящего руководства).

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

3. Работа с комплексом

3.1. Начало работы

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

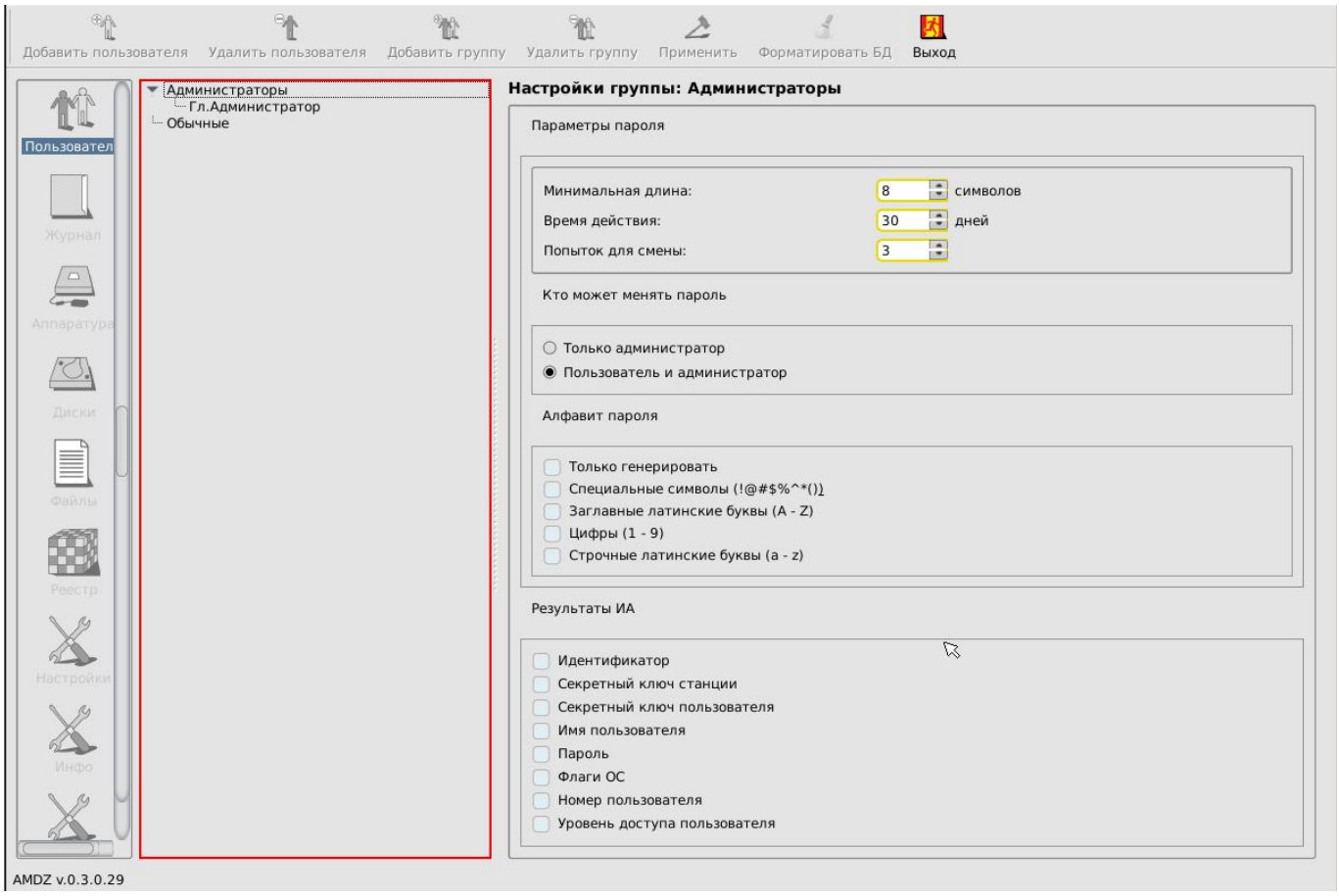

Рисунок 1 - Главное окно программы администрирования

Главное окно программы состоит из следующих областей:

- меню выбора объектов администрирования (левая вертикальная панель);
- панель управления выбранным объектом администрирования:
  - панель инструментов (верхняя панель);
  - рабочее поле.

Меню выбора объектов администрирования позволяет проводить операции администрирования следующих объектов:

- <Пользователи> - работа со списком пользователей и групп;
- <Журнал> - работа с внутренним журналом регистрации событий;
- <Аппаратура> - контроль целостности аппаратной части компьютера;
- <Диски> - контроль целостности системных областей жестких дисков;

- <Файлы> - контроль целостности файлов на жестких дисках;
- <Реестр> - контроль целостности отдельных ветвей реестра;
- <Настройки> - общие настройки комплекса;
- <База данных> – выполнение процедур экспорта/импорта элементов базы данных;
- <Инфо> - информация о версии прошивки контроллера и контрольные суммы ядра защиты.

В начале первого сеанса работы, помимо главного окна программы, на экран также выводится сообщение с требованием выполнить процедуру настройки параметров учетной записи Главного Администратора (рисунок 2), без выполнения которой не доступны никакие функции «Аккорд-АМДЗ».

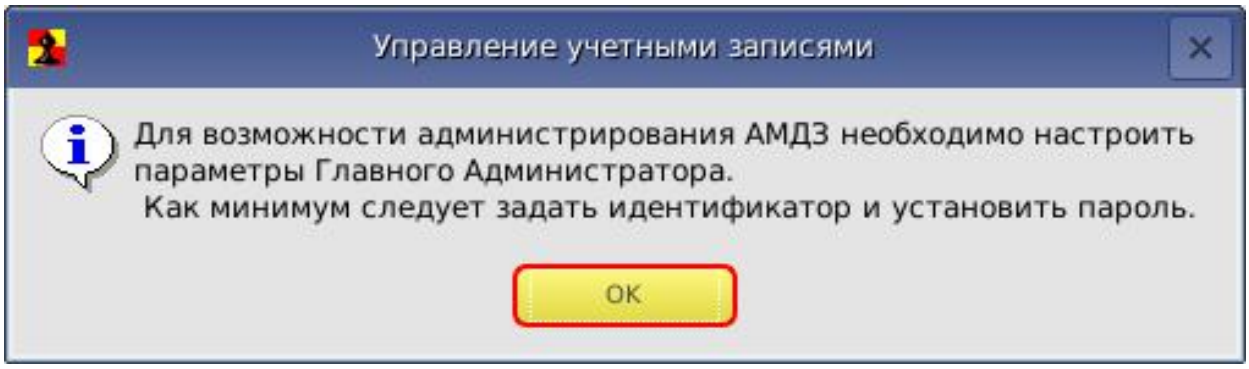

Рисунок 2 - Сообщение с требованием настроить параметры Главного Администратора

После выполнения процедуры установки параметров учетной записи Главного Администратора, описанной в подразделе 3.2 настоящего руководства, функционал «Аккорд-АМДЗ» становится доступным для Главного Администратора.

Далее Главному Администратору следует зарегистрировать необходимое количество пользователей (или групп пользователей), настроить параметры их учетных записей, а также списки контроля целостности аппаратуры, служебных областей жестких дисков, файлов, реестра (подробнее см. соответствующие подразделы настоящего руководства).

3.2. Установка параметров учетной записи Главного Администратора (администратора безопасности информации)

При инициализации контроллера в базе данных создается учетная запись Главного Администратора (супервизора)[1] – «Гл. Администратор» – которому

[1)] В ПО «Аккорд-АМДЗ» имена учетных записей, созданных по умолчанию, отображаются на русском языке. Необходимо помнить, что для имени «Главный Администратор» также зарезервировано имя «SUPERVISOR» (следовательно, невозможно создать нового пользователя с таким именем); для групп «Администраторы» и «Обычные» также зарезервированы имена «ADMINS» и «EVERYONE» соответственно (следовательно, невозможно создать новые группы с такими именами).

будут полностью доступны все функции администрирования. Но при этом идентификатор для этого пользователя не зарегистрирован.

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 нужно отметить мышью пользователя «Гл.Администратор» (рисунок 1) и перейти к выполнению операции назначения персонального идентификатора (см. подраздел 3.2.1).

3.2.1. Назначение персонального идентификатора

Для регистрации идентификатора на правой панели в строке «Идентификатор» нужно нажать кнопку <Сменить>. На экран выводится окно, в котором требуется указать, какой секретный ключ будет использоваться. При этом можно оставить существующий секретный ключ, если идентификатор использовался ранее и секретный ключ уже был сгенерирован, или сгенерировать новый.

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).

Следует сделать выбор и нажать кнопку <Далее> (рисунок 3).

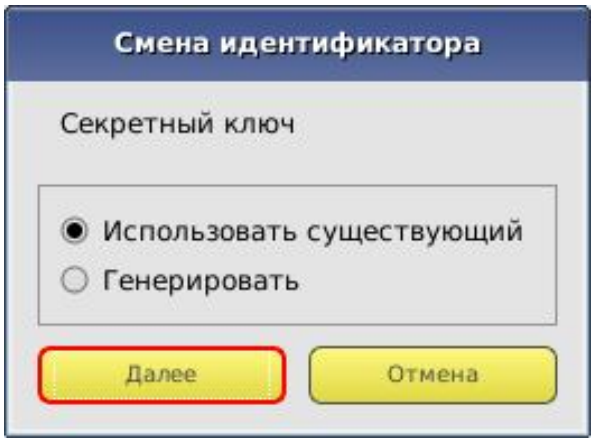

Рисунок 3 – Окно выбора секретного ключа

На экране появится окно с запросом идентификатора для смены (рисунок 4).

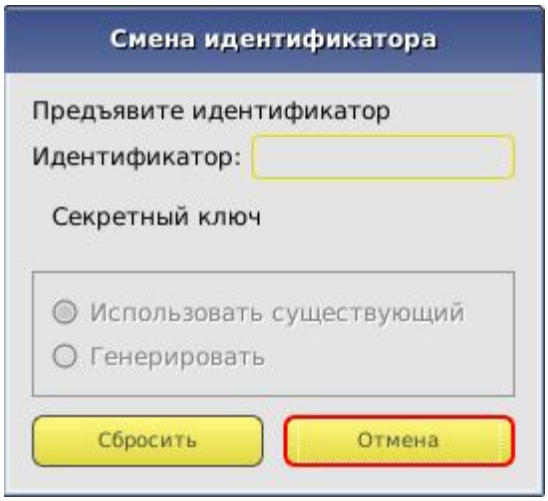

Рисунок 4 – Окно с запросом идентификатора для смены

Если идентификатор еще не предъявлен, поле «Идентификатор» пустое. Программа в этот момент ожидает контакта идентификатора со съемником информации. Необходимо предъявить идентификатор и дождаться момента, пока в поле не появится серийный номер идентификатора (рисунок 5).

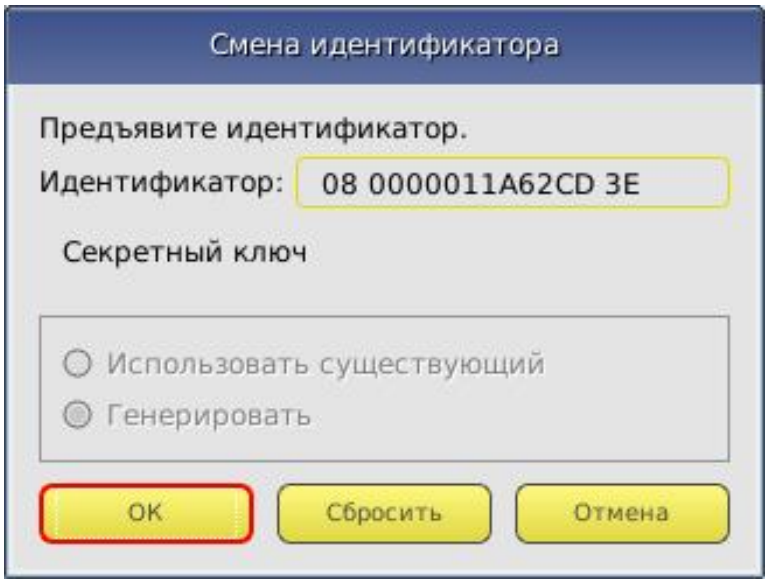

Рисунок 5 – Окно смены идентификатора

Необходимо подтвердить завершение операции нажатием кнопки <OK>.

После корректного выполнения описанной последовательности действий номер идентификатора появляется в поле «Идентификатор» главного окна программы (рисунок 6).

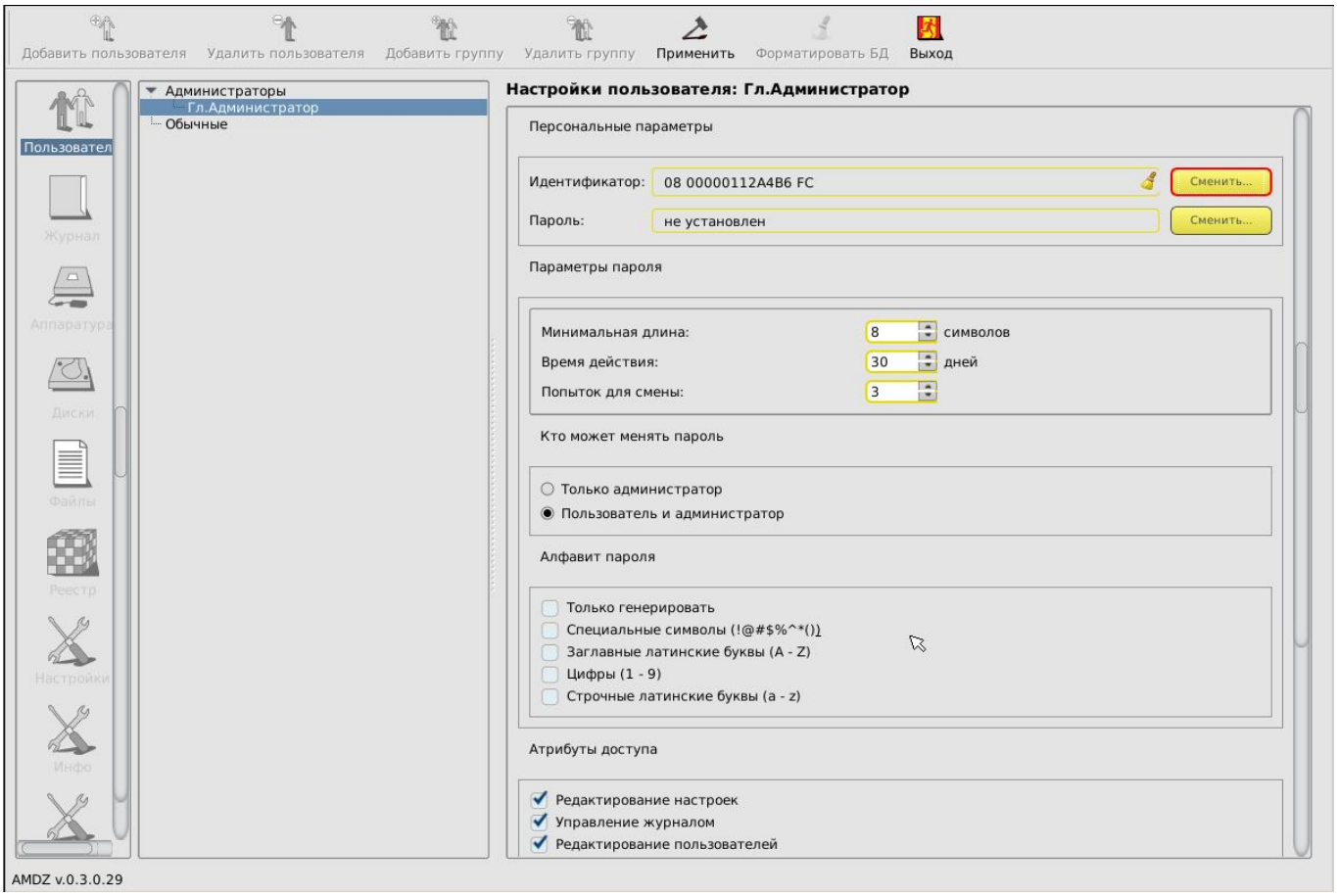

Рисунок 6 - Идентификатор Главного Администратора установлен

Далее необходимо перейти к процедуре назначения пароля (см. 3.2.2).

ВНИМАНИЕ! Следует помнить, что для корректного завершения процедуры редактирования параметров учетной записи необходимо выполнить как процедуру установки идентификатора, так и процедуру установки пароля.

В противном случае, по нажатии кнопки <Применить> в главном окне программы на экран выводится предупреждение о том, что идентификатор (и)или пароль пользователя не установлены (рисунок 7), и программа ожидает от администратора завершения процедуры настройки параметров авторизации пользователя.

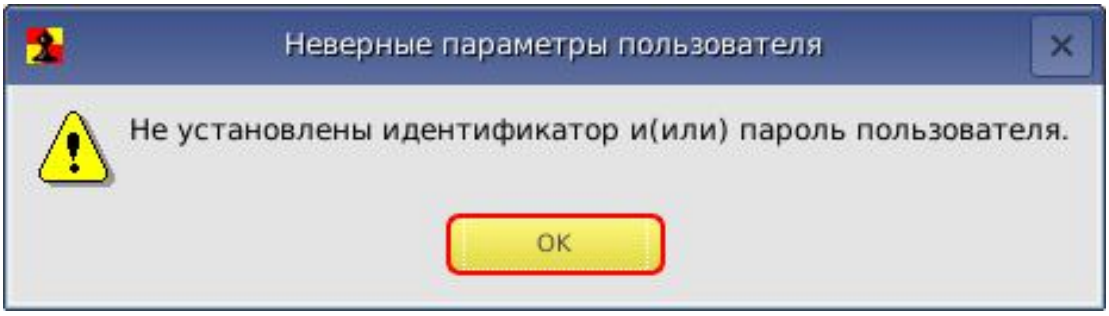

Рисунок 7 - Сообщение о том, что идентификатор или пароль пользователя не установлены

3.2.2. Назначение пароля

На правой панели главного окна программы (рисунок 1) нужно установить необходимые параметры пароля (подробнее см. 3.3.2.1), а затем в строке «Пароль» нажать кнопку <Сменить>. На экран выводится окно ввода пароля (рисунок 8). При первоначальной регистрации параметров пользователя строка «Старый пароль» недоступна. Необходимо ввести новый пароль и подтвердить 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. Следует учитывать, что 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 типичных последовательностей типа: '123456' или 'qwerty'. При вводе подобных последовательностей символов выдается сообщение об ошибке.

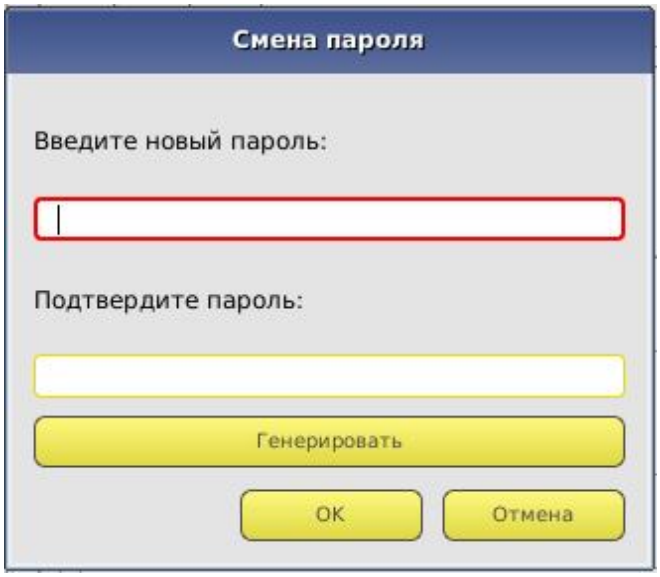

Рисунок 8 – Окно ввода пароля

ВНИМАНИЕ! Если пользователю не назначается пароль, то при редактировании параметров пароля в строке «Минимальная длина» в разделе «Параметры пароля» следует установить длину пароля 0, иначе при записи данных о пользователе выводится сообщение об ошибке (рисунок 7).

Имеется возможность выбора процедуры генерации пароля случайным образом (кнопка <Генерировать>). В этом случае пароль генерируется таким образом, чтобы в нем обязательно присутствовал хотя бы один символ из набора, заданного в параметре «Алфавит пароля». После генерации новый пароль выводится в строке «Введите новый пароль» и пользователь должен его ввести с клавиатуры в поле «Подтвердите пароль».

После успешного выполнения процедуры установки (или генерации) нового пароля в главном окне программы значение параметра в поле «Пароль» меняется на «Установлен» (рисунок 9).

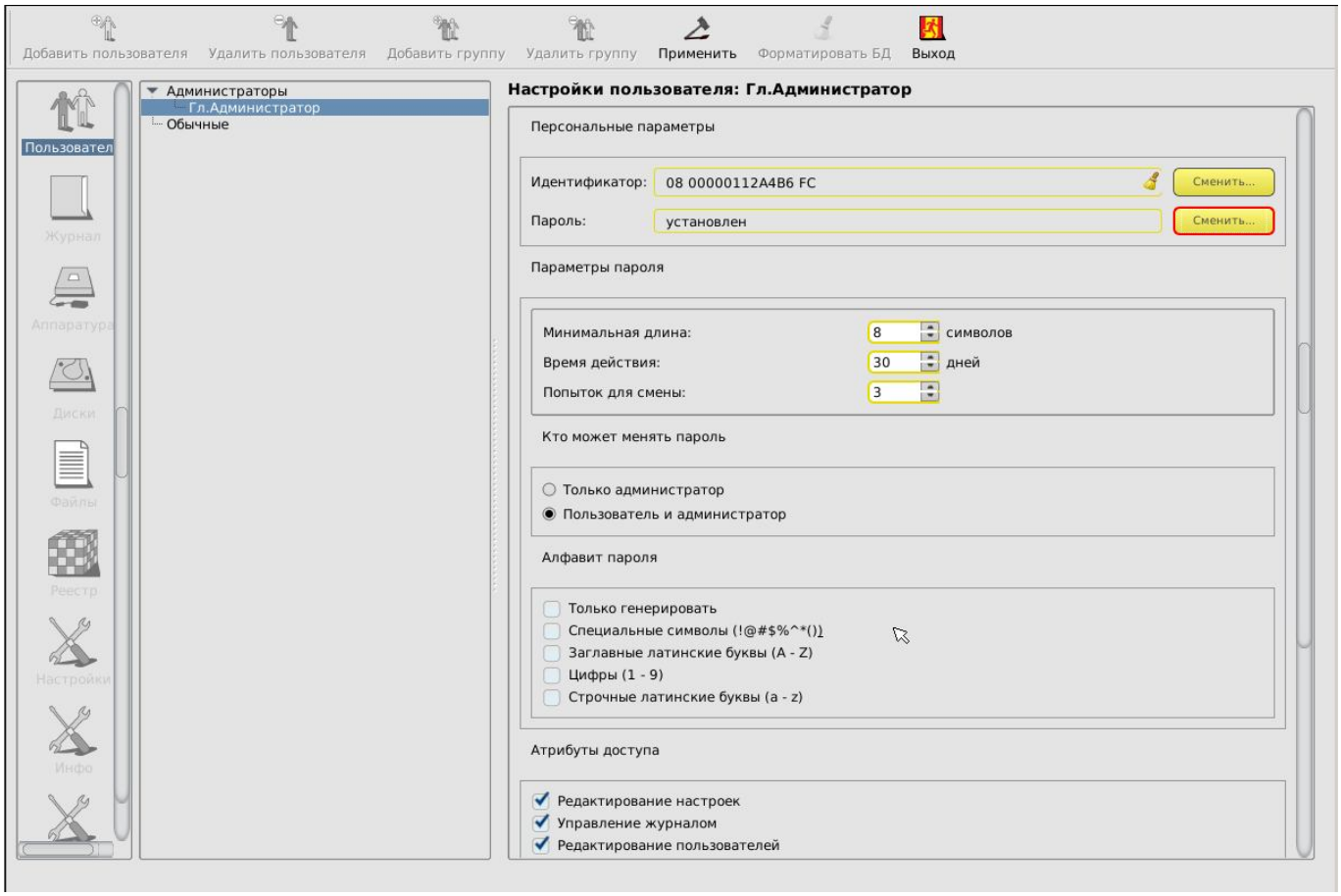

Рисунок 9 - Пароль Главного Администратора установлен

Для сохранения параметров пользователя «Гл.Администратор» нужно нажать кнопку <Применить> на панели инструментов вверху главного окна (рисунок 9).

После корректного выполнения описанной последовательности действий, на экран выводится сообщение о сохранении внесенных изменений (рисунок 10).

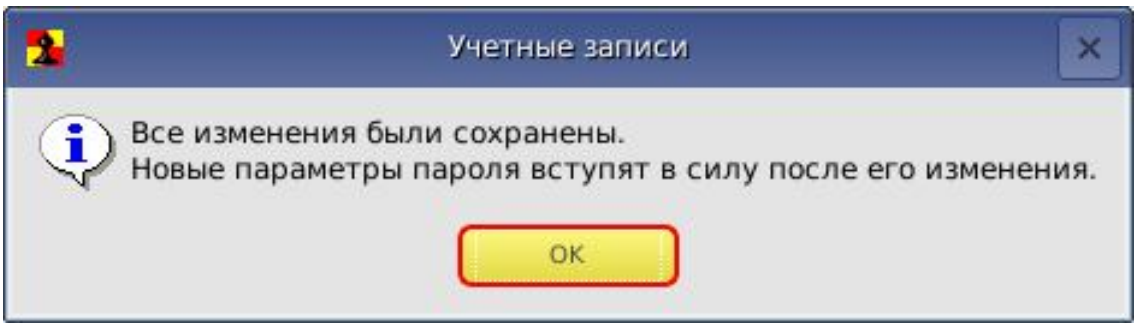

Рисунок 10 - Сообщение о сохранении внесенных изменений

После сохранения параметров пользователя «Гл.Администратор» имеется возможность в любое время получить доступ к процедуре администрирования.

3.3. Настройка параметров групп и учетных записей пользователей

3.3.1. Список пользователей

При инициализации контроллера создаются две зарезервированные группы пользователей – «ADMINS» (далее – «Администраторы») и «EVERYONE» (далее – «Обычные»)[1]. 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 в главном окне программы клавишами <стрелка> или мышью установить курсор на строке заголовка группы и нажать <Enter> или дважды щелкнуть левой кнопкой мыши (рисунок 1).

3.3.2. Общие параметры группы «Администраторы»

Для группы «Администраторы» установлены следующие общие параметры (рисунок 11):

- параметры пароля;
- результаты ИА (идентификации/аутентификации пользователя).

[1)] В ПО «Аккорд-АМДЗ» имена учетных записей, созданных по умолчанию, отображаются на русском языке. Необходимо помнить, что для имени «Главный Администратор» также зарезервировано имя «SUPERVISOR» (следовательно, невозможно создать нового пользователя с таким именем); для групп «Администраторы» и «Обычные» также зарезервированы имена «ADMINS» и «EVERYONE» соответственно (следовательно, невозможно создать новые группы с такими именами).

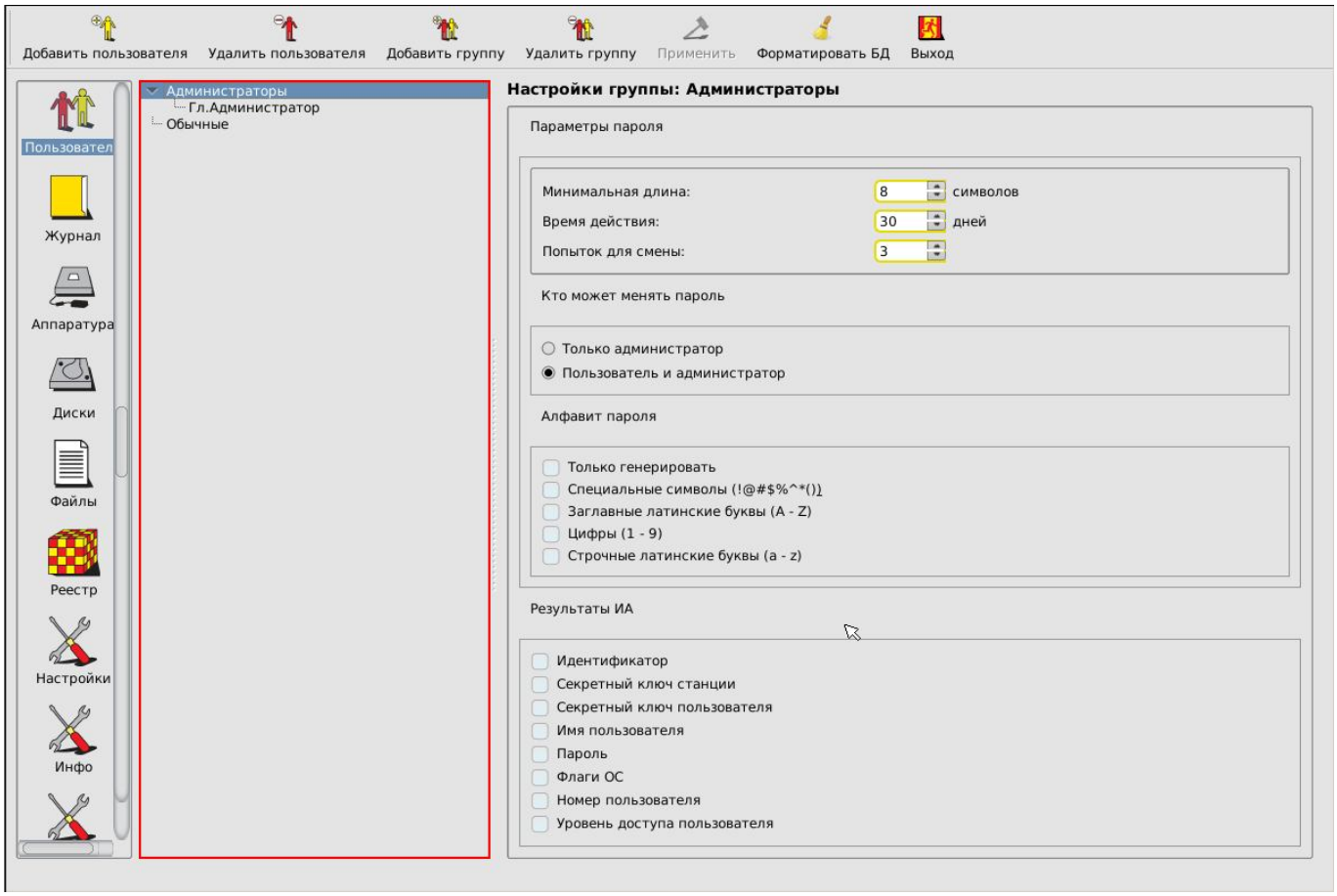

Рисунок 11 - Общие параметры группы «Администраторы»

3.3.2.1. Параметры пароля

Для управления парольной политикой можно регулировать следующие параметры пароля на правой вертикальной панели (рисунок 11):

- «Минимальная длина» - параметр определяет количество символов, контролируемое при создании и смене пароля. Нельзя ввести пароль меньшей длины. Если для авторизации пользователя предполагается использовать только идентификатор, этот параметр нужно установить равным 0 (пароль задавать не обязательно). По умолчанию длина пароля установлена равной 8 символам, максимальное допустимое значение - 12 символов.
- «Время действия» - 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, выполняется перезагрузка компьютера.
- «Кто может менять пароль» - установка этого параметра позволяет задать политику в отношении смены пароля: пользователь может самостоятельно менять пароль (после истечения времени действия или

в произвольный момент времени по своей инициативе) или смену пароля осуществляет только администратор.

- «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, изменения его параметров вступят в силу только при смене пароля.

3.3.2.2. 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 ИА». Установки по умолчанию, при которых не включен ни один флаг, предполагают использование только контроллера «Аккорд-АМДЗ».

3.3.3. Общие параметры группы «Обычные» (пользователи)

Для группы «Обычные» (пользователи) установлены следующие общие параметры (рисунок 12):

- параметры пароля;
- результаты ИА (идентификации/аутентификации пользователя).

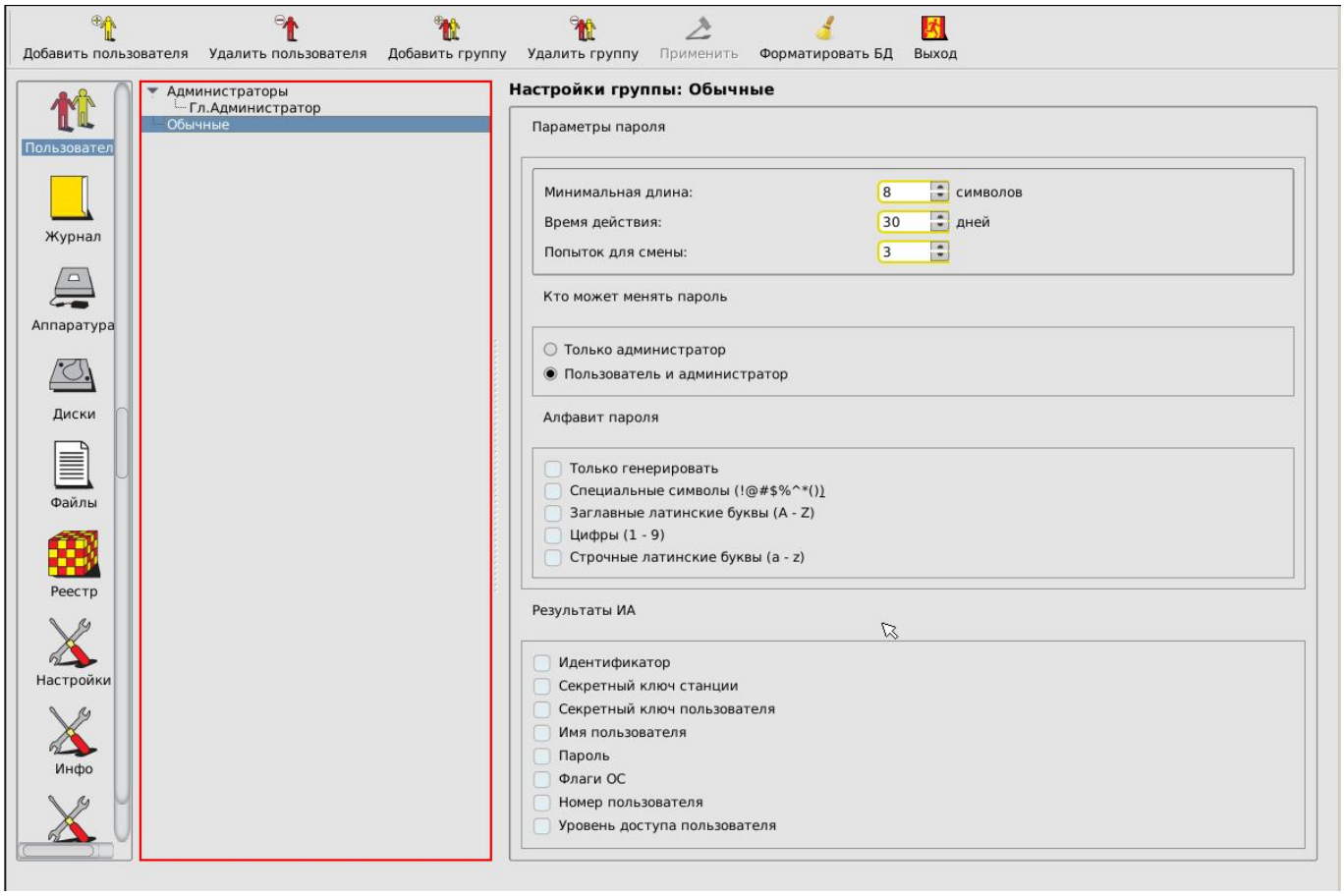

Рисунок 12 – Общие параметры группы «Обычные»

Настройки параметров пароля и результатов идентификации/аутентификации аналогичны настройкам соответствующих общих параметров для группы «Администраторы».

3.3.4. Параметры пользователей в группе «Администраторы»

Для пользователей группы «Администраторы» установлены следующие параметры (рисунок 13):

- персональные параметры;
- параметры пароля;
- атрибуты доступа;
- результаты ИА (идентификации/аутентификации пользователя).

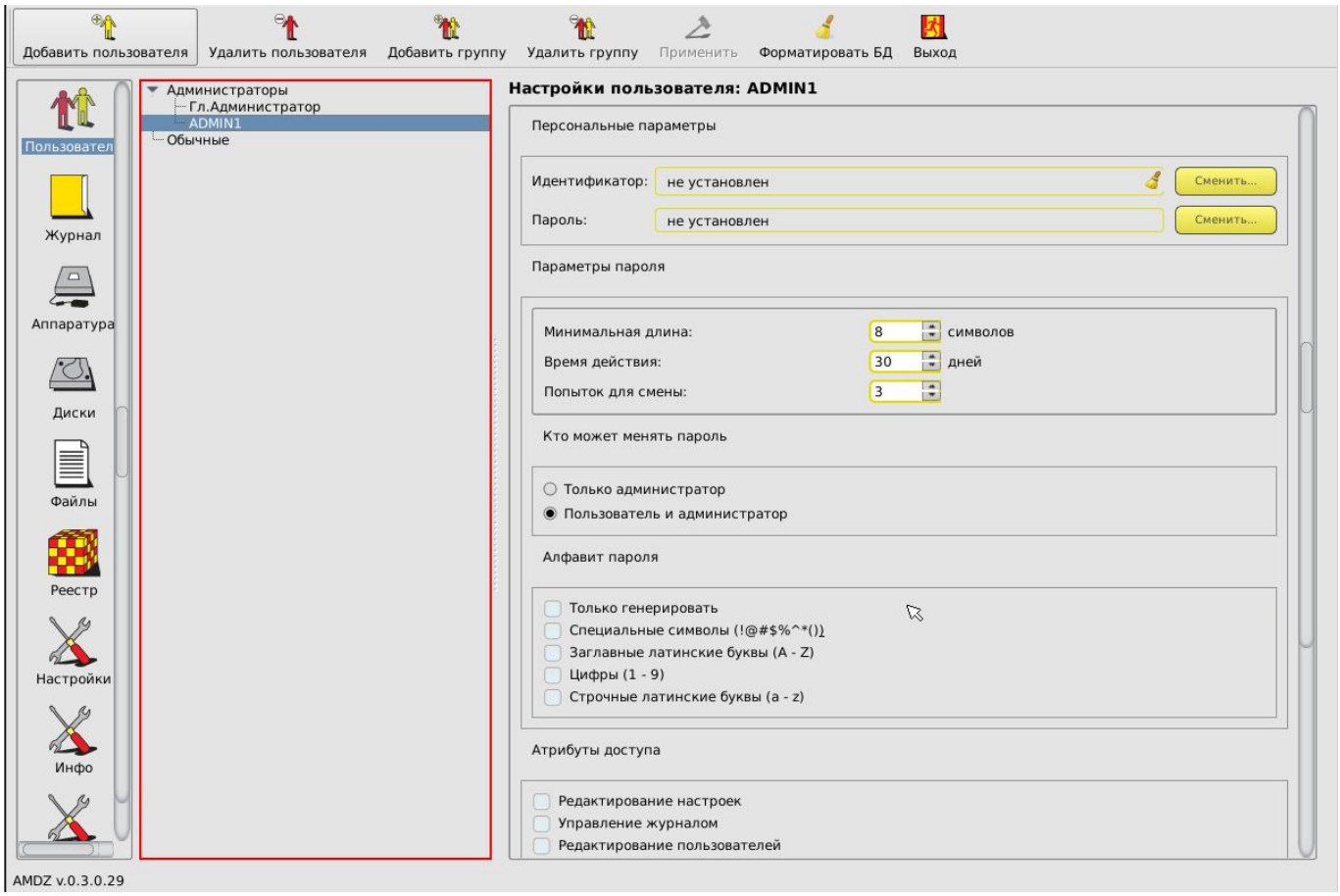

Рисунок 13 – Параметры пользователей в группе «Администраторы»

3.3.4.1. Персональные параметры

Каждый пользователь группы «Администраторы» обладает персональными параметрами, которые включают в себя:

- идентификатор;
- пароль.

Значения данных параметров отображаются на правой панели рабочего поля главного окна программы (см. рисунок 13).

В поле «Идентификатор» отображается шестнадцатизначный номер установленного для данного пользователя идентификатора. Если идентификатор для пользователя еще не установлен, то поле содержит фразу «не установлен». Идентификатор может быть установлен или сменен посредством выполнения операций, описанных в подразделе 3.2.1.

Поле «Пароль» содержит информацию о наличии установленного пароля пользователя и может иметь только одно из двух значений: «установлен» или «не установлен». Пароль пользователя может быть установлен или сменен посредством выполнения операций, описанных в подразделе 3.2.2.

3.3.4.2. Параметры пароля

Настройки параметров пароля для пользователей группы «Администраторы» аналогичны соответствующим настройкам общих параметров пароля для группы «Администраторы».

3.3.4.3. Атрибуты доступа

В разделе «Атрибуты доступа» устанавливаются персональные настройки функций редактирования и управления, которые будут доступны для данного пользователя из группы «Администраторы» (рисунок 14). Изменять настройки атрибутов доступа может главный администратор – супервизор (подробнее о супервизоре см. в подразделе 3.2.2) – или любой администратор, обладающий правом редактирования пользователей (т.е. входящий в группу «Администраторы» пользователь, при настройке учетной записи которого в атрибутах доступа установлен флаг «Редактирование пользователей»).

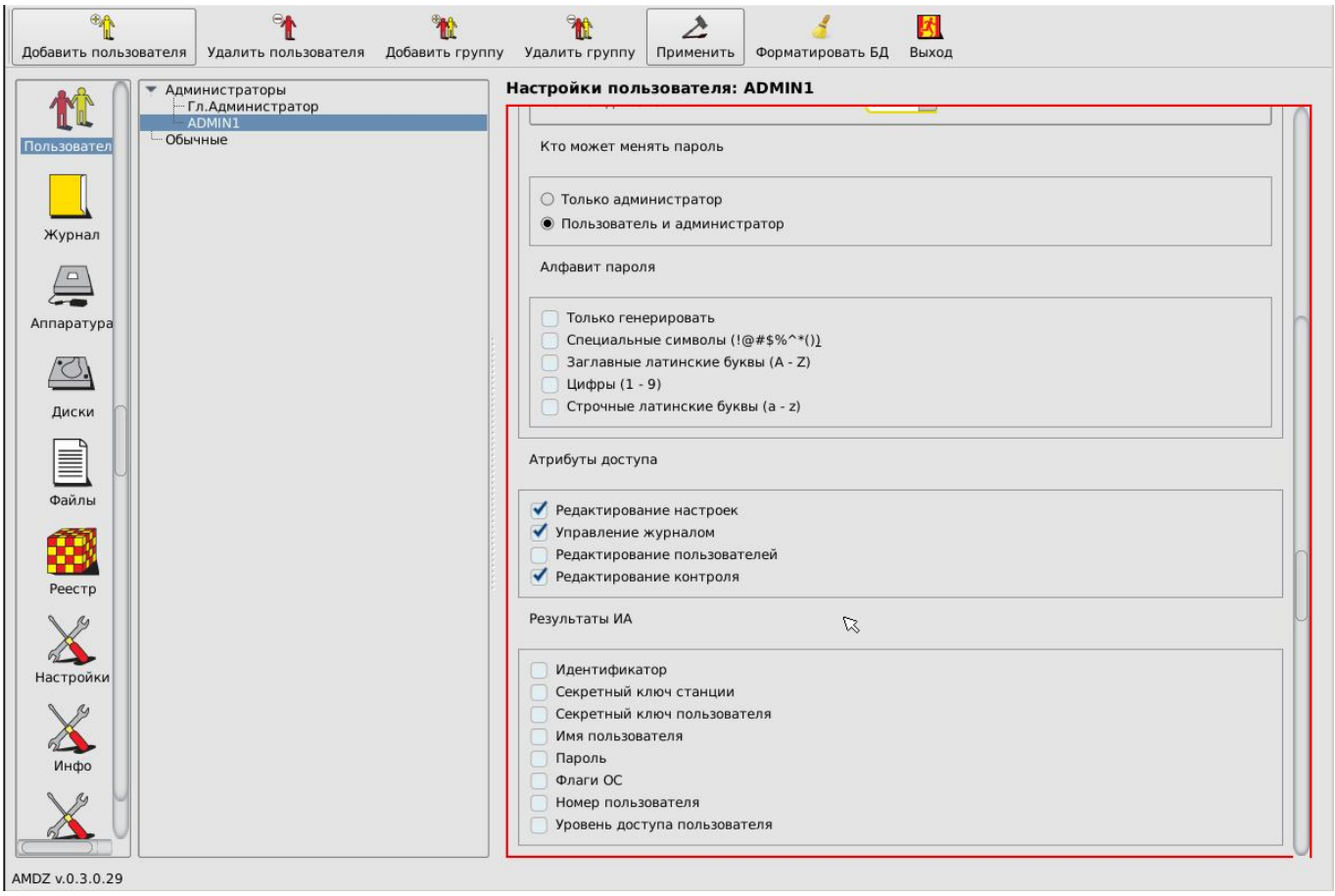

Рисунок 14 – Атрибуты доступа для пользователей из группы «Администраторы»

В данном разделе для выбранного пользователя из группы «Администраторы» супервизор может установить или снять следующие флаги:

- Редактирование настроек. При установке данного флага выбранный пользователь может изменять общие настройки комплекса (подробнее см. 3.12). При снятии данного флага для выбранного пользователя

функции изменения настроек недоступны, кнопка <Настройки> в меню выбора объектов администрирования отсутствует.

- Управление журналом. При установке данного флага выбранный пользователь может просматривать и очищать системный журнал (подробнее см. 3.11). При снятии данного флага для выбранного пользователя функции редактирования журнала недоступны, кнопка <Журнал> в меню выбора объектов администрирования отсутствует.
- Редактирование пользователей. При установке данного флага выбранный пользователь может выполнять редактирование списков пользователей (подробнее см. подразделы 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.5, 3.6, 3.9, 3.7, 3.8). При снятии данного флага для выбранного пользователя функции редактирования списков пользователей недоступны, кнопка <Пользователи> в меню выбора объектов администрирования отсутствует.
- Редактирование контроля. При установке данного флага выбранный пользователь может выполнять редактирование списков контроля целостности аппаратуры и реестра, служебных областей жестких дисков, файлов (подробнее см. 3.10). При снятии данного флага для выбранного пользователя функции редактирования списков контроля целостности недоступны, кнопки <Аппаратура>, <Диски>, <Файлы> в меню выбора объектов администрирования отсутствуют.

Снятие всех флагов для выбранного пользователя из группы «Администраторы» не лишает его возможности выполнять загрузку ОС с CD (например, для создания резервных копий дисков или восстановления ОС после сбоя) без привлечения главного администратора; данный пользователь не будет иметь доступа к настройкам комплекса «Аккорд».

3.3.4.4. Результаты ИА

Настройки параметров в разделе «Результаты ИА» для пользователей группы «Администраторы» аналогичны соответствующим настройкам общих параметров для группы «Администраторы».

3.3.5. Параметры пользователей в группе «Обычные»

Для пользователей группы «Обычные» установлены следующие параметры (рисунок 15):

- персональные параметры;
- параметры авторизации;
- параметры пароля;
- результаты ИА (идентификации/аутентификации пользователя).

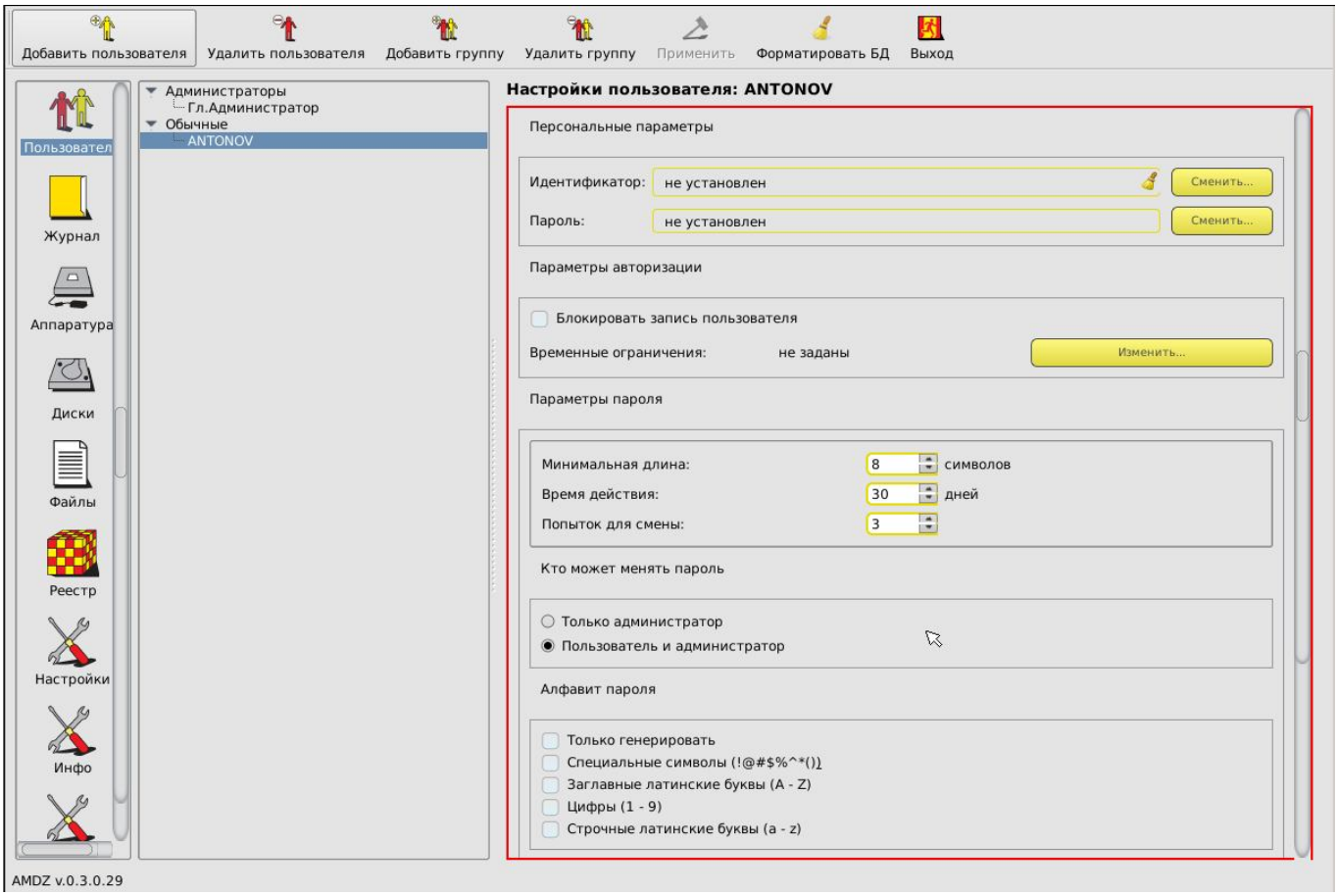

Рисунок 15 – Параметры пользователей в группе «Обычные»

3.3.5.1. Персональные параметры

Настройки персональных параметров пользователей группы «Обычные» аналогичны настройкам соответствующих персональных параметров пользователей группы «Администраторы».

3.3.5.2. Параметры авторизации

Для пользователей группы «Обычные» установлены следующие параметры авторизации:

- режим блокировки;
- временные ограничения.

3.3.5.2.1. 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. Изменить состояние данного флага можно щелчком мыши.

3.3.5.2.2. Временные ограничения

Администратор может устанавливать для пользователя ограничения на вход в систему с точностью до 30 минут в любой день недели. Для этого нужно нажать кнопку <Изменить> в строке «Временные ограничения». На экран выводится окно редактирования параметров «Временные ограничения» (рисунок 16).

Рисунок 16 - Временные ограничения на загрузку компьютера

В строках отображаются дни недели, в столбцах – время с точностью до 30 минут. Мышью можно отметить отдельную ячейку или сразу целую область. Кнопка <OK> подтверждает произведенные изменения.

3.3.5.3. Параметры пароля

Настройки параметров пароля для пользователей группы «Обычные» аналогичны соответствующим настройкам общих параметров пароля для группы «Обычные».

3.3.5.4. Результаты ИА

Настройки параметров в разделе «Результаты ИА» для пользователей группы «Обычные» аналогичны соответствующим настройкам общих параметров для группы «Обычные».

3.4. Регистрация нового администратора

Для выполнения процедуры регистрации нового администратора необходимо установить в списке пользователей курсор на группе «Администраторы» («ADMINS») и нажать кнопку <Добавить пользователя> на панели инструментов.

На экран выводится окно ввода имени пользователя, в котором необходимо задать имя нового пользователя в группе «Администраторы». Администратор должен присвоить каждому пользователю уникальное в данной

вычислительной среде (отдельный компьютер или локальная сеть) имя. В качестве такого уникального имени рекомендуется использовать фамилию пользователя.

Далее необходимо зарегистрировать идентификатор и задать пароль пользователя. Данная процедура аналогична соответствующим процедурам, выполняемым при настройке параметров учетной записи Главного Администратора (подробнее см. в 3.2.1 и 3.2.2).

При вводе нового пользователя общие параметры, установленные для группы, присваиваются ему по умолчанию, но в панели «Настройки пользователя» их можно изменить.

ВНИМАНИЕ! В случае если для регистрации пользователя используется идентификатор с красным стикером, необходимо учитывать, что если контроллер «Аккорд-АМДЗ» используется в составе комплекса «Аккорд NT/2000» v. 3.0, «Аккорд-Win32» или «Аккорд-Win64», регистрацию пользователя следует выполнять только ПОСЛЕ установки СПО на жесткий диск и считывания из ТМ-идентификатора с красным стикером (дискеты, CD-диска) ключевого файла лицензии.

3.5. Регистрация нового пользователя

Для выполнения процедуры регистрации нового пользователя необходимо установить в списке пользователей курсор на группе «Обычные» («EVERYONE») и нажать кнопку <Добавить пользователя> на панели инструментов.

На экран выводится окно ввода имени пользователя, в котором необходимо задать имя нового пользователя. Администратор должен присвоить каждому пользователю уникальное в данной вычислительной среде (отдельный компьютер или локальная сеть) имя. В качестве такого уникального имени рекомендуется использовать фамилию пользователя.

Далее необходимо зарегистрировать идентификатор и задать пароль пользователя. Данная процедура аналогична соответствующим процедурам, выполняемым при настройке параметров учетной записи Главного Администратора (подробнее см. в 3.2.1 и 3.2.2).

При вводе нового пользователя общие параметры, установленные для группы, присваиваются ему по умолчанию, но в панели «Настройки пользователя» их можно изменить.

ВНИМАНИЕ! В случае если для регистрации пользователя используется идентификатор с красным стикером, необходимо учитывать, что если контроллер «Аккорд-АМДЗ» используется в составе комплекса «Аккорд NT/2000» v. 3.0, «Аккорд-Win32» или «Аккорд-Win64», регистрацию пользователя следует выполнять только ПОСЛЕ установки СПО на жесткий диск и считывания из ТМ-идентификатора с красным стикером (дискеты, CD-диска) ключевого файла лицензии.

3.6. Удаление пользователя из списка

Для выполнения процедуры удаления пользователя из списка (рисунок 1) необходимо выбрать и пометить имя пользователя, предназначенного для удаления. Далее нужно нажать кнопку <Удалить пользователя> на панели инструментов и подтвердить удаление.

Пользователя «Гл.Администратор» нельзя удалить из списка.

3.7. Создание новой группы пользователей

Для выполнения процедуры создания новой группы пользователей необходимо в главном окне программы нажать кнопку <Добавить группу> на панели инструментов.

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 3.3.3.

3.8. Удаление группы пользователей

Для выполнения процедуры удаления группы пользователей необходимо в главном окне программы нажать кнопку <Удалить группу> на панели инструментов и в появившемся далее окне кнопкой <OK> подтвердить удаление группы.

Группы «Администраторы» и «Обычные» нельзя удалить из списка.

3.9. Редактирование параметров доступа пользователей

В этом режиме администратор производит изменение параметров доступа пользователя к объектам СЗИ. В подменю списка пользователей (рисунок 1) необходимо выбрать имя пользователя, параметры которого необходимо отредактировать. На правой панели выводятся параметры пользователя. После изменения параметров необходимо нажать кнопку <Применить> на панели инструментов.

3.10.Контроль целостности

В этом режиме администратор контролирует состав и параметры аппаратной части ПЭВМ, целостность системных областей и файлов на жестком диске.

Для выполнения соответствующих операций по контролю целостности в меню выбора объектов администрирования имеется возможность проводить операции администрирования следующих объектов:

- <Аппаратура>;
- <Диски>;
- <Файлы>;
- <Реестр>.

3.10.1. Контроль аппаратуры

ПАК «Аккорд-АМДЗ» позволяет выполнять контроль целостности следующего оборудования:

1) процессоры ЭВМ (подраздел CPU);
2) BIOS;
3) ОЗУ(подраздел MEMORY);
4) жесткие диски, приводы оптических и гибких дисков, (подраздел MEDIA);
5) устройства шины PCI;
6) устройства USB;
7) мониторы.

Для настройки списков контроля целостности аппаратуры в главном окне программы нужно выбрать объект администрирования <Аппаратура> и нажать <Enter>. На экран выводится окно контроля аппаратуры (рисунок 17).

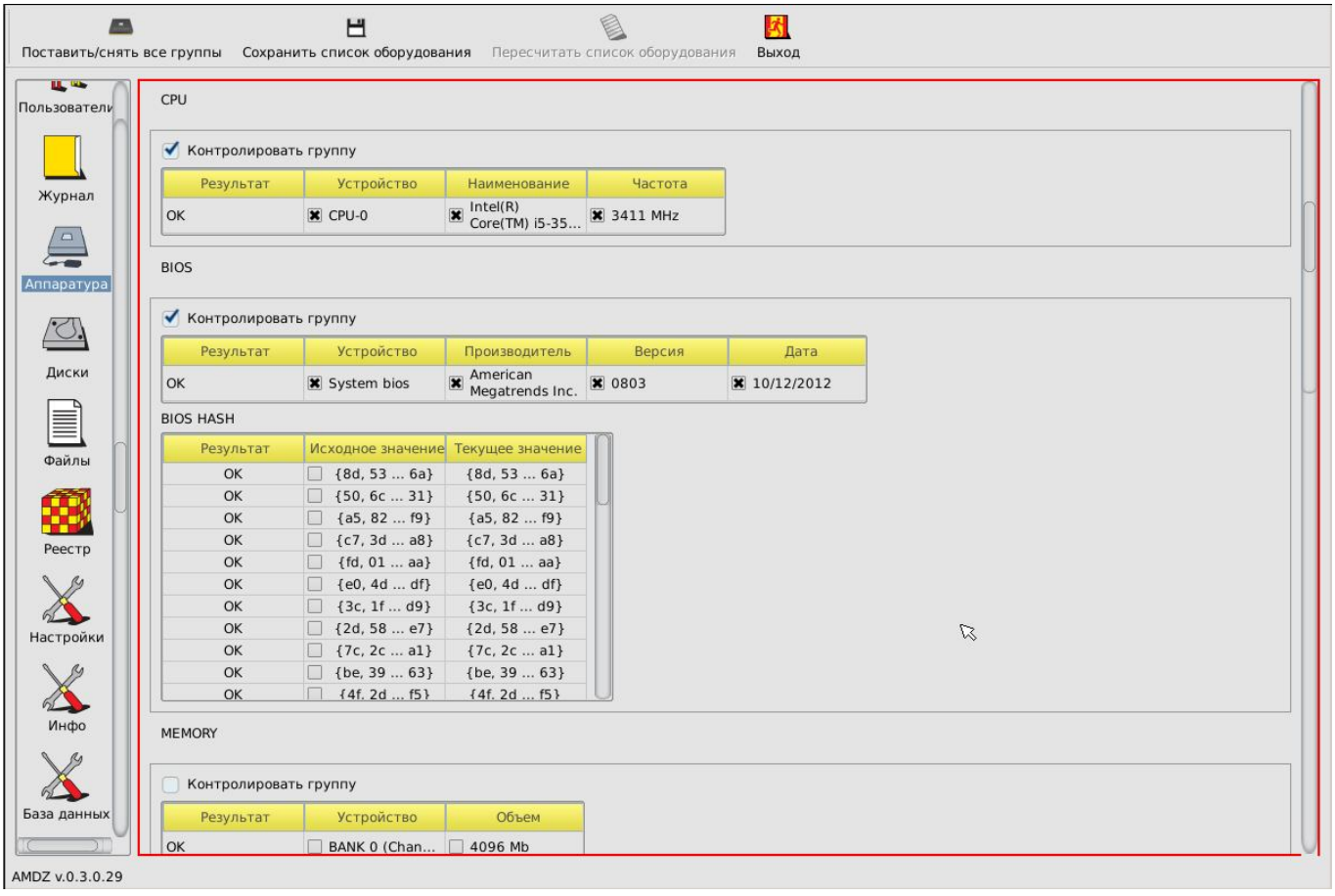

Рисунок 17 - Окно контроля аппаратной части компьютера

В данном окне выводится список классов контролируемых устройств, содержащий отдельные устройства и их параметры. Мышью можно включить/исключить в процедуру контроля любой класс или устройство. На

панели инструментов изменения подтверждаются кнопкой <Сохранить список оборудования>.

ВНИМАНИЕ! Установка на контроль содержимого раздела «BIOS HASH» предполагает обязательную установку на контроль раздела «System BIOS».

В случае нарушения целостности имеется возможность пересчитать контрольные суммы оборудования в сохраненном списке, нажав на кнопку <Пересчитать список оборудования>.

После регистрации в СЗИ «Аккорд-АМДЗ» 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 «Контроль не пройден» и загрузка компьютера блокируется – для обычного пользователя или выводится запрос на администрирование, если идентифицирован администратор.

Может встречаться ситуация, когда после перезагрузки СЗИ «Аккорд-АМДЗ» 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 повторяется сообщение об ошибке контроля аппаратуры. Это означает, что в компьютере установлена «интеллектуальная» материнская плата или устройство с расширенным собственным BIOS. При каждой перезагрузке или выключении они записывают информацию в определенные области своих BIOS. Поскольку каждый раз пересчитывать контрольные суммы того, что меняется при перезагрузке, не имеет смысла, нужно исключить меняющиеся параметры из списка контролируемых объектов и нажать кнопку <Сохранить список оборудования>.

3.10.2. Контроль целостности служебных областей жестких дисков

После выбора объекта администрирования <Диски> в левой панели главного окна программы на экран выводится окно контроля служебных областей дисков (рисунок 18). В рамках контроля поддерживаются файловые системы, список которых приведен в подразделе 1.1 настоящего руководства.

В окне контроля выводится дерево всех дисков, установленных на данном компьютере, с указанием файловой системы каждого диска. Для включения области диска в список контролируемых объектов необходимо мышью отметить контролируемый параметр. Для снятия отметки также используется мышь. В список контролируемых можно вносить служебные области с любых дисков, установленных в компьютере, независимо от файловой системы. Для записи в память контроллера хэш-функций контролируемых областей используется кнопка <Сохранить список оборудования>.

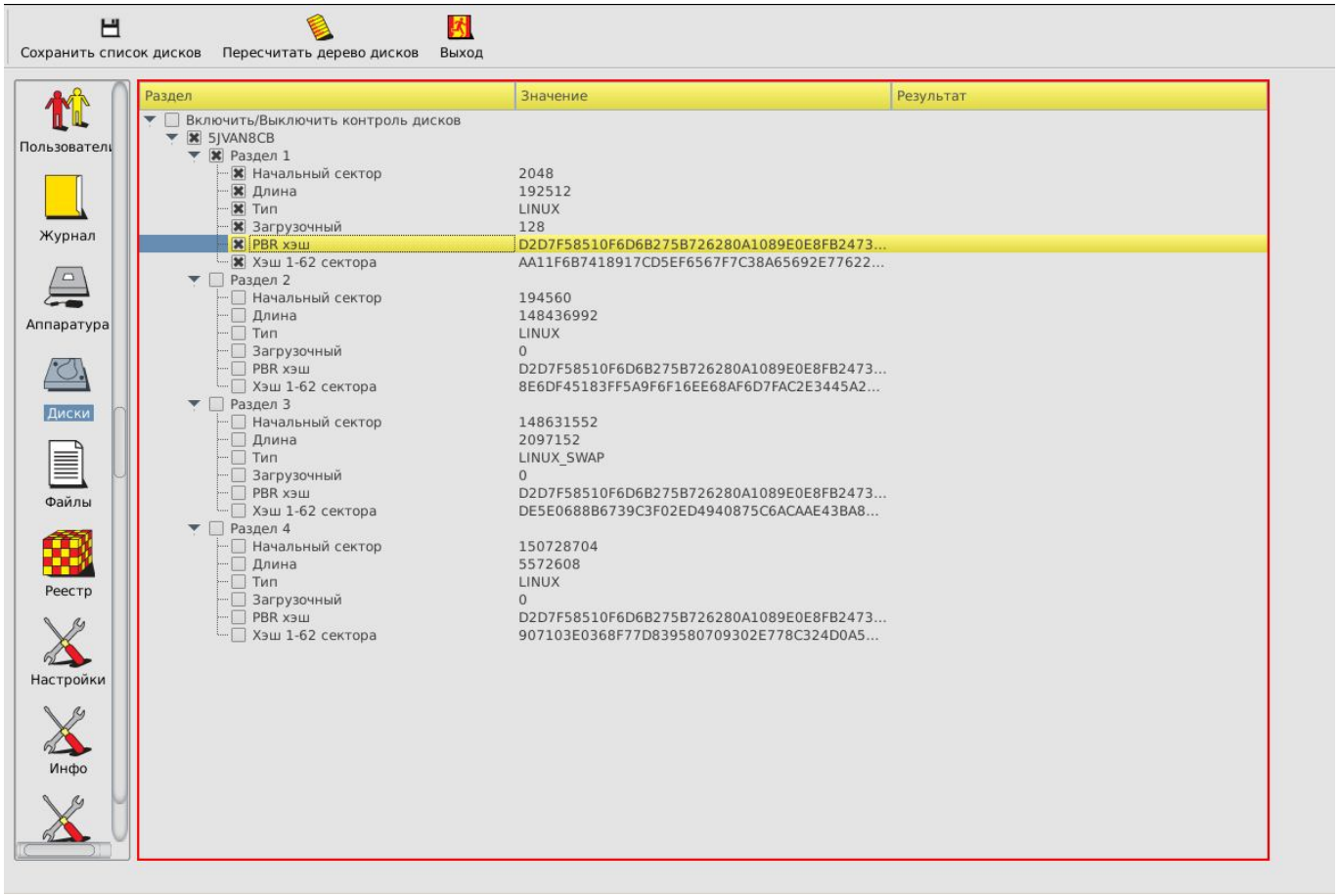

Рисунок 18 - Окно контроля служебных областей диска

3.10.3. Контроль целостности файлов

После выбора объекта администрирования <Файлы> в левой панели на экран выводится окно контроля файлов (рисунок 19). СЗИ «Аккорд-АМДЗ» обеспечивает контроль целостности программ и данных до загрузки ОС, защиту от внедрения разрушающих программных воздействий (РПВ). В рамках контроля поддерживаются файловые системы, список которых приведен в подразделе 1.1 настоящего руководства.

В окне контроля файлов выводится список всех дисков, установленных в системе, с указанием файловой системы каждого диска.

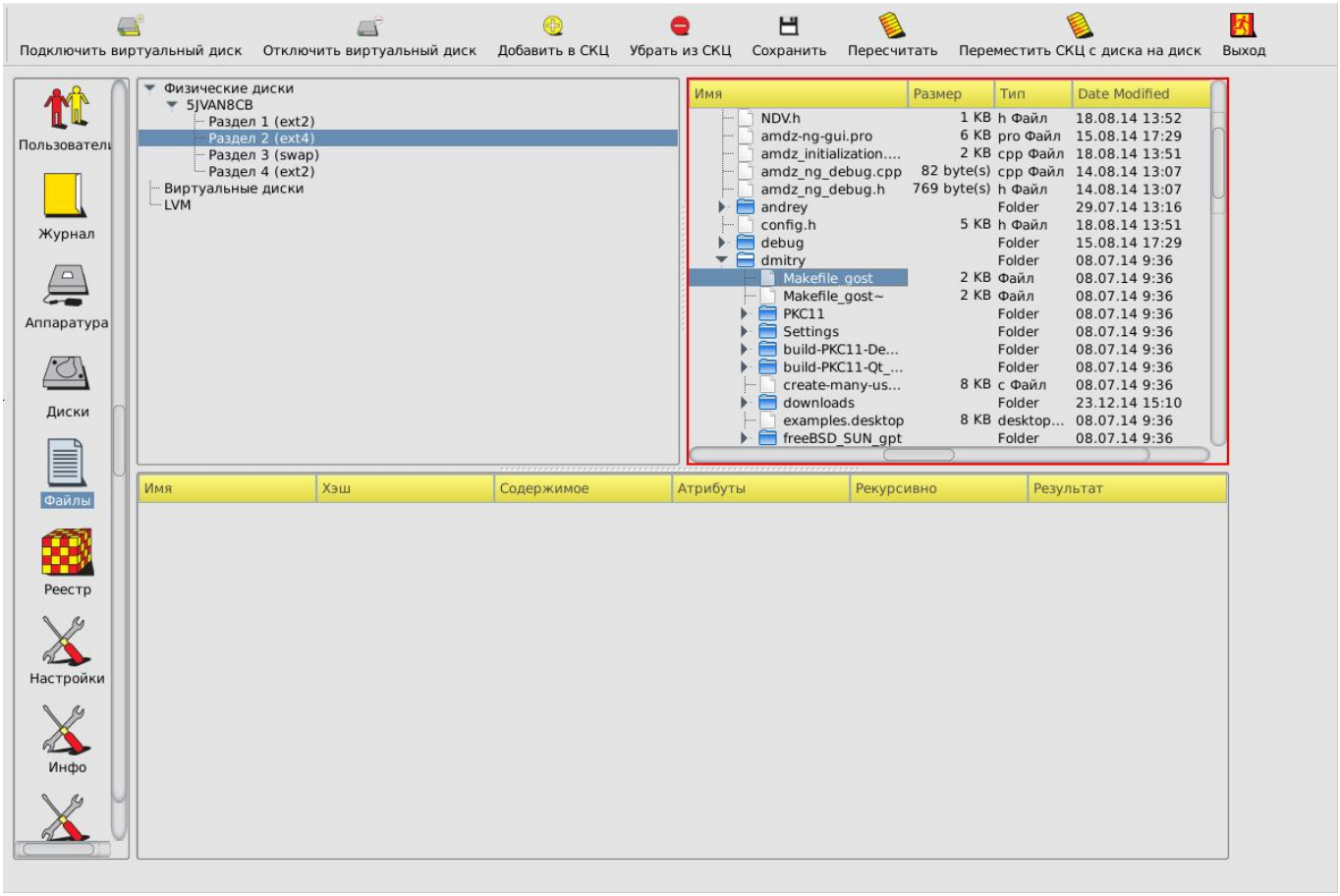

Рисунок 19 - Окно контроля целостности файлов

В правой части экрана можно выбрать конкретные файлы или каталоги.

Добавить каталог в список контроля целостности можно одним из следующих способов:

- выбрать левой кнопкой мыши нужный каталог или файл и нажать кнопку <Добавить в СКЦ> (рисунок 19);
- кликнуть правой кнопкой мыши по нужному файлу или каталогу и выбрать пункт «Добавить» в открывшемся контекстном меню.

В случае если для добавления в список контроля целостности был выбран каталог, на экран выводится окно, в котором необходимо выбрать нужные атрибуты добавления каталога (рисунок 20).

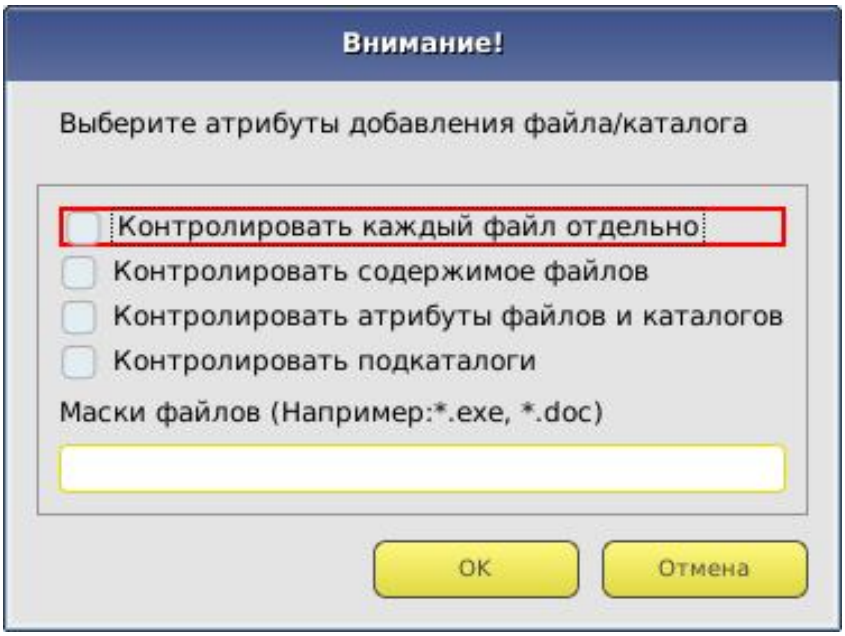

Рисунок 20 – Окно выбора атрибутов добавления каталога

По кнопке <OK> выбранный каталог будет добавлен в список контроля целостности (рисунок 21).

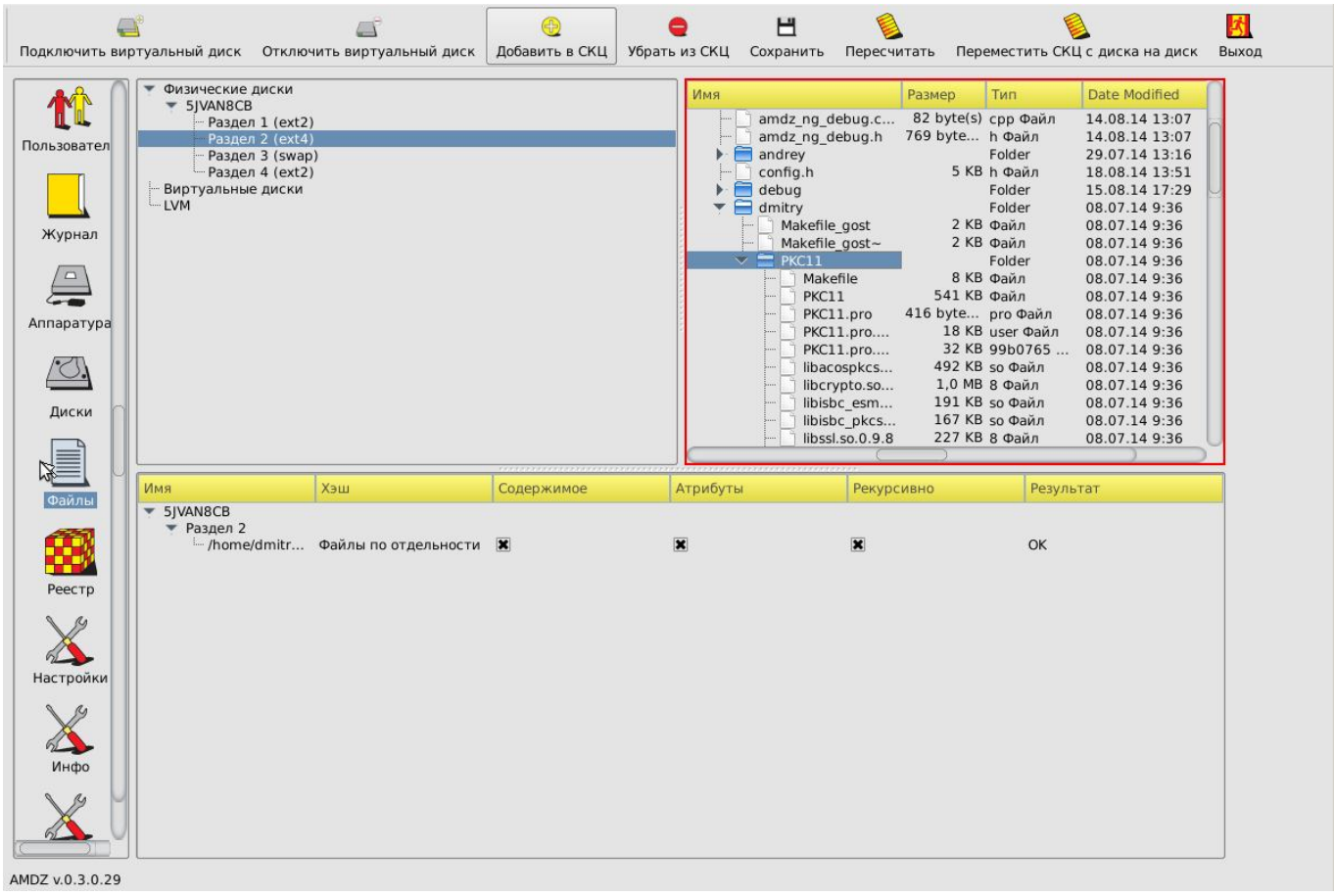

Рисунок 21 – Список контроля целостности с добавленным в него каталогом

В случае если для добавления в список контроля целостности был выбран файл, на экран выводится окно, в котором необходимо выбрать нужные атрибуты добавления файла (рисунок 22).

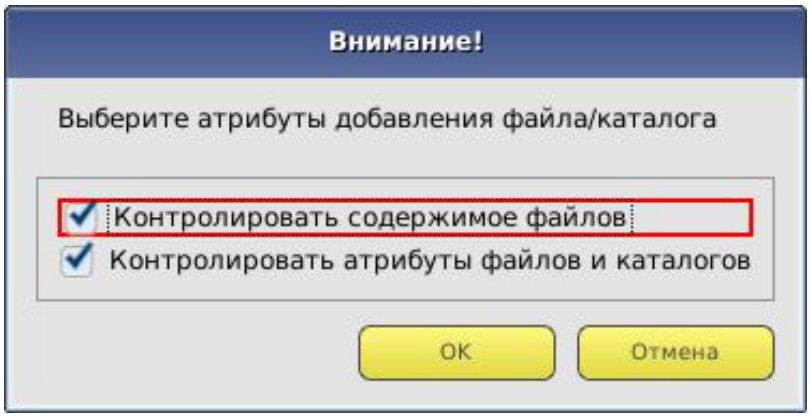

Рисунок 22 – Окно выбора атрибутов добавления файла

По кнопке <OK> выбранный файл будет добавлен в список контроля целостности (рисунок 23).

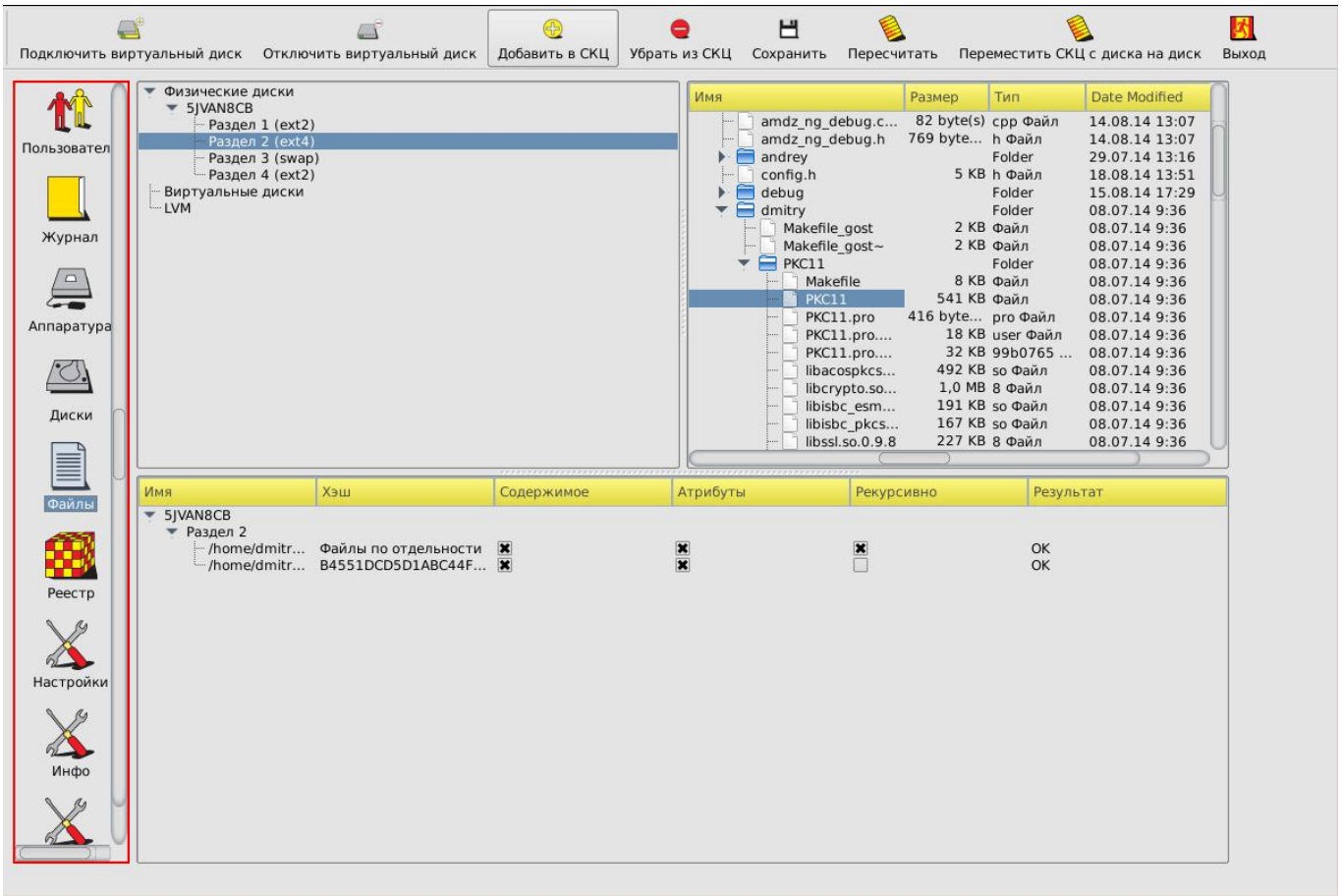

Рисунок 23 – Список контроля целостности с добавленным в него файлом

После добавления в список контролируемых файлов всех необходимых файлов и каталогов по кнопке <Сохранить> данные заносятся в память контроллера.

При необходимости можно убрать отдельный каталог или файл из списка контролируемых, выбрав в списке контроля целостности нужный каталог или файл и нажав кнопку <Убрать из СКЦ>.

В случае нарушения целостности имеется возможность пересчитать контрольные суммы файлов и каталогов в сохраненном списке, нажав на кнопку <Пересчитать>.

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, выдается сообщение «Нарушена целостность» с указанием на каком файле выявлена ошибка и загрузка компьютера блокируется для обычного пользователя, или выводится стартовое меню, если идентифицирован администратор. Администратор, запустив программу администрирования, может выполнить операцию проверки в разделе <Файлы> и выявить измененные файлы.

Примечание: *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. Список файлов ОС Windows 7 (x32, x64), рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»), приведен в Приложении 2.*

3.11. Системный журнал

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

После выбора объекта администрирования <Журнал> в меню выбора объектов администрирования на экран выводится окно системного журнала (рисунок 24). Подробнее об основных параметрах, фиксируемых в журнале, и их обозначениях см. Приложение 1.

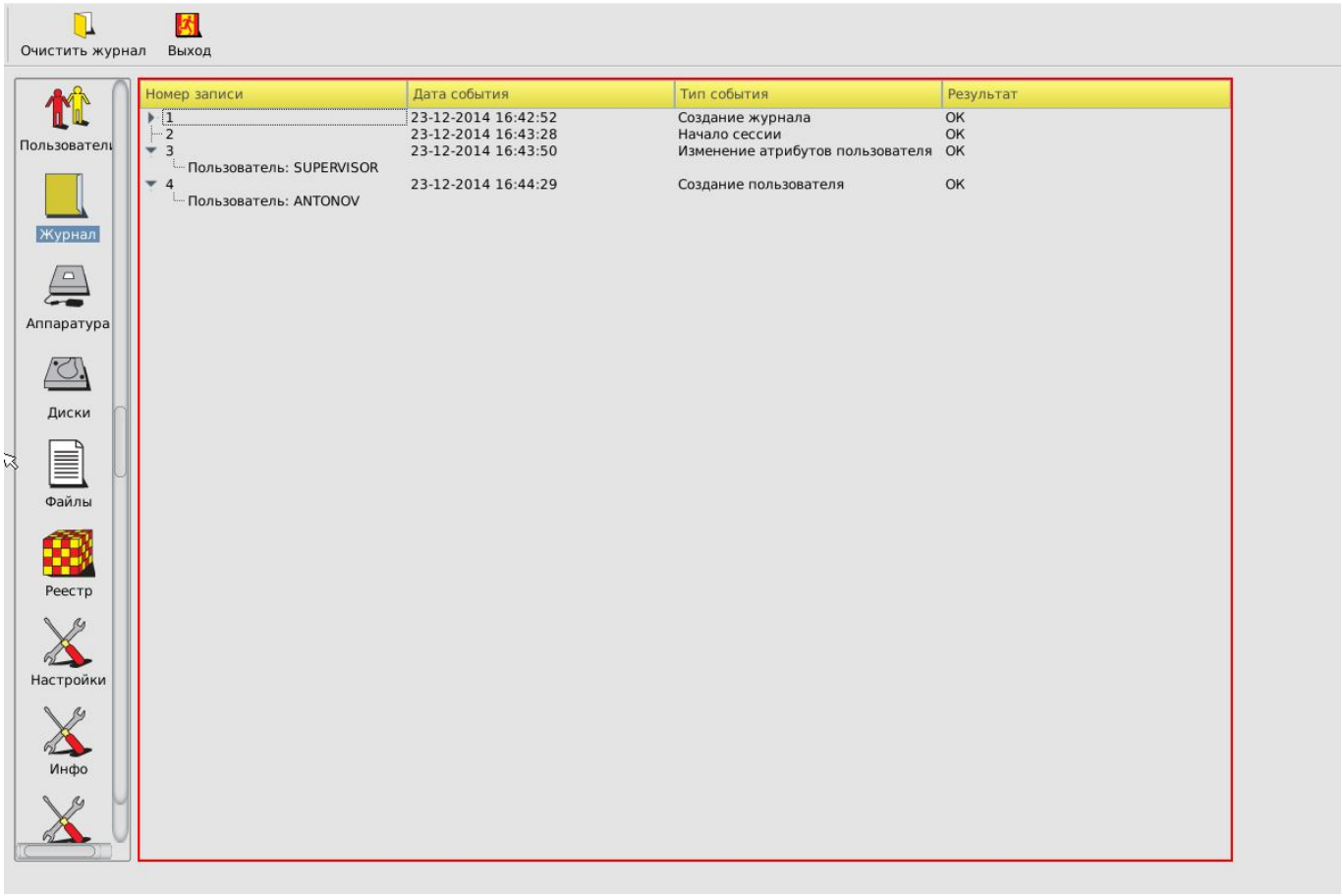

Рисунок 24 - Системный журнал контроллера

Если процент заполнения журнала превышает 85%, при загрузке компьютера выдается предупреждение, но загрузка продолжается. Если процент заполнения журнала превышает 95%, то загрузка для пользователя блокируется и требуется вмешательство администратора. Для очистки журнала служит кнопка <Очистить журнал> (рисунок 24).

3.12. Общие настройки комплекса

Для изменения общих настроек комплекса необходимо нажать кнопку <Настройки> в меню выбора объектов администрирования. На экран выводится окно с настройками комплекса (рисунок 25).

В настройках комплекса установлены следующие разделы:

- данные конфигурации;
- режим запуска ACRUN;
- сторожевой таймер.

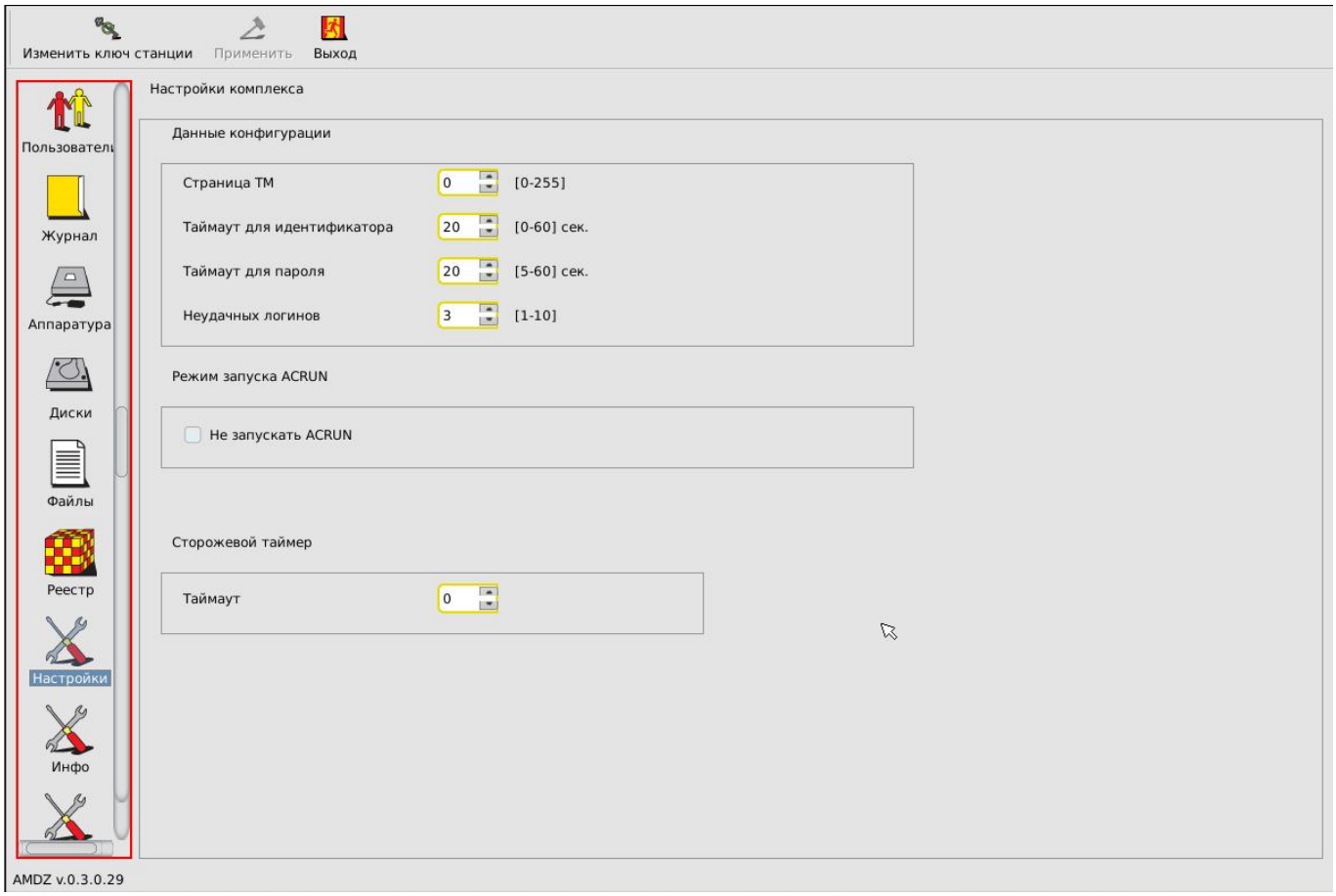

Рисунок 25 – Общие настройки комплекса

3.12.1. Данные конфигурации

Для настроек данных конфигурации установлены следующие параметры:

- страница идентификатора;
- таймаут для идентификатора;
- таймаут для пароля;
- количество неудачных логинов.

«Страница идентификатора» – определяет, с какой страницы внутренней памяти персонального идентификатора располагается служебная информация СЗИ «Аккорд-АМДЗ». 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.

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

«Таймаут для идентификатора» и «Таймаут для пароля» определяют интервал времени, отведенный для процедур начальной идентификации и аутентификации соответственно.

Параметр «Количество неудачных логинов» позволяет определять максимальное количество попыток входа в систему, заканчивающихся неудачей. При превышении допустимого лимита на экран выводится сообщение «Исчерпан лимит попыток ввода пароля или идентификатора» и загрузка становится невозможной. В таком случае необходимо перезагрузить компьютер и заново повторить операцию входа в систему.

3.12.2. Режим запуска ACRUN

Пункт настроек "Режим запуска ACRUN" позволяет изменять режим старта монитора безопасности подсистемы разграничения доступа из состава СПО «Аккорд NT/2000» v. 3.0, «Аккорд-Win32» и «Аккорд-Win64». 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.

3.12.3. Сторожевой таймер

Параметр «Сторожевой таймер» определяет интервал времени в секундах, по истечении которого блокируется возможность загрузки операционной системы, при условии, что за это время управление не передано расширению BIOS АМДЗ.

3.13.Экспорт/импорт баз данных

3.13.1. Общие сведения

Базу данных «Аккорд-АМДЗ» можно скопировать на раздел жесткого диска СВТ или специальный USB-носитель, а в случае необходимости, загрузить эту копию с жесткого диска СВТ или специального USB-носителя (обычный USB-накопитель в случае использования его для выполнения процедур экспорта/импорта списка пользователей, нуждается в специальной подготовке – подробнее см. 3.13.2).

3.13.2. Подготовка USB-носителей для выполнения процедур экспорта/импорта баз данных

Для выполнения процедур экспорта/импорта баз данных необходимо использовать специально подготовленные USB-накопители. Для создания такого накопителя необходимо отформатировать обычный USB-накопитель в файловых системах FAT12, FAT16, FAT32, Ext2, Ext3 или Ext4 с меткой «amdz».

После успешного выполнения описанной последовательности действий накопитель можно использовать для выполнения процедур экспорта/импорта списка пользователей (подробнее см. 3.13.3).

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

3.13.3. Экспорт/импорт баз данных

Для того чтобы начать процедуру экспорта/импорта базы данных «Аккорд-АМДЗ», следует в главном окне программы перейти на вкладку «База данных» и в поле «Носитель» выбрать носитель, на который (с которого) будет выполняться экспорт (импорт) базы данных (рисунок 26).

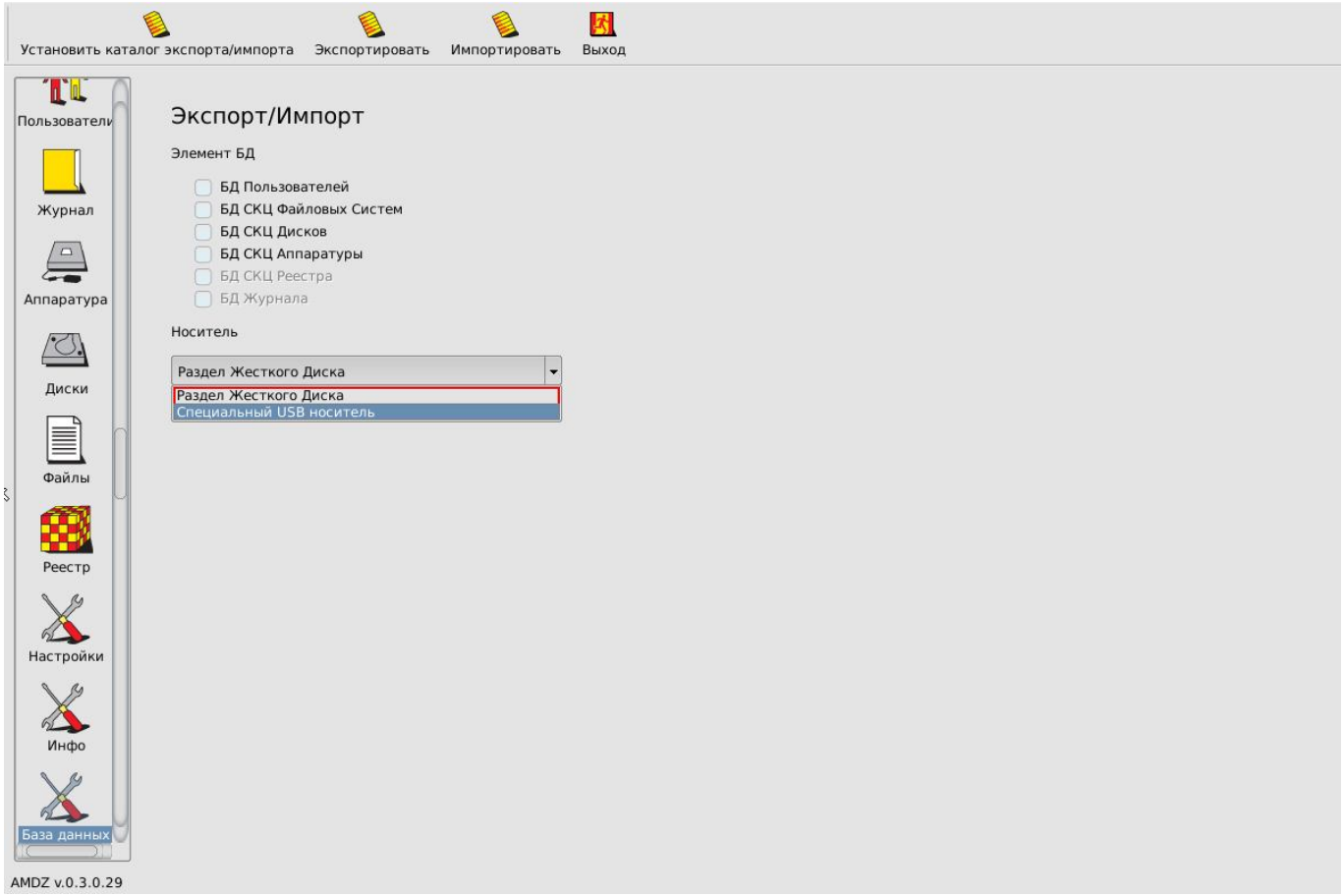

Рисунок 26 - Выбор носителя для экспорта базы пользователей

Далее следует установить директорию экспорта/импорта, нажав на кнопку <Установить директорию экспорта/импорта>, в появившемся окне указав путь к нужной директории и нажав кнопку <OK> (рисунок 27).

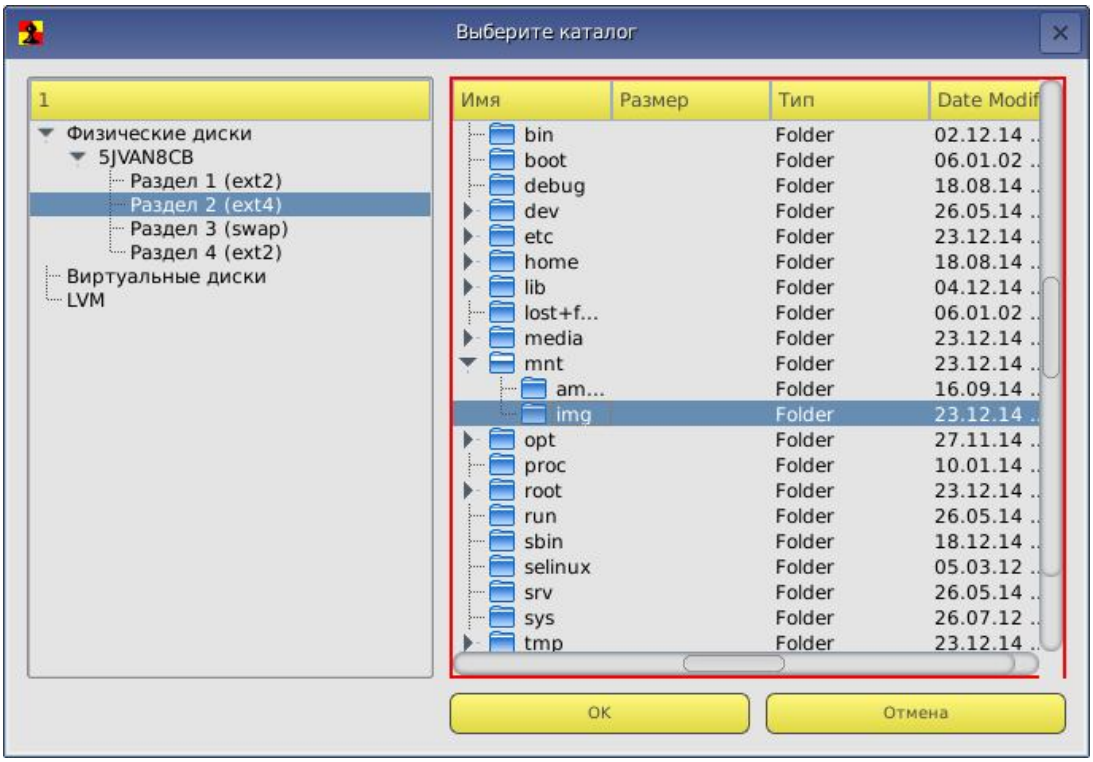

Рисунок 27 - Установка директории экспорта/импорта БД

После установки директории экспорта/импорта следует выбрать нужные элементы БД, указав их галочками, и нажать кнопку <Экспортировать>/<Импортировать> (рисунок 26).

ВНИМАНИЕ! Не отключайте специальный USB-носитель сразу после появления сообщения «Данные успешно экспортированы». Для корректного завершения процедуры экспорта БД нужно обязательно перезагрузить ПК с подключенным USB-носителем!

3.14. Форматирование баз данных контроллера

Процедура форматирования баз данных контроллера, вызываемая кнопкой <Форматировать БД> на вкладке «Пользователи» главного окна программы администрирования, позволяет Главному Администратору очистить все внутренние базы данных без перевода контроллера в технологический режим, т.е. провести повторную инициализацию контроллера без вскрытия корпуса компьютера.

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

Данная функция может пригодиться 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 нужно проверить работоспособность компьютера, а для этого нужно зарегистрировать идентификатор Главного Администратора и ввести пароль. Специалисту,

который выполняет проверку, придется для каждого компьютера регистрировать отдельный идентификатор и прикладывать к нему бумажку с записанным паролем, а можно выполнять 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 на вкладке «Пользователи» главного окна программы администрирования нажать кнопку <Форматировать БД> (рисунок 28).

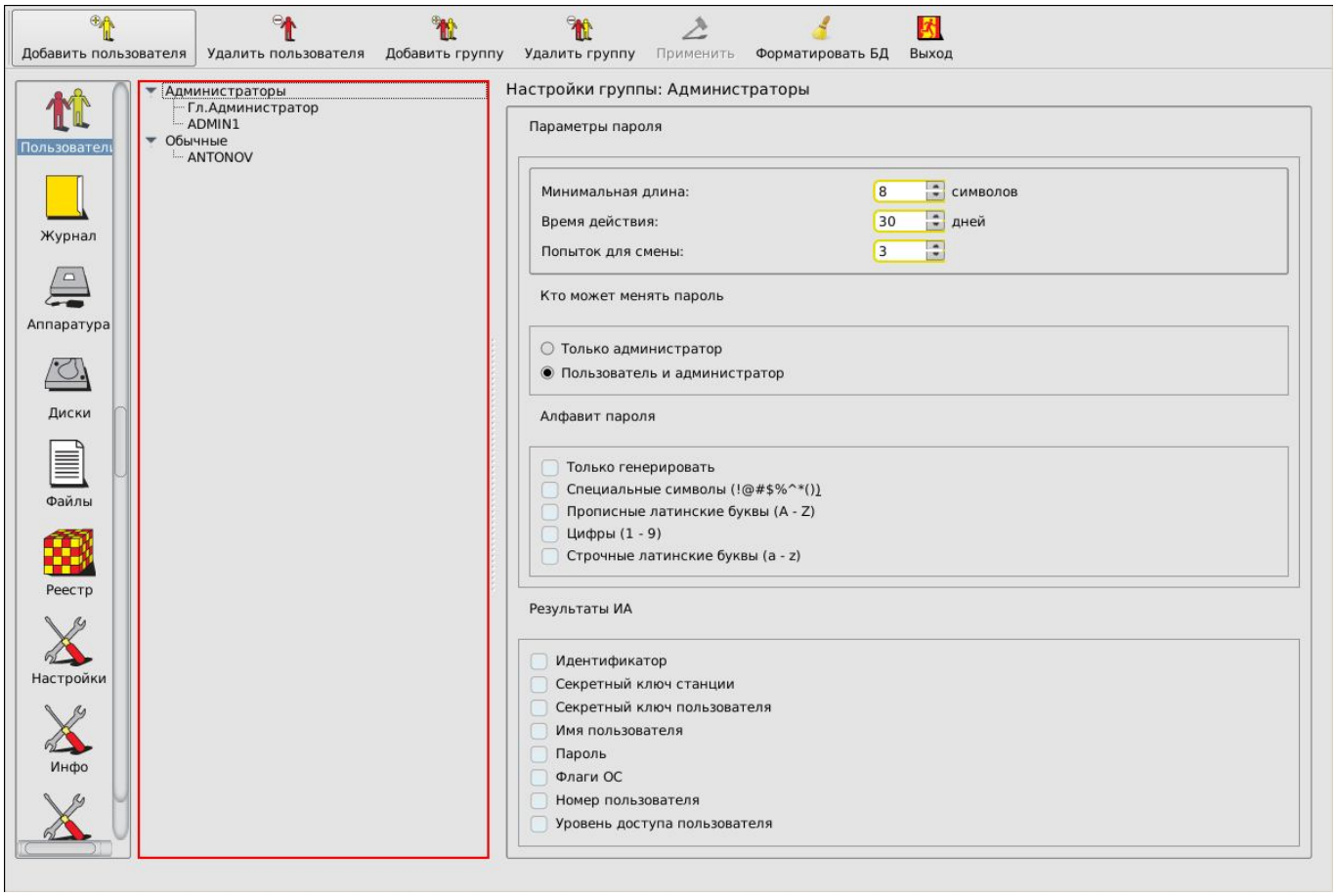

Рисунок 28 - Главное окно программы администрирования. Кнопка <Форматировать БД>

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 кнопкой <Форматировать БД>, следует выполнять процедуру аппаратной очистки баз данных (подробнее см. раздел 4).

3.15. Работа с дополнительным функционалом «Аккорд-АМДЗ» – СУЦУ

В «Аккорд-АМДЗ» предусмотрена возможность работы в режиме удаленного централизованного управления (СУЦУ).

Данный функционал доступен для «Аккорд-АМДЗ» с вариантами исполнения ФПО 3 и 4. Вариант исполнения прошивки «Аккорд-АМДЗ» см. в разделе «Свидетельство о приемке» (пункт «Вариант исполнения ФПО») Формуляра (11443195.4012.038 30), входящего в комплект поставки комплекса

Работа с функционалом СУЦУ выполняется в главном окне программы администрирования на вкладке «СУЦУ» (рисунок 29).

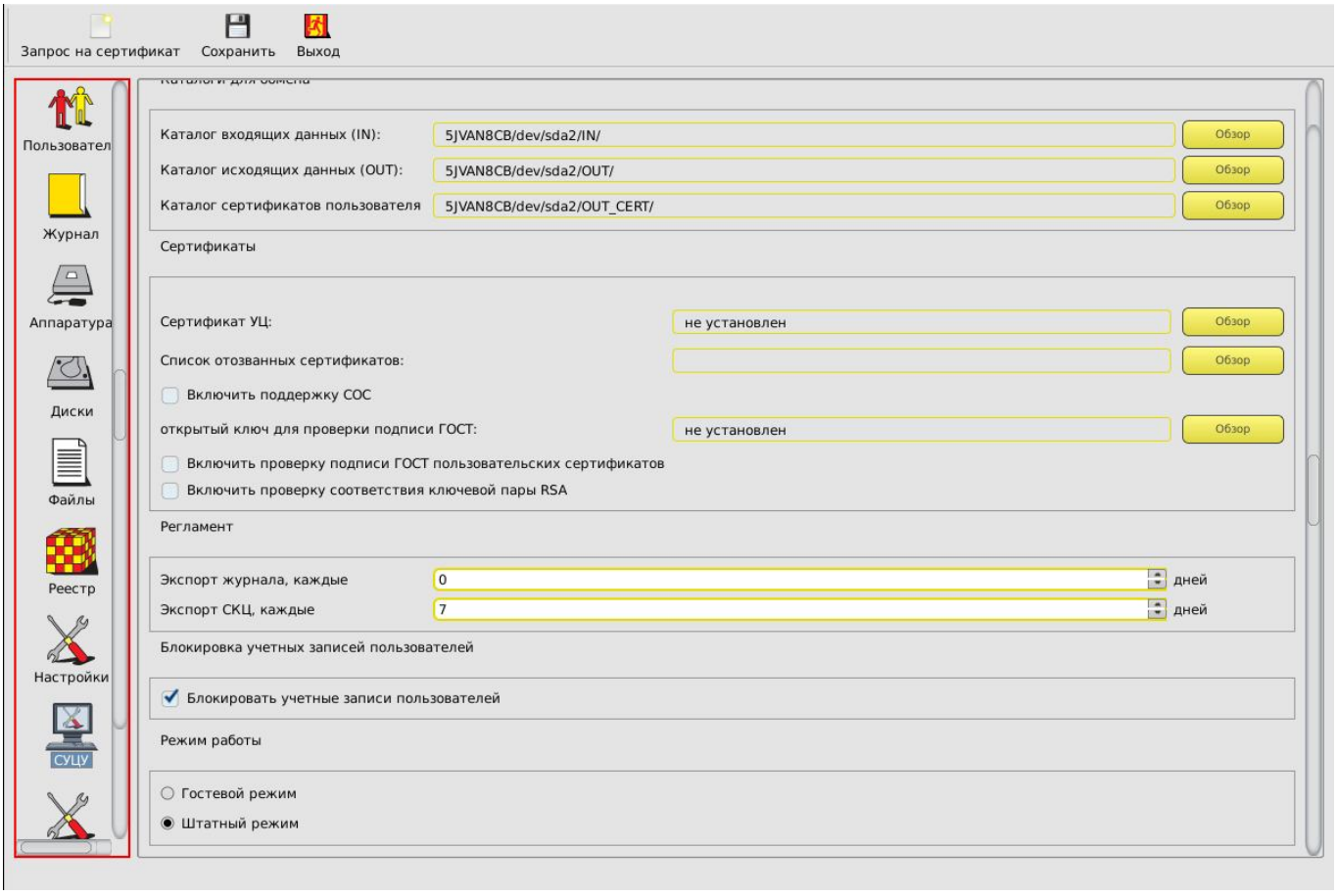

Рисунок 29 - Дополнительный функционал «Аккорд-АМДЗ» – СУЦУ

На вкладке «СУЦУ» доступны для установки следующие параметры.

«Включить СУЦУ» – установка галочки напротив данного пункта позволяет включить модуль поддержки удаленных операций. Снятие галочки влечет за собой прекращение работы с СУЦУ и продолжение работы «Аккорд-АМДЗ» в обычном, локальном, режиме.

«Каталоги для обмена»:

- «Каталог входящих данных (IN)» – каталог, из которого «Аккорд-АМДЗ» считывает входящие файлы-сообщения протокола удаленного управления;
- «Каталог исходящих данных (OUT)» - каталог, в который «Аккорд-АМДЗ» помещает ответные квитанции на соответствующие запросы удаленного управления;
- «Каталог сертификатов пользователя (OUT_CERT)» - каталог в который «Аккорд-АМДЗ» сохраняет сертификаты, по которым произошла аутентификация пользователя.

«Регламент»:

- «Экспорт журнала, каждые» – данный параметр определяет периодичность (в днях), с которой выполняется процедура автоматического экспорта журнала;
- «Экспорт СКЦ, каждые» – данный параметр определяет периодичность (в днях), с которой выполняется процедура автоматического экспорта списков контроля целостности.

«Сертификаты»:

- «Сертификат УЦ» – кнопка <Обзор> в данном поле позволяет выбрать на диске и загрузить в базу «Аккорд-АМДЗ» сертификат удостоверяющего центра. В соответствующем поле указано, установлен или нет на данный момент какой-либо сертификат УЦ;
- «Список отозванных сертификатов (СОС)» – показывает путь до списка отозванных сертификатов на диске, кнопка <Обзор> позволяет указать и установить данный путь;
- «Включить поддержку СОС» – установка (снятие) галочки напротив данного пункта позволяет включить (отключить) проверку по СОС;
- «Открытый ключ для проверки подписи ГОСТ» – показывает, установлен или нет (есть ли в базе) ключ для проверки подписи пользовательского сертификата. Кнопка <Обзор> позволяет выбрать на жестком диске открытый ключ для проверки подписи и записать его в базу;
- «Включить проверку подписи ГОСТ пользовательских сертификатов» – установка (снятие) галочки напротив данного пункта включить (отключить) проверку подписи сертификатов;
- «Включить проверку соответствия ключевой пары RSA» – установка (снятие) галочки напротив данного пункта позволяет включить (отключить) взаимопроверку соответствия открытого ключа в сертификате пользователя и закрытого в идентификаторе.

«Блокировка учетных записей пользователей»:

«Блокировать учетные записи пользователей» – установка (снятие) галочки напротив данного пункта позволяет включить (отключить) блокировку учетных записей пользователей, не входящих в группу «Администраторы».

«Режим работы»:

- «Гостевой режим» – выбор данного пункта позволяет включить гостевой режим аутентификации;
- «Штатный режим» – выбор данного пункта позволяет включить штатный режим аутентификации.

3.16. Выход из программы

Выход из программы администрирования выполняется по нажатию кнопки <Выход> в главном меню. После этого на экране появляется запрос дальнейших действий администратора. Администратор может выбрать вариант загрузки или перезагрузить компьютер.

4. Аппаратная очистка баз данных

Функция аппаратной очистки баз данных необходима при утере идентификатора администратора или при передаче компьютера в другое подразделение, где есть собственный администратор БИ и иной состав пользователей.

Для того чтобы выполнить операцию аппаратной 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 98/11443195.4012.038 98)).

3) Вставить плату в компьютер.

4) Загрузить с CD и запустить программу ipgx.exe (данная программа находится в каталоге UTILS на CD, прилагаемом к контроллеру «Аккорд-АМДЗ»).

5) Выключить компьютер, вернуть контроллер в рабочий режим (подробнее см. пункт «Режимы доступа к аппаратным ресурсам платы контроллера» «Руководства по установке» (11443195.4012.006 98/11443195.4012.038 98)).

6) Установить контроллер в компьютер.

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

5. Программная активация/деактивация СЗИ НСД без механических операций вскрытия и установки или извлечения компонентов

В случае необходимости можно выполнить процедуру активации/деактивации СЗИ НСД «Аккорд-АМДЗ» программным образом, без выполнения механических операций вскрытия и установки/извлечения компонентов. Данная процедура выполняется администратором комплекса.

Для этого следует скопировать утилиту программной активации/деактивации комплекса amdzctrl.exe в каталог Accord.NT и запустить ее с правами администратора. В появившемся окне следует выполнить соответствующую команду:

- «AMDZCTRL /A» – для активации комплекса;
- «AMDZCTRL /D» – для деактивации комплекса.

В процессе выполнения процедуры активации/деактивации комплекса на экран выводится запрос идентификатора и пароля администратора комплекса[1].

Процедура активации/деактивации комплекса может быть вызвана также нажатием кнопки <Ctrl> в процессе старта компьютера. Далее, в ответ на запрос «Press Ctrl-A to activate...», следует нажать клавишу <A>, затем (в ответ на запрос «Press any key to reboot») – любую клавишу на клавиатуре. По нажатии любой клавиши выполняется перезагрузка компьютера с уже активным комплексом «Аккорд-АМДЗ».

[1)] Поддерживаемые идентификаторы определяются настройкой идентификаторов в установленном на СВТ ПАК СЗИ НСД «Аккорд-Win32»/«Аккорд-Win64»

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(499)235-89-17, +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

Событие	Результат
Лог Создан	ОК
Старт Сессии	ОК
Логин пользователя	Таймаут идентификатора
	Таймаут пароля
	Неизвестный идентификатор
	Неверный пароль
	Пользователь Заблокирован
	Временное ограничение для пользователя
Проверка целостности аппаратуры	ОК
	Ошибка целостности
Проверка целостности дисков	ОК
	Ошибка целостности
Проверка целостности объектов ФС	ОК
	Ошибка целостности
Проверка целостности реестра	ОК
	Ошибка целостности
База данных Пуста ОК	ОК
Изменен пароль пользователя	ОК
Создан новый пользователь	ОК
Удален пользователь	ОК
Изменены атрибуты пользователя	ОК
Создана новая группа	ОК
Удалена группа	ОК
Модифицированы атрибуты	ОК
Импорт базы данных	ОК
Экспорт базы данных	ОК
Модификация СКЦ Дисков	ОК
Модификация СКЦ Аппаратуры	ОК
Модификация СКЦ объектов ФС	ОК
Неизвестная ошибка	Неизвестная Ошибка

Приложение 2.
Список файлов ОС Windows 7, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»)

Список файлов ОС Windows 7 x32, рекомендованный к контролю на аппаратном уровне.

\Windows\Explorer.EXE
\Windows\system32\audidog.exe
\Windows\system32\autochk.exe
\Windows\System32\comctl32.dll
\Windows\System32\csrsrv.dll
\Windows\system32\csrss.exe
\Windows\system32\DllHost.exe
\Windows\System32\drivers\acpi.sys
\Windows\System32\drivers\ataport.SYS
\Windows\System32\drivers\blbdrive.sys
\Windows\System32\drivers\bowser.sys
\Windows\System32\drivers\CLASSPNP.SYS
\Windows\System32\drivers\CLFS.SYS
\Windows\System32\drivers\cng.sys
\Windows\System32\drivers\csc.sys
\Windows\System32\drivers\disk.sys
\Windows\System32\drivers\dxgkrnl.sys
\Windows\System32\drivers\dxgmms1.sys
\Windows\System32\drivers\fileinfo.sys
\Windows\System32\drivers\fltmgr.sys
\Windows\System32\drivers\fvevol.sys
\Windows\System32\drivers\hdaudbus.sys
\Windows\System32\drivers\http.sys
\Windows\System32\drivers\luafv.sys
\Windows\System32\drivers\msrpc.sys
\Windows\System32\drivers\ndis.sys
\Windows\System32\drivers\NETIO.SYS
\Windows\System32\drivers\npfs.sys
\Windows\System32\drivers\nsiproxy.sys
\Windows\System32\drivers\ntfs.sys
\Windows\System32\drivers\pacer.sys
\Windows\System32\drivers\partmgr.sys
\Windows\System32\drivers\PCIIDEX.SYS
\Windows\System32\drivers\raspptp.sys
\Windows\System32\drivers\rdbss.sys
\Windows\System32\drivers\rdyboost.sys
\Windows\System32\drivers\serenum.sys
\Windows\System32\drivers\srv.sys
\Windows\System32\drivers\srv2.sys
\Windows\System32\drivers\tcpip.sys
\Windows\System32\drivers\volmgr.sys
\Windows\System32\drivers\volsnap.sys
\Windows\System32\drivers\watchdog.sys
\Windows\System32\drivers\Wdf01000.sys
\Windows\system32\Dwm.exe
\Windows\System32\dwmcore.dll
\Windows\System32\gdi32.dll

\Windows\System32\halmacpi.dll
\Windows\System32\hkcmd.exe
\Windows\System32\kernel32.dll
\Windows\System32\KernelBase.dll
\Windows\System32\LogonUI.exe
\Windows\System32\lsasrv.dll
\Windows\system32\lsass.exe
\Windows\system32\lsm.exe
\Windows\System32\ntdll.dll
\Windows\System32\ntkrnlpa.exe
\Windows\System32\ntoskrnl.exe
\Windows\System32\rundll32.exe
\Windows\system32\SearchIndexer.exe
\Windows\system32\SearchProtocolHost.exe
\Windows\System32\smss.exe
\Windows\System32\spoolsv.exe
\Windows\system32\svchost.exe
\Windows\system32\taskhost.exe
\Windows\System32\user32.dll
\Windows\system32\userinit.exe
\Windows\System32\win32k.sys
\Windows\system32\wininit.exe
\Windows\system32\winlogon.exe
\Windows\System32\xbootmgr.exe
<диск с каталогом Boot>\Boot\BOOTSTAT.DAT
<диск с каталогом Boot>\Boot\memtest.exe

Список файлов ОС Windows 7 x64, рекомендованный к контролю на аппаратном уровне.

\Windows\Explorer.EXE
\Windows\System32\audiodg.exe
\Windows\System32\autochk.exe
\Windows\System32\consent.exe
\Windows\System32\csrsrv.dll
\Windows\System32\csrss.exe
\Windows\System32\dllhost.exe
\Windows\System32\drivers\ACPI.sys
\Windows\System32\drivers\afd.sys
\Windows\System32\drivers\atapi.sys
\Windows\System32\drivers\ataport.SYS
\Windows\System32\drivers\blbdrive.sys
\Windows\System32\drivers\bowser.sys
\Windows\System32\drivers\CLASSPNP.SYS
\Windows\System32\drivers\CLFS.SYS
\Windows\System32\drivers\cng.sys
\Windows\System32\drivers\csc.sys
\Windows\System32\drivers\dxgkrnl.sys
\Windows\System32\drivers\dxgmms1.sys
\Windows\System32\drivers\fileinfo.sys
\Windows\System32\drivers\fltmgr.sys
\Windows\System32\drivers\fvevol.sys
\Windows\System32\drivers\hdaudbus.sys
\Windows\System32\drivers\http.sys
\Windows\System32\drivers\i8042prt.sys
\Windows\System32\drivers\intelppm.sys

\Windows\System32\drivers\luafv.sys
\Windows\System32\drivers\mpsdrv.sys
\Windows\System32\drivers\msrpc.sys
\Windows\System32\drivers\ndis.sys
\Windows\System32\drivers\netbt.sys
\Windows\System32\drivers\NETIO.SYS
\Windows\System32\drivers\nsiproxy.sys
\Windows\System32\drivers\Ntfs.sys
\Windows\System32\drivers\nwifi.sys
\Windows\System32\drivers\partmgr.sys
\Windows\System32\drivers\pciide.sys
\Windows\System32\drivers\PCIIDEX.SYS
\Windows\System32\drivers\raspptp.sys
\Windows\System32\drivers\rdbss.sys
\Windows\System32\drivers\rdyboost.sys
\Windows\System32\drivers\Rt64win7.sys
\Windows\System32\drivers\serenum.sys
\Windows\System32\drivers\serial.sys
\Windows\System32\drivers\srv.sys
\Windows\System32\drivers\srv2.sys
\Windows\System32\drivers\tcpip.sys
\Windows\System32\drivers\tdi.sys
\Windows\System32\drivers\usbehci.sys
\Windows\System32\drivers\usbport.sys
\Windows\System32\drivers\volmgr.sys
\Windows\System32\drivers\volsnap.sys
\Windows\System32\drivers\vwififlt.sys
\Windows\System32\drivers\watchdog.sys
\Windows\System32\drivers\Wdf01000.sys
\Windows\System32\drivers\wdmaud.drv
\Windows\System32\dwm.exe
\Windows\System32\gdi32.dll
\Windows\System32\hal.dll
\Windows\System32\hkcmd.exe
\Windows\System32\kernel32.dll
\Windows\System32\KernelBase.dll
\Windows\System32\LogonUI.exe
\Windows\System32\lsasrv.dll
\Windows\System32\lsass.exe
\Windows\System32\lsm.exe
\Windows\System32\ntdll.dll
\Windows\System32\ntoskrnl.exe
\Windows\System32\SearchIndexer.exe
\Windows\System32\services.exe
\Windows\System32\smss.exe
\Windows\System32\spoolsv.exe
\Windows\System32\svchost.exe
\Windows\System32\taskhost.exe
\Windows\System32\user32.dll
\Windows\System32\userinit.exe
\Windows\System32\win32k.sys
\Windows\System32\wininit.exe
\Windows\System32\winlogon.exe
<диск с каталогом Boot>\Boot\BOOTSTAT.DAT
<диск с каталогом Boot>\Boot\memtest.exe