ОКБ АПР
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

11443195.4012.054 90

37222406.26.20.40.140.079 90

Листов 121

Москва
2019

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 его 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, Аккорд-GXM2 (для СЗИ НСД «Аккорд-АМДЗ», выпускаемого по ТУ 4012-038-11443195-2011);
- Аккорд-GX, Аккорд-GXMH, Аккорд-GXM2 (для СЗИ НСД «Аккорд-АМДЗ», выпускаемых по ТУ 4012-054-11443195-2013);
- Аккорд-GX, Аккорд-GXMH, Аккорд-GXM, Аккорд-GXM2 (для СЗИ НСД «Аккорд-АМДЗ», выпускаемых по ТУ 26.20.40.140-079-37222406-2019).

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

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 (супервизор). 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 ресурсов СВТ с использованием алгоритма пошагового контроля целостности.

Идентификатор – специальное устройство, содержащее уникальный признак пользователя, с которым зарегистрированный пользователь входит в систему и который используется системой для определения его прав, а также для регистрации факта доступа и характера выполняемых им работ или предоставляемых ему услуг.

Пользователь – субъект доступа к объектам (ресурсам) СВТ.

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

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
ПЭВМ	Персональная электронно-вычислительная машина
РС	Рабочая станция
СВТ	Средство вычислительной техники
СЗИ	Средство защиты информации
ТУ	Технические условия
СКЦ	Список (списки) контроля целостности

1. Общие сведения

1.1. Назначение комплекса

ПАК СЗИ НСД «Аккорд-АМДЗ» является программно-техническим средством, которое реализует функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки и прошел сертификационные испытания:

- в ФСТЭК России в соответствии с требованиями документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты. ИТ.СДЗ. ПР4.ПЗ» (ФСТЭК России, 2013) при выполнении ограничений, указанных в ТУ 4012-038-11443195-2011;
- в ФСБ России на соответствие требованиям к аппаратно-программным модулям доверенной загрузки ЭВМ по 1-му классу защиты и классу сервиса Б (ТУ 4012-054-11443195-2013);
- в ФСТЭК России в соответствии с требованиями документов «Требования к средствам доверенной загрузки» (ФСТЭК России, 2013), «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) и «Профиль защиты средства доверенной загрузки уровня платы расширения второго класса защиты. ИТ.СДЗ.ПР2.ПЗ» (ФСЭК России, 2013) при выполнении ограничений, указанных в ТУ 26.20.40.140-079-37222406-2019.

ПАК СЗИ НСД «Аккорд-АМДЗ» обеспечивает нейтрализацию следующих основных угроз безопасности информации:

- несанкционированный доступ к информации за счет загрузки нештатной операционной системы (ОС) и обхода правил разграничения доступа штатной ОС и (или) других средств защиты информации, работающих в среде штатной ОС;
- нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе;
- нарушение целостности программного обеспечения средства доверенной загрузки;
- несанкционированное изменение конфигурации (параметров) средств доверенной загрузки;
- преодоление или обход функций безопасности средств доверенной загрузки.

Комплекс начинает работу сразу после выполнения кода системного BIOS компьютера – до загрузки операционной системы, и обеспечивает доверенную загрузку[1] для ОС, поддерживающих файловые системы:

- FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX, Ext4, ReiserFS (ТУ 4012-038-11443195-2011);

- FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX, Ext4, ReiserFS (ТУ 4012-054-11443195-2013);

- FAT12, FAT16, FAT32, NTFS, Ext2, Ext3 Ext4, FreeBSD UFS/UFS2, QNX4, QNX6, XFS (ТУ 26.20.40.140-079-37222406-2019).

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);
- 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;
- контроль целостности объектов файловых систем, размещенных на динамических дисках;
- 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(е)») 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(е)»);
- администрирование встроенного ПО комплекса (регистрацию пользователей и персональных идентификаторов, назначение файлов для контроля целостности, контроль аппаратной части ПЭВМ (РС), просмотр системного журнала);

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

- 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.

1.2. Состав комплекса

Комплекс СЗИ НСД «Аккорд-АМДЗ» выпускается в программно-аппаратном исполнении и включает:

- специализированный контроллер (далее по тексту – контроллер);
- функциональное программное обеспечение (далее по тексту - ФПО), размещаемое в энергонезависимой флэш-памяти специализированного контроллера.

Модификация контроллера определяется размером и шинным интерфейсом.

ФПО является ядром защиты и реализует комплекс мер по защите информации от НСД.

В состав программных средств (ФПО), размещенных в энергонезависимой памяти контроллера комплекса, входят следующие функциональные модули:

- средства идентификации пользователей;
- средства аутентификации пользователей;
- средства контроля целостности технических средств ПЭВМ (РС);
- 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 (среда администрирования).

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

Среда администрирования является частью комплекса «Аккорд-АМДЗ» и не требует установки какого-либо дополнительного ПО. С помощью нее

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.

Модификация контроллера оговаривается при поставке комплекса и указывается в Формуляре (11443195.4012.038 30, 11443195.4012.054 ФО, 37222406.26.20.40.140.079 30). Подробнее о контроллерах «Аккорд-АМДЗ», а также об устройствах, с которыми СЗИ НСД «Аккорд-АМДЗ» поддерживает работу, см. «Руководство по установке», входящее в комплект поставки комплекса.

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 на материнской плате ПЭВМ свободного слота PCI/ PCI-X/ PCI-Express/ miniPCI-Express/ M2 – в соответствии с типом специализированного контроллера.

Технические средства защищаемой ПЭВМ (PC) не должны содержать аппаратно-программных механизмов, ориентированных на целенаправленное нарушение правильности функционирования комплекса.

В составе ПЭВМ (PC), в котором установлен комплекс СЗИ НСД, должны отсутствовать средства, позволяющие за счет воздействия со стороны пользователей на штатные органы управления ПЭВМ (PC) 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(PC), эксплуатацию и контроль правильности использования СВТ(PC) 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

Перед установкой и эксплуатацией комплекса СЗИ НСД «Аккорд-АМДЗ» Администратор БИ составляет организационно-распорядительный документ о вводе комплекса в эксплуатацию и вносит сведения о нем в раздел Формуляра «Сведения о вводе в эксплуатацию и закреплении 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 – см. «Руководство по установке» (11443195.4012.006 98 / 11443195.4012.038 98 / 11443195.4012.054 98 / 37222406.26.20.40.140.079 98);

2)Установку пароля на вход в BIOS;

3)Установку параметров учетной записи «Гл. Администратор» и настройку комплекса в соответствии с конфигурацией технических средств ПЭВМ (подробнее см. «Руководство по установке» и подраздел 3.2 настоящего Руководства);

4)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 среды администрирования (рисунок 1, рисунок 2).

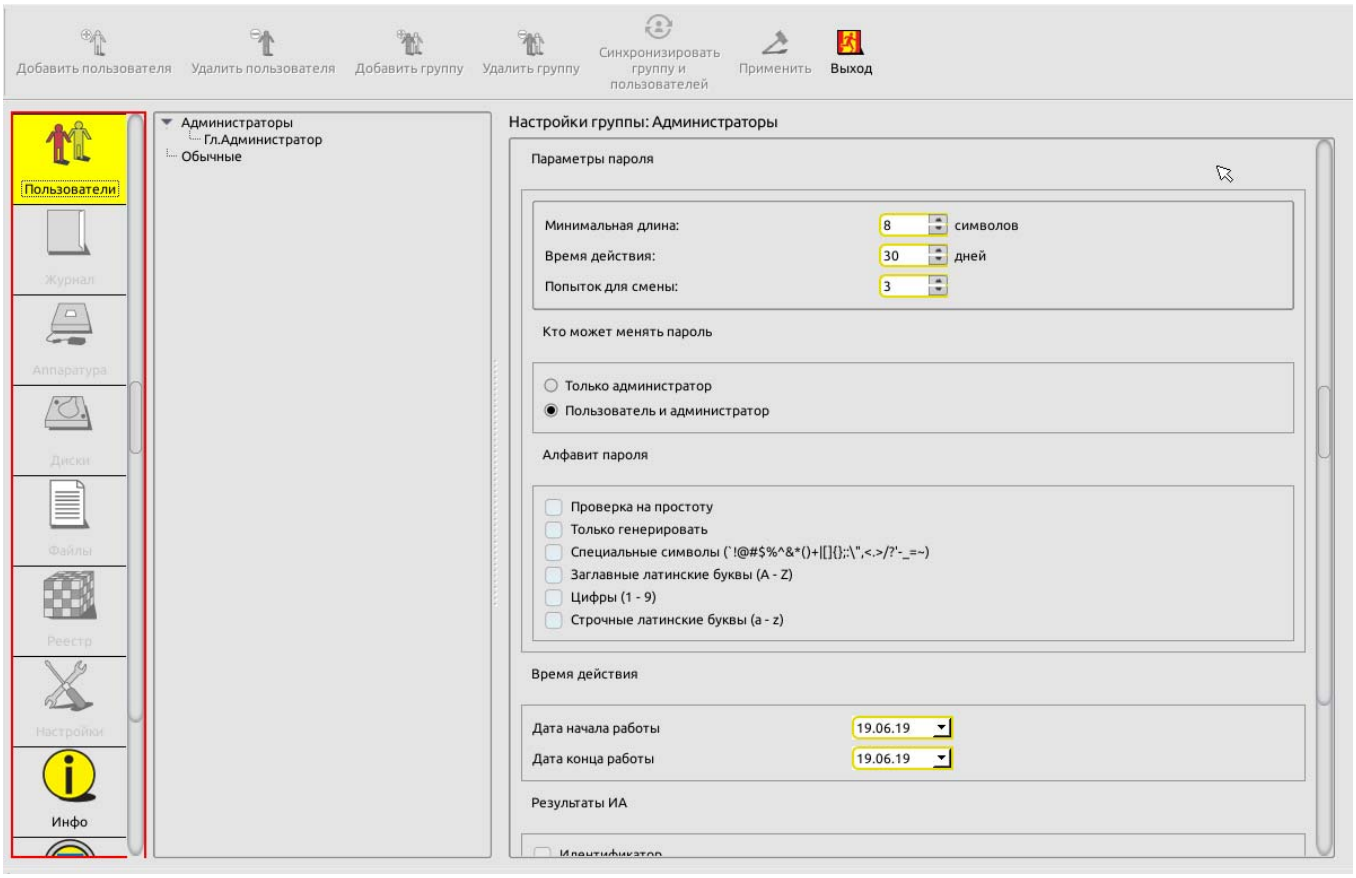

Рисунок 1 - Главное окно среды администрирования (для моделей Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019)

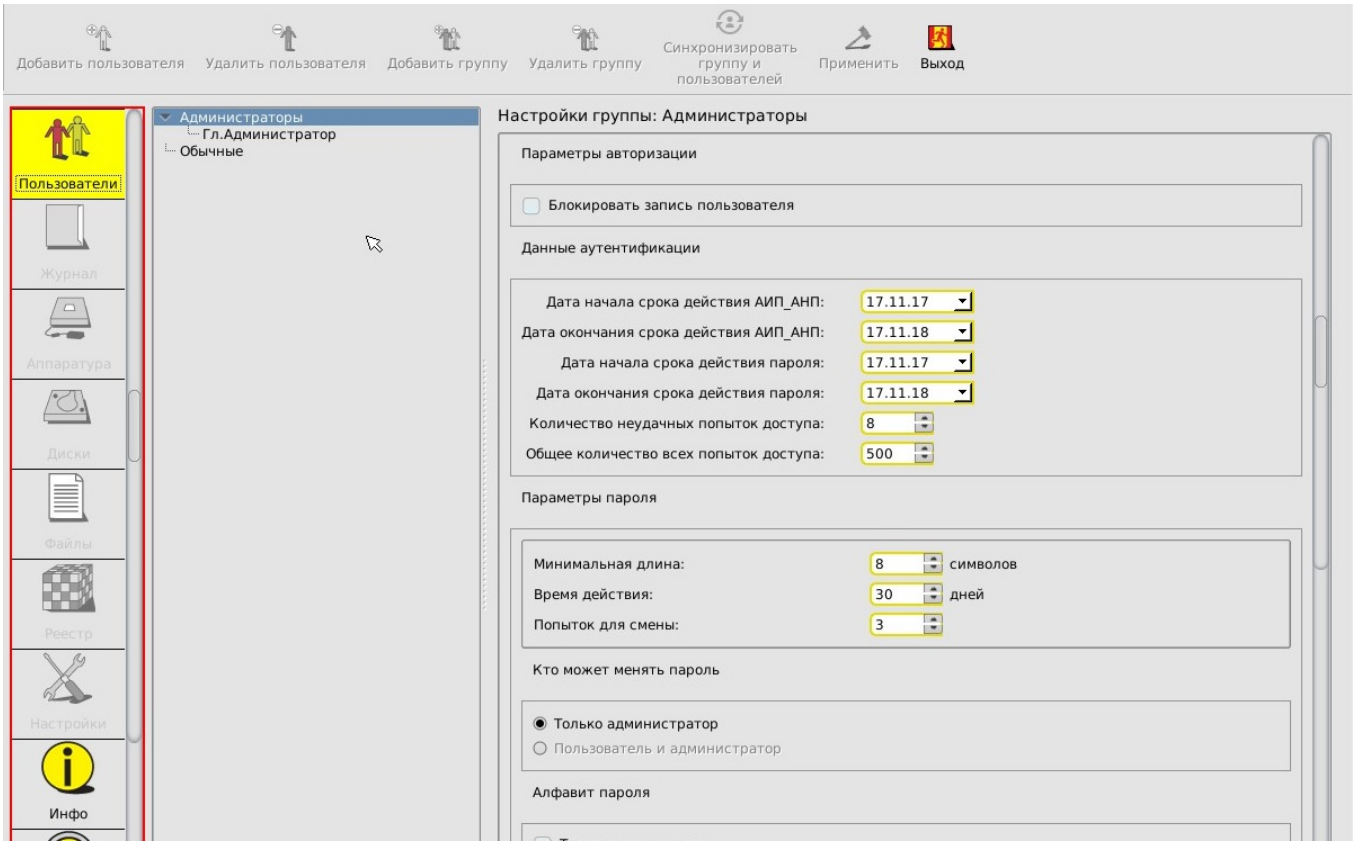

Рисунок 2 - Главное окно среды администрирования (для моделей Аккорд-АМДЗ» ТУ 4012-054-11443195-2013)

Главное окно среды администрирования 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 (для ОС семейства Windows);
- <Настройки> - общие настройки комплекса;
- <Инфо> - информация о версии прошивки контроллера и контрольные суммы ядра защиты;
- <База данных> – выполнение процедур экспорта/импорта элементов базы данных;

- <Регламенты> – запуск процессов самотестирования комплекса.

В начале первого сеанса работы помимо главного окна среды администрирования на экран также выводится сообщение с требованием выполнить процедуру настройки параметров учетной записи «Гл.Администратор» (рисунок 3), без выполнения которой недоступны никакие функции «Аккорд-АМДЗ».

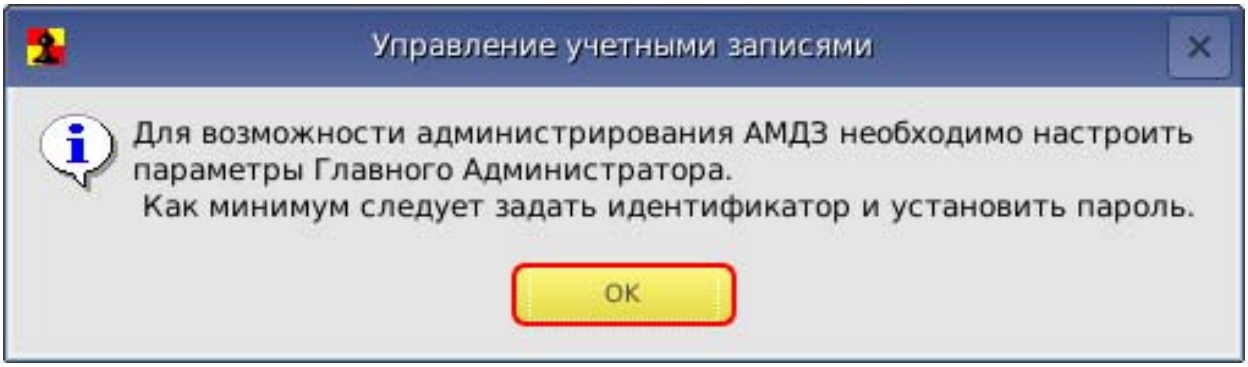

Рисунок 3 - Сообщение с требованием настроить параметры учетной записи «Гл. Администратор»

После выполнения процедуры установки параметров учетной записи «Гл. Администратор», описанной в подразделе 3.2 настоящего Руководства, функционал «Аккорд-АМДЗ» становится доступным для пользователя «Гл. Администратор».

Далее 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 «Гл.Администратор»

3.2.1. Общие сведения

При инициализации контроллера в базе данных создается учетная запись «Гл. Администратор»[1] – пользователя, имеющего особый статус и абсолютные полномочия в среде – которому будут полностью доступны все функции администрирования «Аккорд-АМДЗ».

При этом для данного пользователя не установлены параметры учетной записи.

[1)] В ПО «Аккорд-АМДЗ» имена учетных записей, созданных по умолчанию, отображаются на русском языке. Необходимо помнить, что для имени «Гл.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).

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

Для установки параметров учетной записи нужно в списке пользователей отметить мышью пользователя «Гл.Администратор» (рисунок 1).

В появившемся рабочем поле редактирования параметров учетной записи «Гл. Администратор» предварительно можно выполнить настройки следующих параметров:

- параметры пароля (см. подраздел 3.3.2.4);
- атрибуты доступа (см. подраздел 3.3.4.7);
- результаты ИА (см. подраздел 3.3.2.6).

Настройка данных параметров не является обязательной и может быть выполнена в любой момент после завершения процедуры настройки обязательных параметров учетной записи.

После выполнения указанных настроек следует перейти к настройке обязательных для учетной записи параметров:

- данные аутентификации (только для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013 – подраздел 3.2.2);
- персональный идентификатор (подраздел 3.2.3);
- пароль (подраздел 3.2.4).

Для моделей «Аккорд-АМДЗ», ТУ 4012-054-11443195-2013, назначение персонального идентификатора и установка пароля выполняются в рамках одной операции.

3.2.2. Настройка данных аутентификации

ВНИМАНИЕ! Данный пункт распространяется только на модели «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013.

Перед выполнением процедуры назначения идентификатора и установки пароля необходимо выполнить процедуру настройки данных аутентификации.

Для этого в группе элементов «Данные аутентификации» окна настройки параметров учетной записи «Гл. Администратор» следует настроить следующие параметры (рисунок 2):

- «Дата начала срока действия АИП_АНП» – дата начала срока действия аутентифицирующей информации, хранящейся на аутентифицирующем носителе пользователя;
- «Дата окончания срока действия АИП_АНП» – дата окончания срока действия аутентифицирующей информации, хранящейся на аутентифицирующем носителе пользователя;
- «Дата начала срока действия пароля» – дата начала срока действия пароля пользователя;

- «Дата окончания срока действия пароля» – дата окончания срока действия пароля пользователя;
- «Количество неудачных попыток доступа» – количество неудачных подряд идущих попыток доступа пользователя, по превышении которого работа пользователя блокируется;
- «Общее количество всех попыток доступа» – общее количество всех попыток доступа пользователя, по превышении которого работа пользователя блокируется.

Примечание: *Данные аутентификации, установленные для аутентифицирующего носителя пользователя в процессе первичной регистрации, будут также учитываться при работе данного пользователя на всех рабочих станциях, на которых он впоследствии будет зарегистрирован с применением одного и того же аутентифицирующего носителя – до тех пор, пока процедура настройки данных аутентификации для данного аутентифицирующего носителя не будет выполнена заново.*

ВНИМАНИЕ! При приближении максимальной границы по любому из параметров потребуется выполнить генерацию данных аутентификации заново. В результате идентификатор будет действителен только на том контроллере «Аккорд-АМДЗ», на котором выполнена генерация.

Для предупреждения возможных трудностей в работе «Аккорд-АМДЗ», связанных с указанными выше условиями, рекомендуется для каждого контроллера «Аккорд-АМДЗ» регистрировать минимум двух администраторов, так, чтобы окончание срока действия АИП_АНП у одного из них всегда наступало позже, оставляя возможность входа в среду администрирования «Аккорд-АМДЗ» с целью обновления истекшей АИП_АНП второго администратора.

Далее следует перейти к выполнению процедур назначения персонального идентификатора и пароля.

3.2.3. Назначение персонального идентификатора

ВНИМАНИЕ! Следует помнить, что если на компьютере с установленным «Аккорд-АМДЗ» используются ключевые носители из числа поддерживаемых «Аккорд-АМДЗ» (подробнее см. «Руководство по установке»), их необходимо отключить до появления запроса идентификатора. Далее следует предъявить идентификатор и ввести пароль в «Аккорд-АМДЗ», а затем подключить ключевой носитель заново.

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 перестанет действовать на тех ПЭВМ, где был зарегистрирован ранее.

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 4).

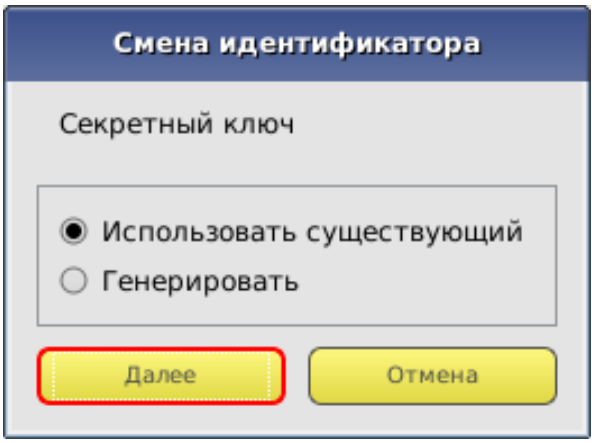

Рисунок 4 – Окно выбора секретного ключа

На экране появится окно с запросом идентификатора для смены (рисунок 5).

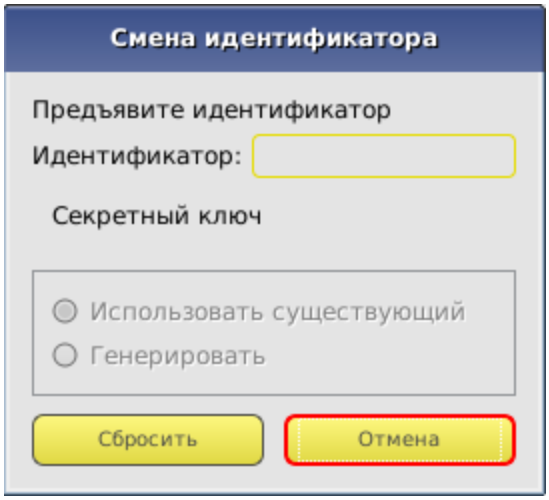

Рисунок 5 – Окно с запросом идентификатора для смены

Если идентификатор еще не предъявлен, поле «Идентификатор» пустое. Необходимо предъявить идентификатор и дождаться момента, пока в поле не появится серийный номер идентификатора (рисунок 6).

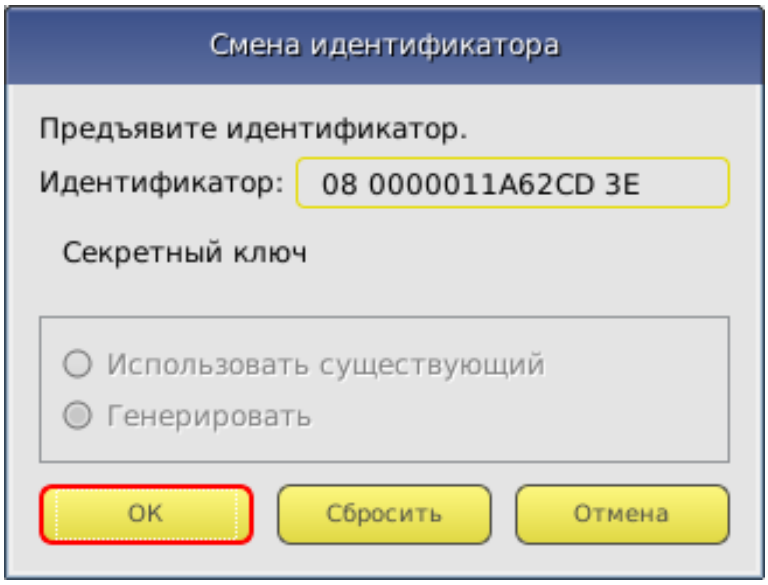

Рисунок 6 – Окно смены идентификатора

Необходимо подтвердить завершение операции нажатием кнопки <ОК>.

ВНИМАНИЕ! Для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013 сразу по завершении процедуры назначения персонального идентификатора автоматически начинается выполнение процедуры назначения пароля (см. 3.2.4).

После корректного выполнения описанной последовательности действий номер идентификатора появляется в поле «Идентификатор» главного окна среды администрирования (для моделей Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019 – рисунок 7).

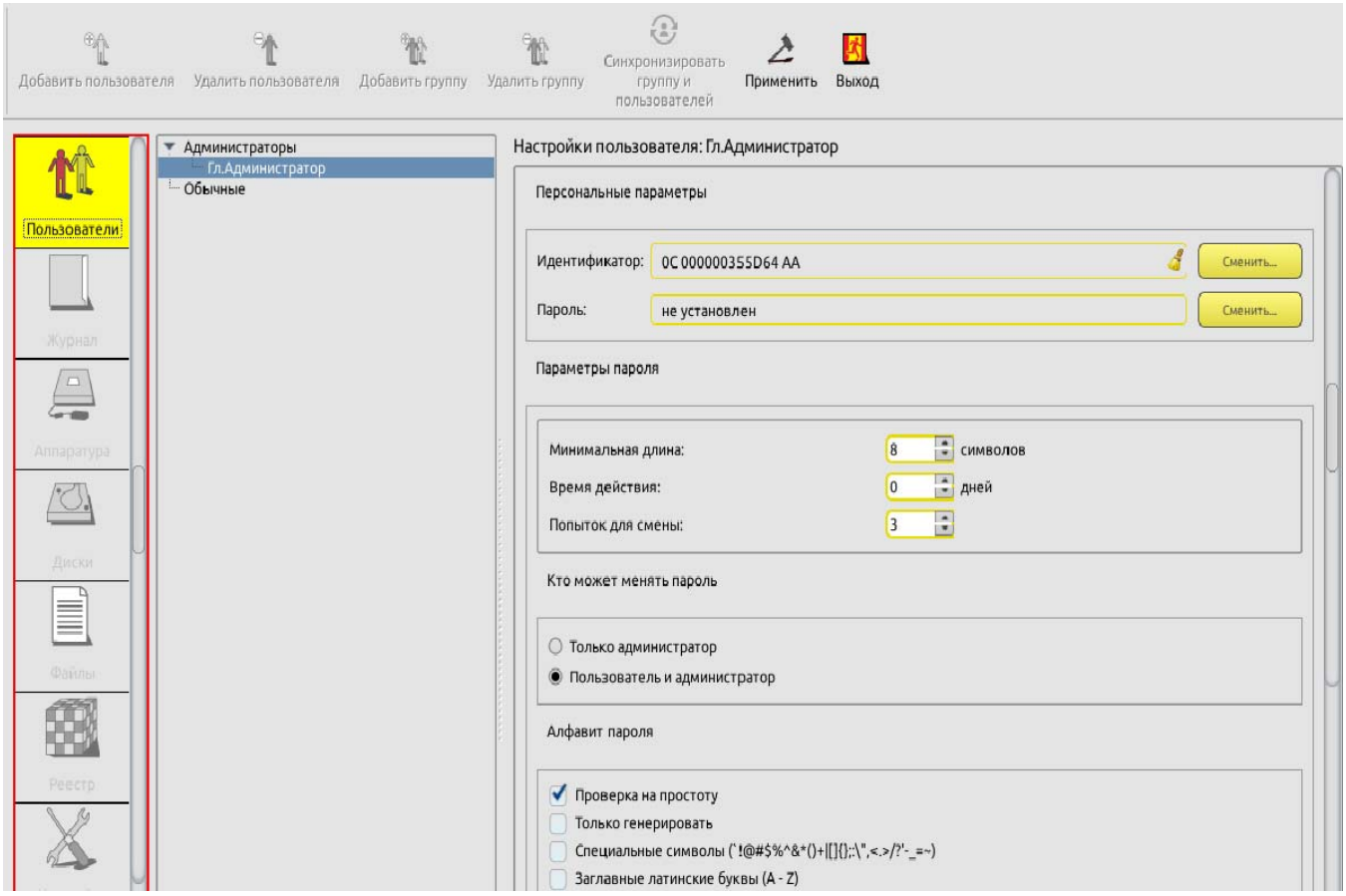

Рисунок 7 - Идентификатор учетной записи «Гл. Администратор» установлен (для моделей Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019)

Далее необходимо перейти к процедуре назначения пароля (см. 3.2.4).

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

В противном случае при нажатии кнопки <Применить> в главном окне среды администрирования на экран выводится предупреждение о том, что идентификатор (и)или пароль пользователя не установлены (рисунок 8), и программа ожидает от администратора завершения процедуры настройки параметров авторизации пользователя.

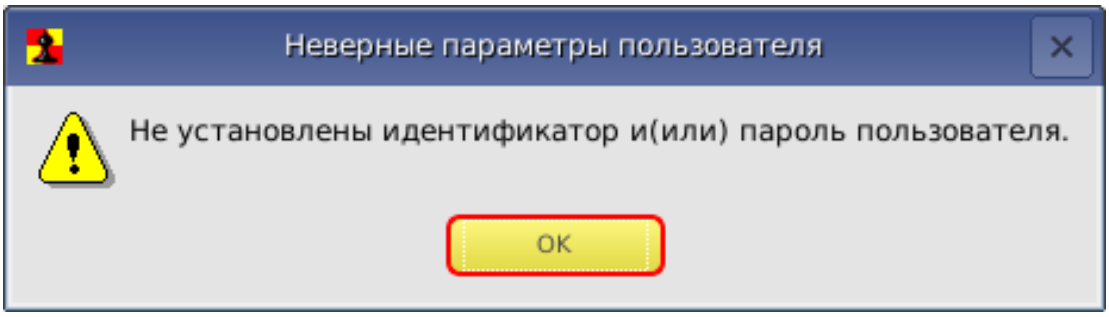

Рисунок 8 - Сообщение о том, что идентификатор или пароль пользователя не установлены

В некоторых случаях при регистрации идентификатора следует учитывать ряд нюансов. Опишем на примере устройства ruToken-S.

До начала регистрации устройство должно быть инициализировано.

Если ruToken-S получен в составе комплекта поставки «Аккорд-АМДЗ» напрямую от ОКБ САПР, то он инициализирован и имеет ПИН-код по умолчанию 12345678.

В противном случае устройство необходимо проинициализировать в соответствии с инструкцией производителя.

Далее при регистрации идентификатора потребуется ввод вышеупомянутого ПИН-кода (рисунок 9).

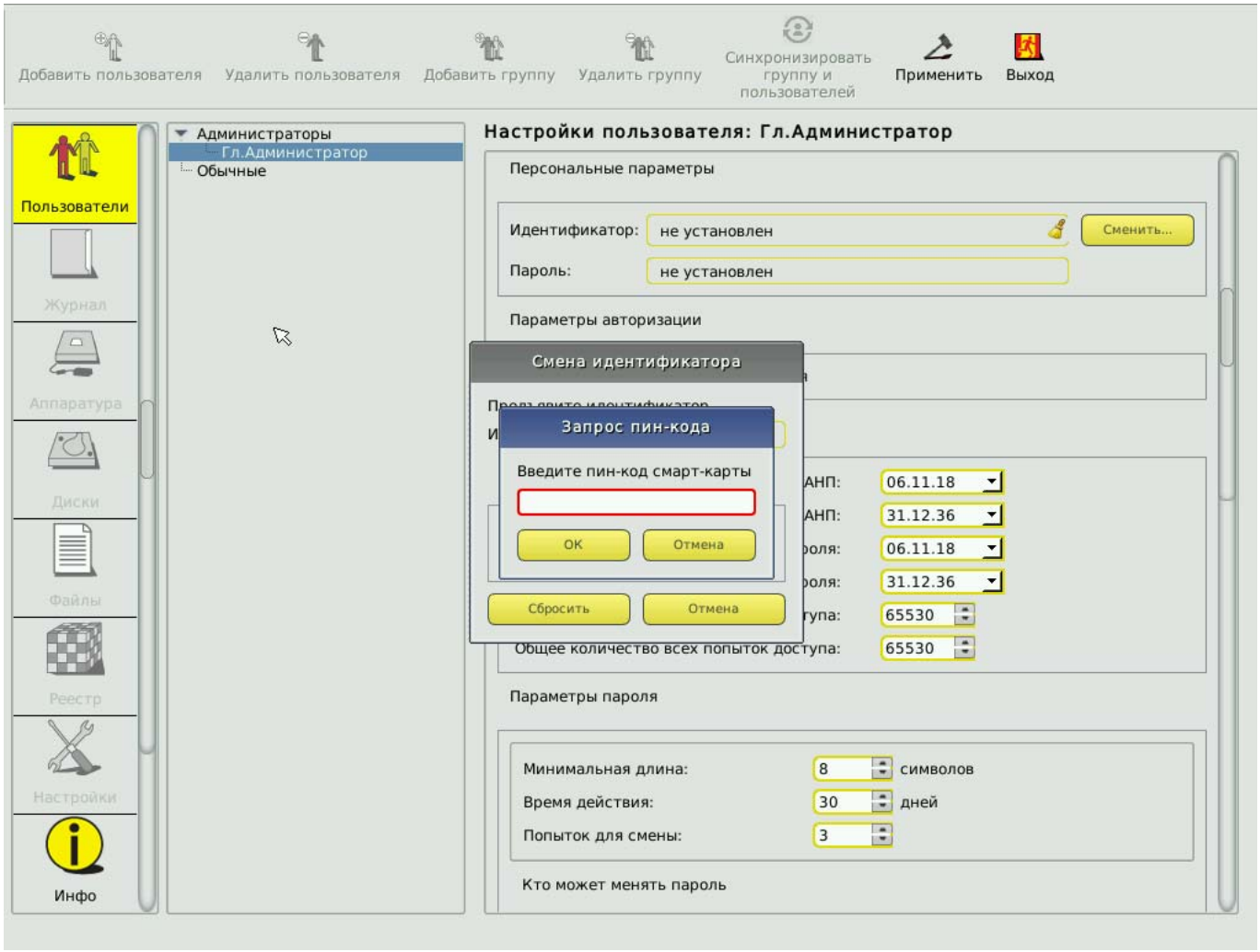

Рисунок 9 – Запрос ПИН-кода при регистрации идентификатора

Если ПИН-код введен неверно, запись идентификатора не производится, а на экран выводится сообщение об этом.

Следует помнить, что устройства подобного типа, являясь по существу смарт-картой, предполагают необходимость ввода ПИН-кода пользователя при регистрации и в дальнейшем при каждой аутентификации, и этот ПИН-код - не пароль пользователя в «Аккорд-АМДЗ», а дополнительный код, который пользователь (в том числе Администратор) будет вводить каждый раз помимо пароля.

Если это представляется избыточным, во вкладке «Настройки» можно установить флаг «Автоматический ввод ПИН-кода» и ввести ПИН-код по умолчанию (рисунок 10).

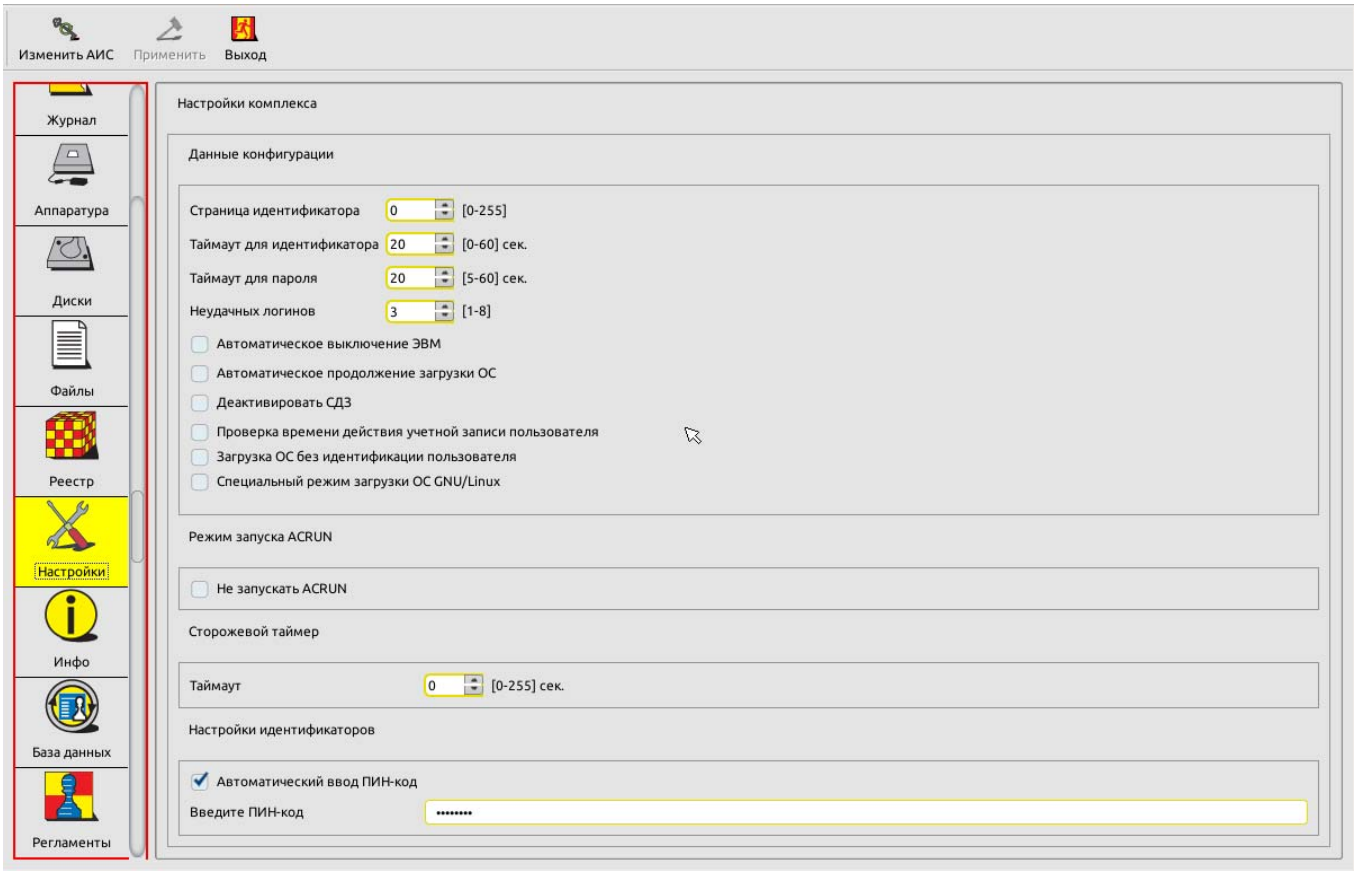

Рисунок 10 – Установка автоматического ввода ПИН-кода

Этот способ можно использовать только в том случае, если у всех устройств (в данном примере ruToken-S) установлен один и тот же ПИН-код или используется ПИН-код по умолчанию.

3.2.4. Назначение пароля

Перед выполнением процедуры назначения пароля на правой панели главного окна среды администрирования (рисунок 1) нужно установить необходимые параметры пароля (подробнее см. 3.3.2.4).

Выполнение процедуры назначения пароля:

- для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013 начинается автоматически после назначения персонального идентификатора;
- для моделей Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019 начинается посредством нажатия кнопки <Сменить> в строке «Пароль» главного окна среды администрирования (рисунок 7).

На экран выводится окно ввода пароля (рисунок 11). 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 (в зависимости от установленных администратором параметров пароля – см. 3.3.2.4). 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.

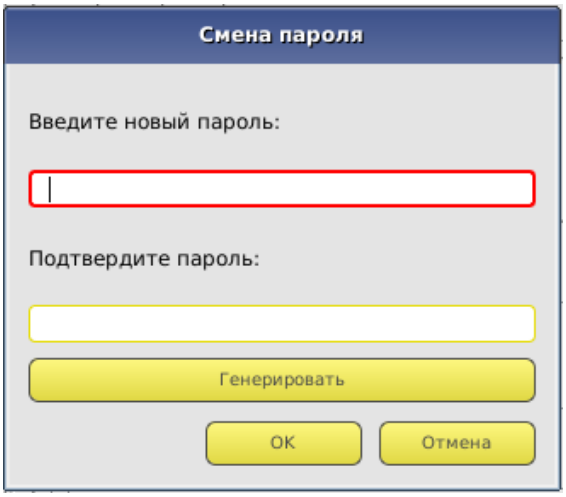

Рисунок 11 – Окно ввода пароля

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 8).

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 среды администрирования значение параметра в поле «Пароль» меняется на «Установлен» (рисунок 12).

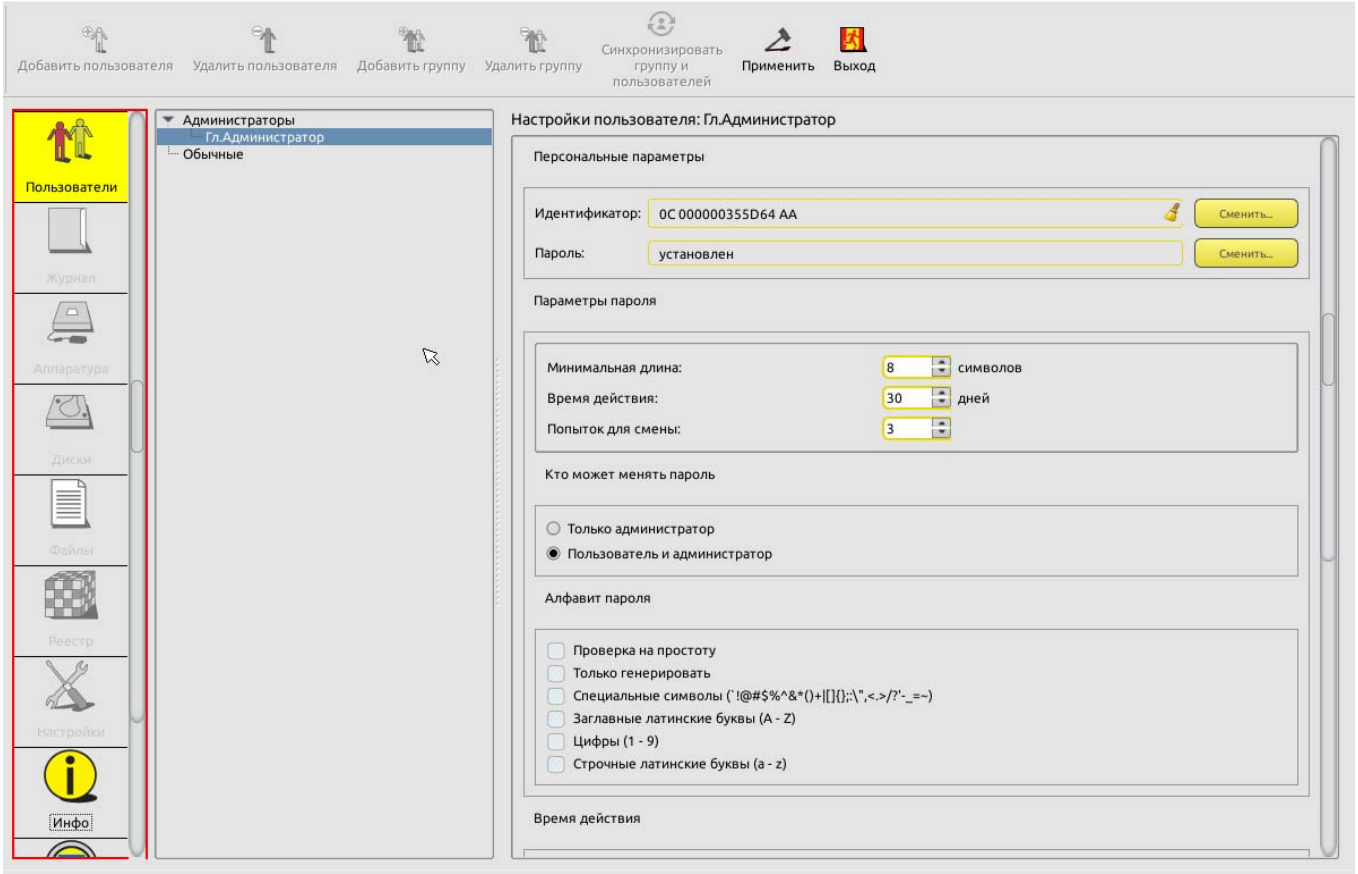

Рисунок 12 - Пароль учетной записи «Гл. Администратор» установлен (для моделей Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019)

Для сохранения параметров пользователя «Гл.Администратор» нужно нажать кнопку <Применить> на панели инструментов вверху главного окна (рисунок 12).

После корректного выполнения описанной последовательности действий на экран выводится сообщение о сохранении внесенных изменений (рисунок 13).

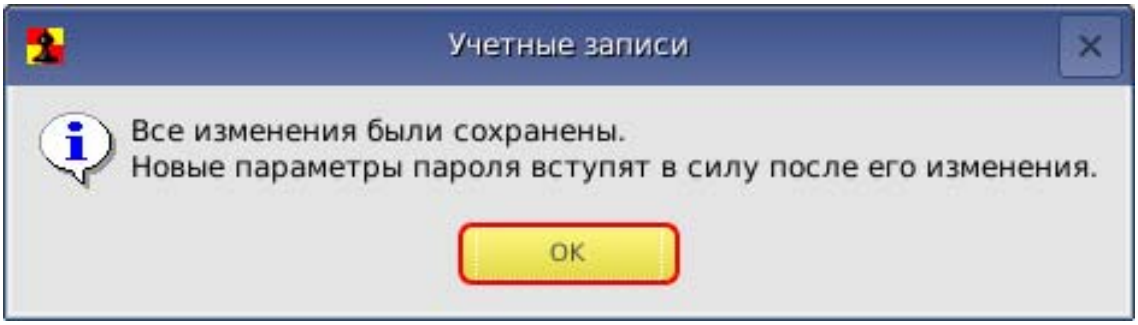

Рисунок 13 - Сообщение о сохранении внесенных изменений

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

ВНИМАНИЕ! В случае работы с комплексом «Аккорд-АМДЗ», функционирующим **на базе контроллеров Аккорд-5.5(е)**, после выполнения описанной в настоящем пункте процедуры установки параметров учетной записи «Гл.Администратор» необходимо выполнить выход из среды администрирования и перезагрузить компьютер.

Дальнейшие настройки комплекса можно выполнять только после перезагрузки компьютера!

3.3. Настройка параметров групп и учетных записей пользователей

3.3.1. Список пользователей

При инициализации контроллера создаются две зарезервированные группы пользователей – «Администраторы» («ADMINS») и «Обычные» («EVERYONE»)[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 среды администрирования выбрать из списка нужную группу пользователей, мышью установив курсор на строке заголовка группы (рисунок 1).

3.3.2. Общие параметры группы «Администраторы»

3.3.2.1. Общие сведения

Для группы «Администраторы» установлены следующие общие параметры (рисунок 14, рисунок 15):

- параметры авторизации (см. 3.3.2.2);
- данные аутентификации (для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013 – см. 3.3.2.3);
- параметры пароля (см. 3.3.2.4);

[1)] В ПО «Аккорд-АМДЗ» имена учетных записей, созданных по умолчанию, отображаются на русском языке. Необходимо помнить, что для имени «Гл. 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).

- время действия (см. 3.3.2.5);
- результаты ИА (идентификации/аутентификации пользователя) (см. 3.3.2.6).

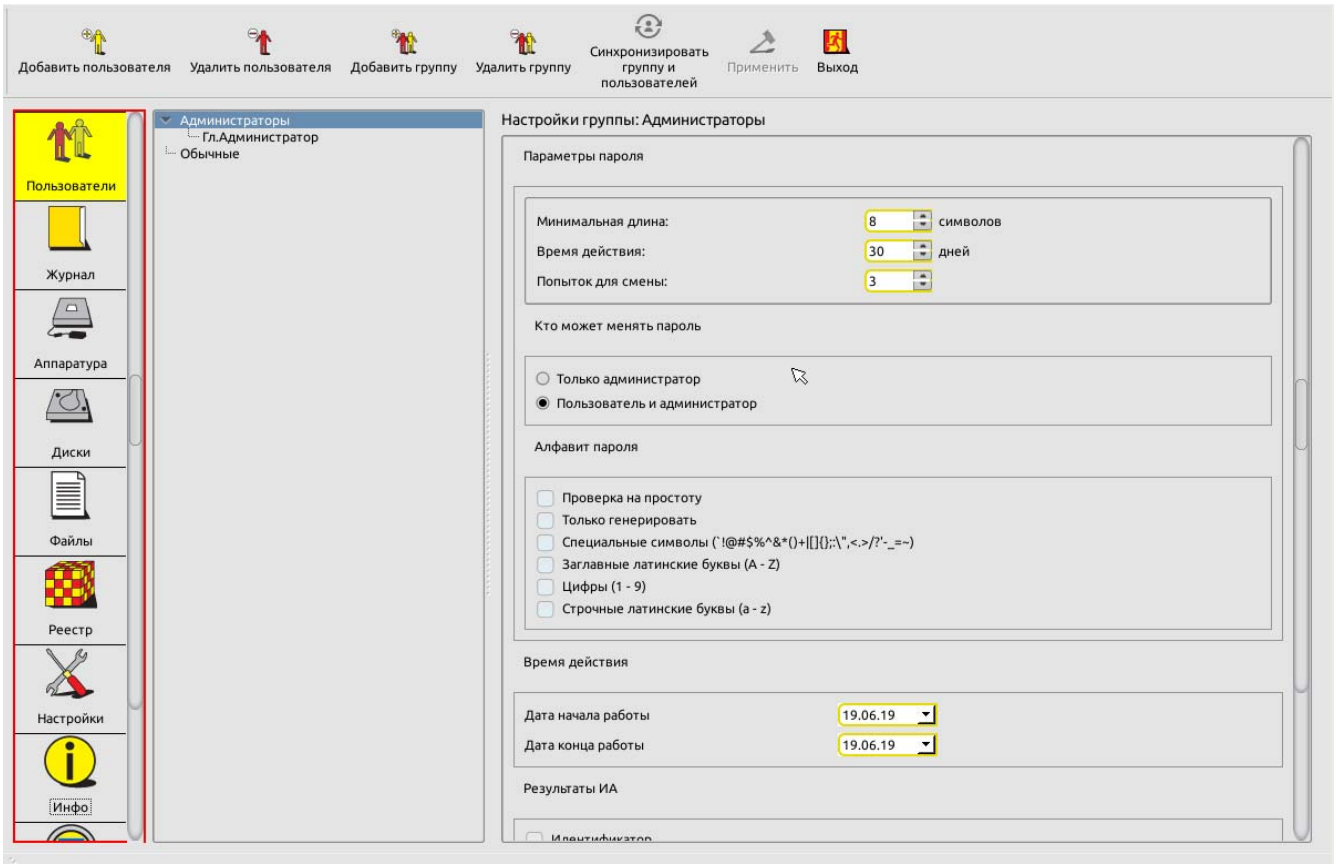

Рисунок 14 - Общие параметры группы «Администраторы» (для моделей Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019)

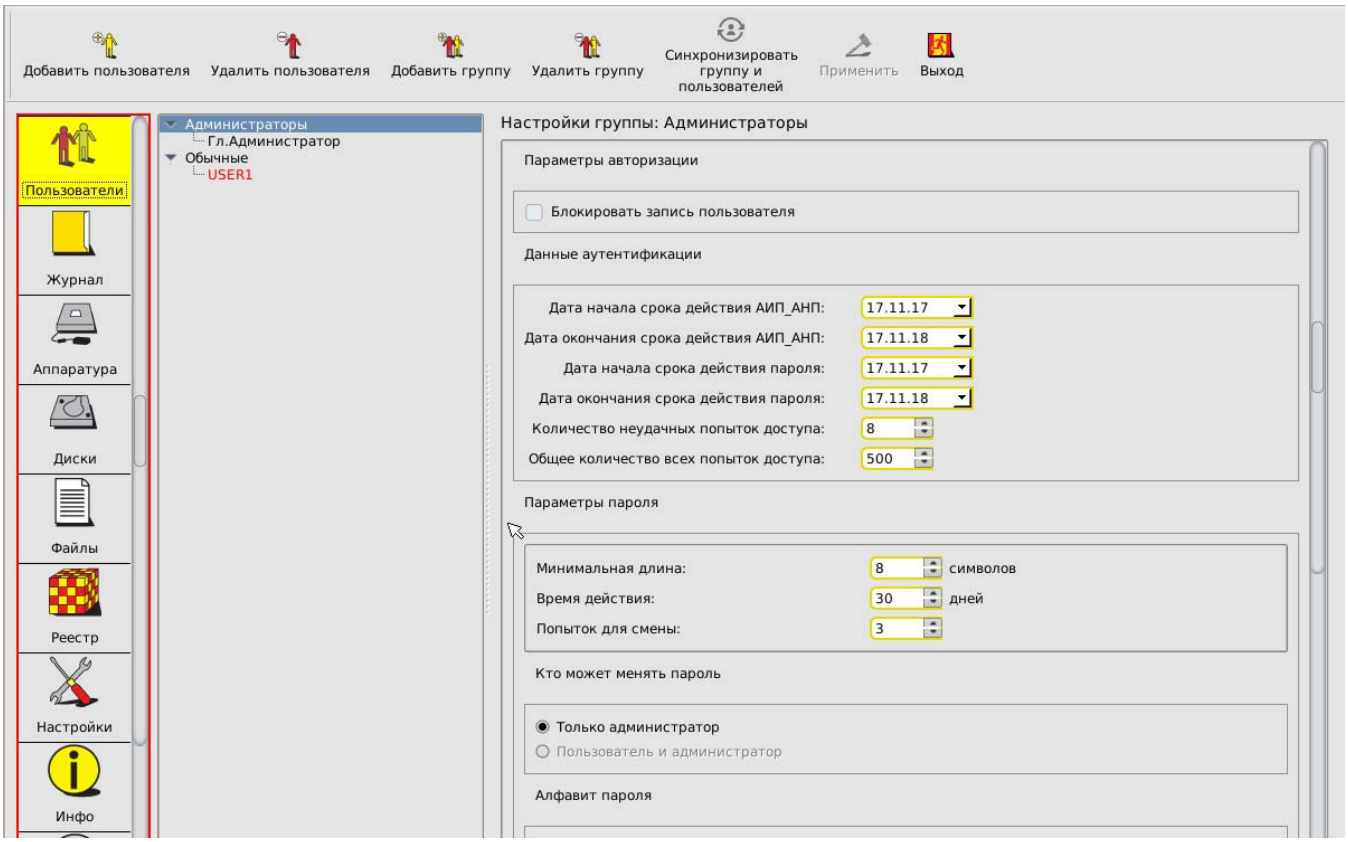

Рисунок 15 - Общие параметры группы «Администраторы» (для моделей Аккорд-АМДЗ» ТУ 4012-054-11443195-2013)

3.3.2.2. Параметры авторизации

Для группы «Администраторы» установлены следующие параметры авторизации:

- режим блокировки.

При установке флага «Блокировать запись пользователя» в состояние «Да» все параметры пользователей, входящих в группу «Администраторы», сохраняются в базе данных, но вход в систему и работа данных пользователей будут запрещены. Данный флаг можно использовать для временной блокировки группы пользователей. После того как обладающий соответствующими привилегиями администратор снимет блокировку, работа пользователей возобновится со всеми установленными настройками. Изменить состояние данного флага можно щелчком мыши.

3.3.2.3. Данные аутентификации

ВНИМАНИЕ! Данный пункт распространяется только на модели «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013.

Для группы «Администраторы» имеется возможность задать данные аутентификации. Процедура настройки данных аутентификации для группы «Администраторы» (выполняется только для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013) аналогична процедуре настройки данных аутентификации для учетной записи «Гл. Администратор» (подробнее см. 3.2.2).

3.3.2.4. Параметры пароля

Для управления парольной политикой можно регулировать следующие параметры пароля на правой вертикальной панели (рисунок 14):

- «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 необязательно). 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 (по истечении 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. Флаг «Проверка на простоту» запускает проверку пароля на соответствие следующим критериям:

  - недопустимость использования более трех одинаковых символов подряд;

  - недопустимость использования более трех подряд символов, расположенных рядом на клавиатуре (как в прямом, так и в обратном порядке);

- недопустимость использования более трех подряд символов, расположенных рядом в таблице ASCII (как в прямом, так и в обратном порядке);
- недопустимость использования в пароле старого пароля или его части, а также идентификатора или его части.

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

3.3.2.5. Время действия

В разделе «Время действия» можно настроить следующие параметры:

- «Дата начала работы» – определяет дату, с наступлением которой работа для пользователей, входящих в группу «Администраторы», разрешается на текущем компьютере;
- «Дата конца работы» – определяет дату, с наступлением которой работа для пользователей, входящих в группу «Администраторы», запрещается на текущем компьютере.

Параметры «Время действия» учитываются в процессе работы комплекса только в том случае, если в разделе «Данные конфигурации» на вкладке «Настройки» (см. п. 3.12.1) администратором установлена галочка «Проверка времени действия учетной записи пользователя».

3.3.2.6. 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) с целью синхронизации базы данных пользователей. Для передачи в программную подсистему разграничения доступа доступны следующие параметры:

- идентификатор;
- секретный ключ станции;
- секретный ключ пользователя;
- имя пользователя;
- пароль;
- флаги ОС;
- номер пользователя;
- уровень доступа пользователя.

Некоторые из этих параметров необходимы для успешного выполнения в программной подсистеме разграничения доступа процедуры «Автоматический логин в ОС», когда пользователь авторизуется на аппаратном уровне, а программная часть автоматически подгружает его профиль доступа.

При этом вход в систему может осуществляться двумя способами:

- контроллер комплекса «Аккорд-АМДЗ» передает подсистеме доступа **имя пользователя**. В этом случае при логине в ОС требуется ввести с клавиатуры пароль пользователя, имя пользователя изменить нельзя. Для настройки работы в таком режиме следует в разделе «Результаты ИА» параметров пользователя установить **первые четыре флага**.
- контроллер комплекса «Аккорд-АМДЗ» передает подсистеме доступа **имя и пароль пользователя**. В этом случае при логине в ОС ввода пароля не требуется. Для настройки работы в таком режиме следует в разделе «Результаты ИА» параметров пользователя установить **первые пять флагов**.

Установки по умолчанию, при которых не включен ни один флаг, предполагают использование только контроллера «Аккорд-АМДЗ» (без подсистемы разграничения доступа).

3.3.3. Общие параметры группы «Обычные» (пользователи)

Для группы «Обычные» (пользователи) установлены следующие общие параметры (рисунок 16, рисунок 17):

- параметры авторизации (режим блокировки);
- данные аутентификации (для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013 см. 3.2.2).
- параметры пароля;
- результаты ИА (идентификации/аутентификации пользователя);

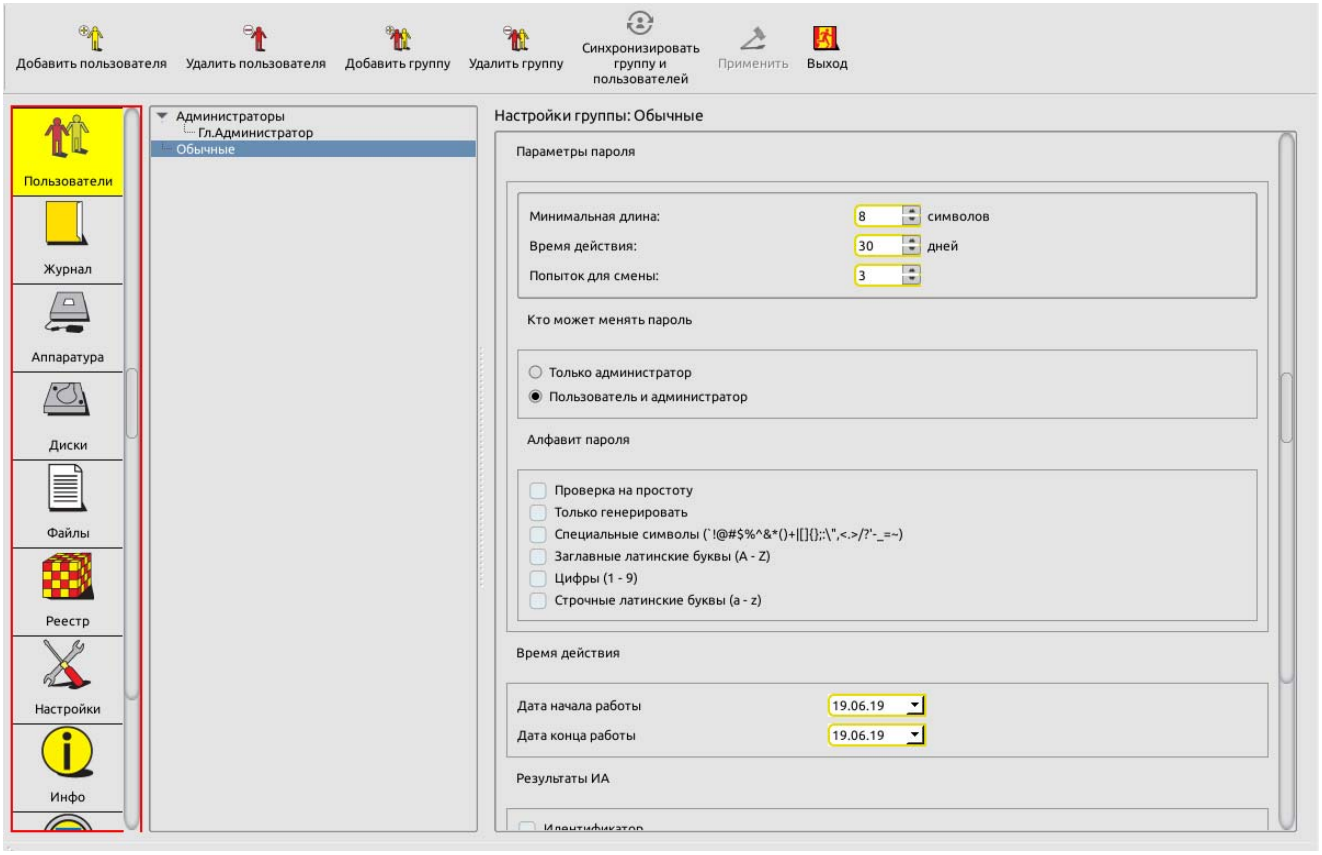

Рисунок 16 – Общие параметры группы «Обычные» (для моделей Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019)

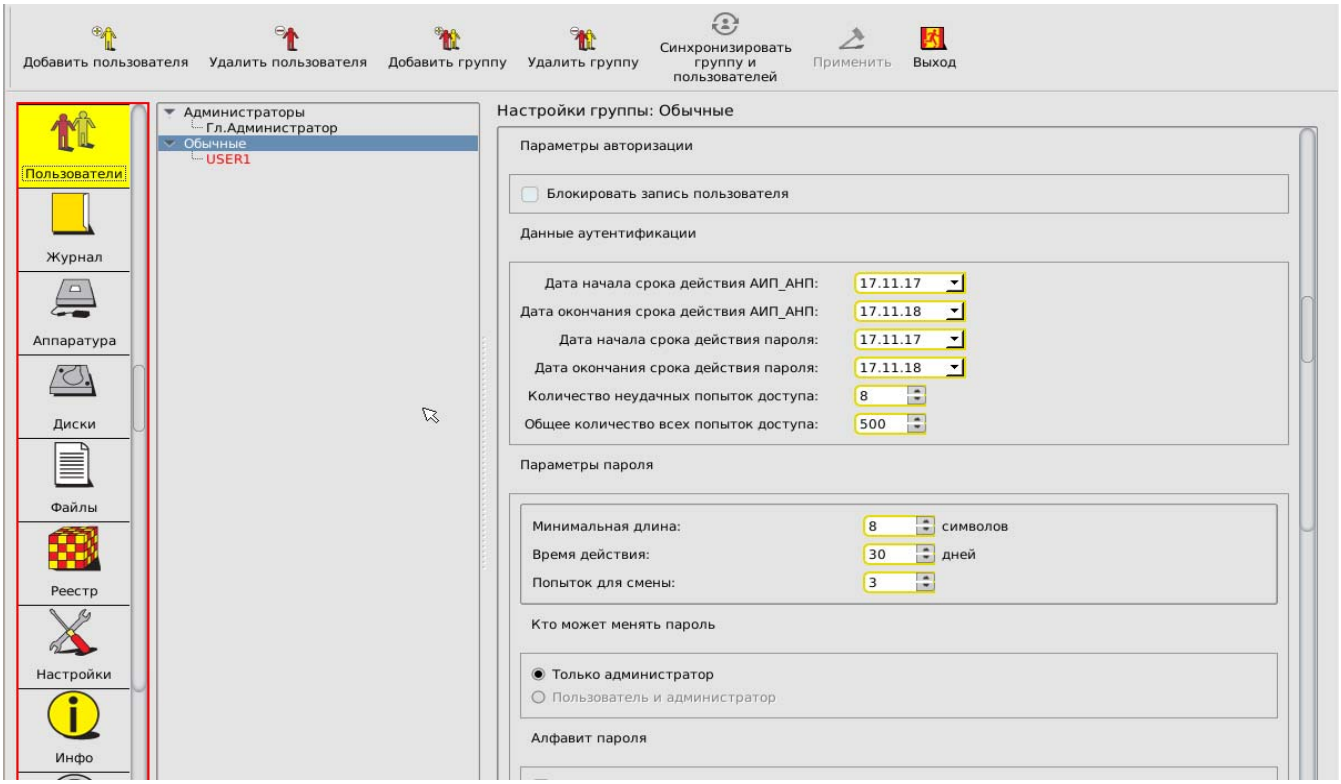

Рисунок 17 - Общие параметры группы «Обычные» (для моделей Аккорд-АМДЗ» ТУ 4012-054-11443195-2013)

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

ВНИМАНИЕ! При работе с «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013 установка параметра «Кто может менять пароль» для пользователей из группы «Обычные» недоступна, менять пароль для пользователя может только администратор.

3.3.4. Параметры пользователей в группе «Администраторы»

3.3.4.1. Общие сведения

Для пользователей группы «Администраторы» установлены следующие параметры (рисунок 18, рисунок 19):

- персональные параметры;
- параметры авторизации (режим блокировки);
- данные аутентификации (для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013 см. 3.2.2)
- параметры пароля;
- время действия;
- атрибуты доступа;
- результаты ИА (идентификации/аутентификации пользователя).

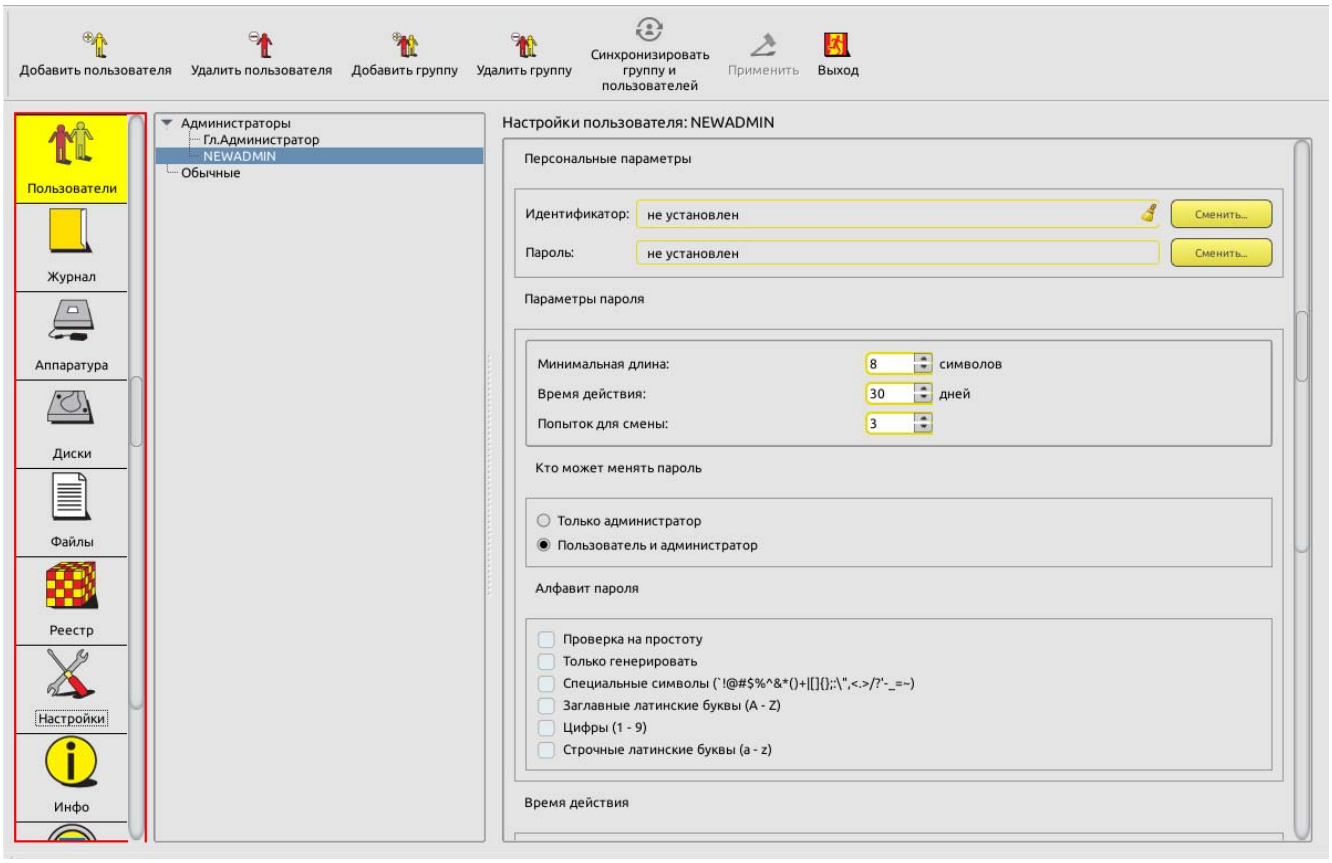

Рисунок 18 – Параметры пользователей в группе «Администраторы» (для моделей Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019)

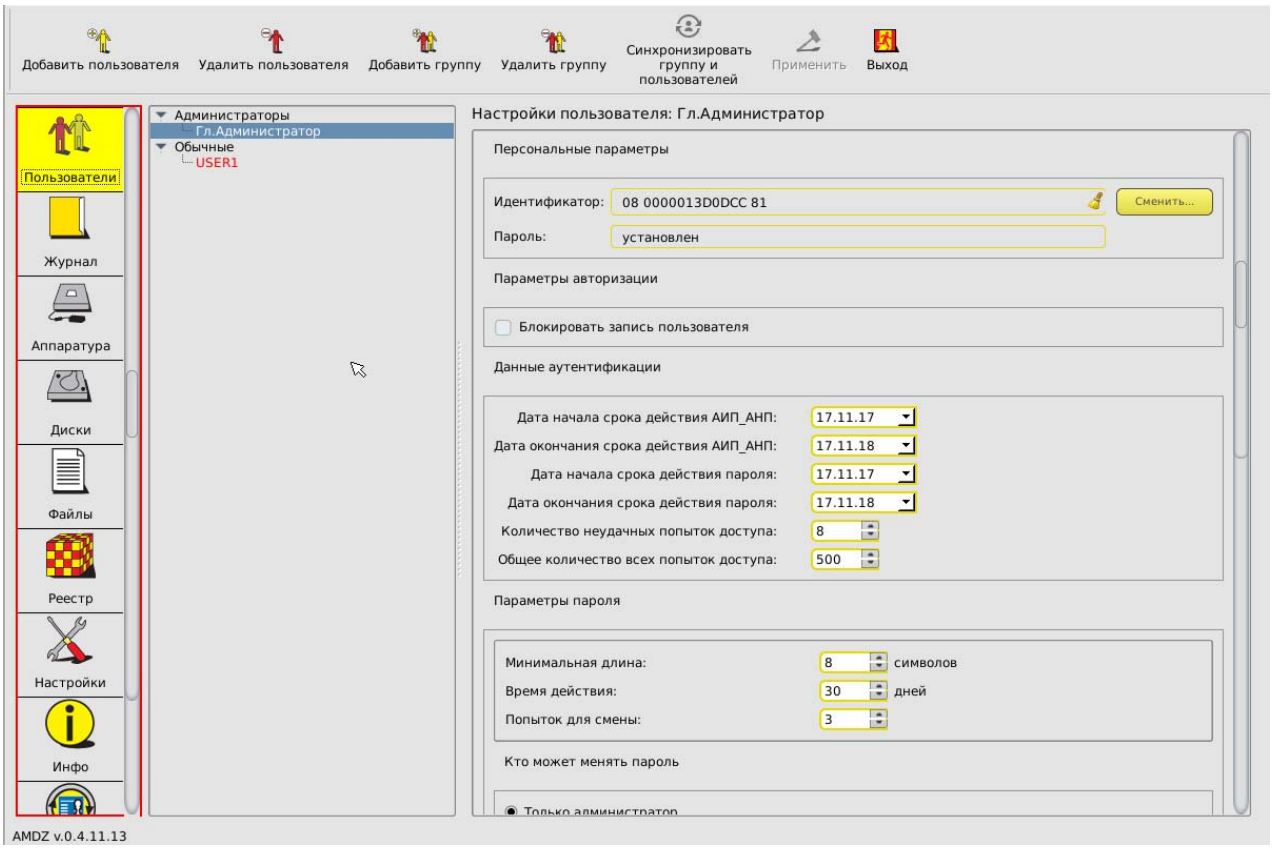

Рисунок 19 - Параметры пользователей в группе «Администраторы» (для моделей Аккорд-АМДЗ» ТУ 4012-054-11443195-2013)

3.3.4.2. 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 среды администрирования (см. рисунок 18).

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 3.2.3.

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 3.2.4.

3.3.4.3. Параметры авторизации

При установке флага «Блокировать запись пользователя» в состояние «Да» все параметры пользователя, входящего в группу «Администраторы», 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 обладающий соответствующими привилегиями администратор снимет блокировку, работа пользователя возобновится со всеми установленными настройками. Изменить состояние данного флага можно щелчком мыши.

3.3.4.4. Данные аутентификации

ВНИМАНИЕ! Данный пункт распространяется только на модели «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013.

Процедура настройки данных аутентификации для учетных записей пользователей из группы «Администраторы»:

- является обязательной (для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013) и может быть выполнена либо на этапе настройки общих параметров группы (см. 3.3.2.3), либо на этапе настройки каждой учетной записи (в рамках настоящего пункта Руководства);
- аналогична процедуре настройке данных аутентификации для учетной записи «Гл. Администратор» (см. 3.2.2).

3.3.4.5. Параметры пароля

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

3.3.4.6. Время действия

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

3.3.4.7. Атрибуты доступа

В разделе «Атрибуты доступа» устанавливаются персональные настройки функций редактирования и управления, которые будут доступны для данного пользователя из группы «Администраторы» (рисунок 20). Изменять настройки атрибутов доступа может 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»).

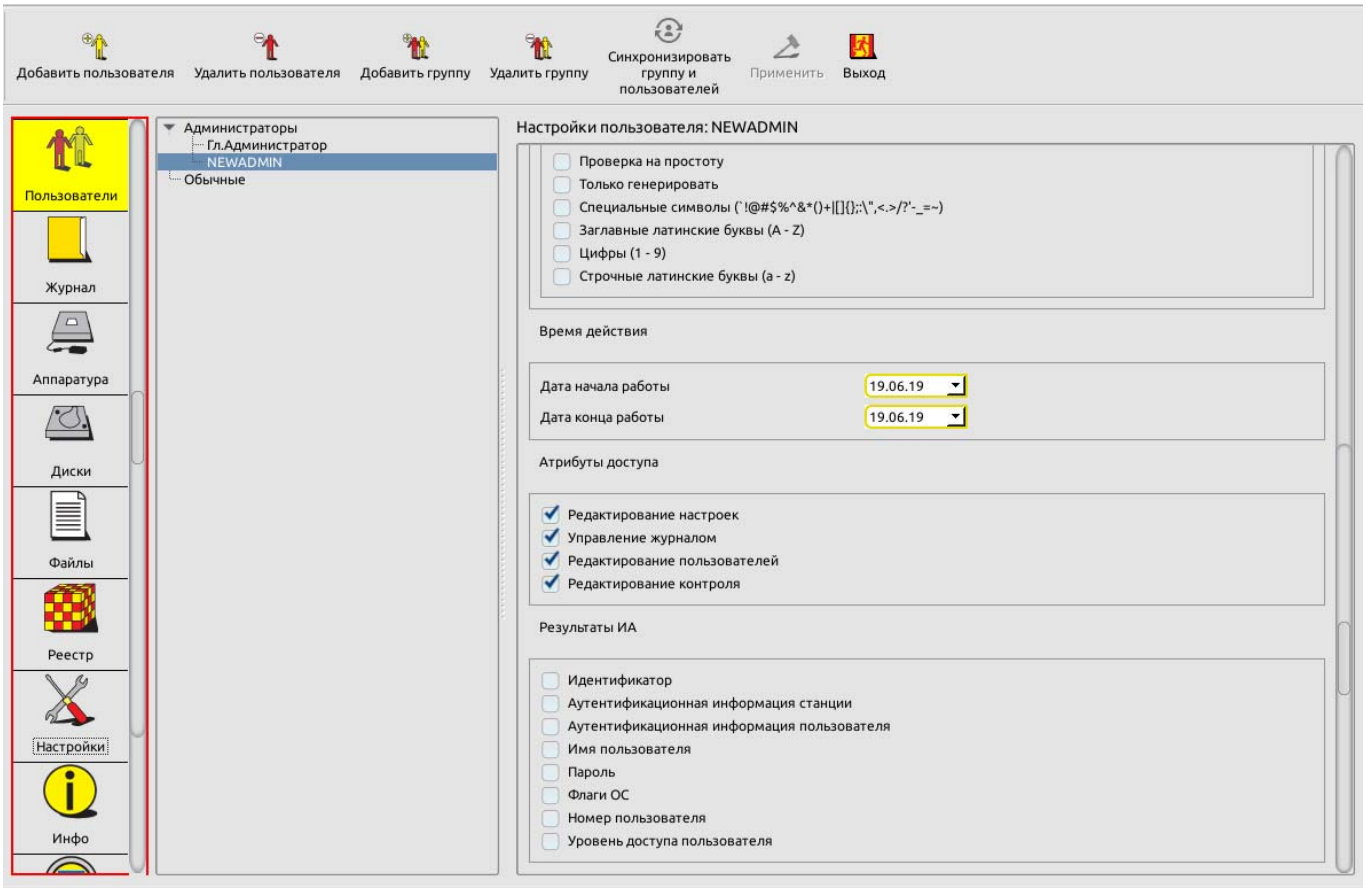

Рисунок 20 – Атрибуты доступа для пользователей из группы «Администраторы»

В данном разделе для выбранного пользователя из группы «Администраторы» администратор, обладающий правом редактирования пользователей, 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.
- 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 функция очищения журнала недоступна.
- 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, 3.7, 3.8). Снятие данного флага соответствует назначению пользователю роли аудитора системы.

- 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.

Снятие всех флагов для выбранного пользователя из группы «Администраторы» не лишает его возможности выполнять загрузку ОС со съемных носителей (например, для создания резервных копий дисков или восстановления ОС после сбоя (подробнее см. Приложение 18)) без привлечения супервизора; данный пользователь не будет иметь доступа к настройкам комплекса «Аккорд» за исключением возможности экспорта баз данных.

3.3.4.8. 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 21, рисунок 22):

- персональные параметры;
- параметры авторизации;
- данные аутентификации (для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013 см. 3.2.2)
- параметры пароля;
- время действия;
- результаты ИА (идентификации/аутентификации пользователя).

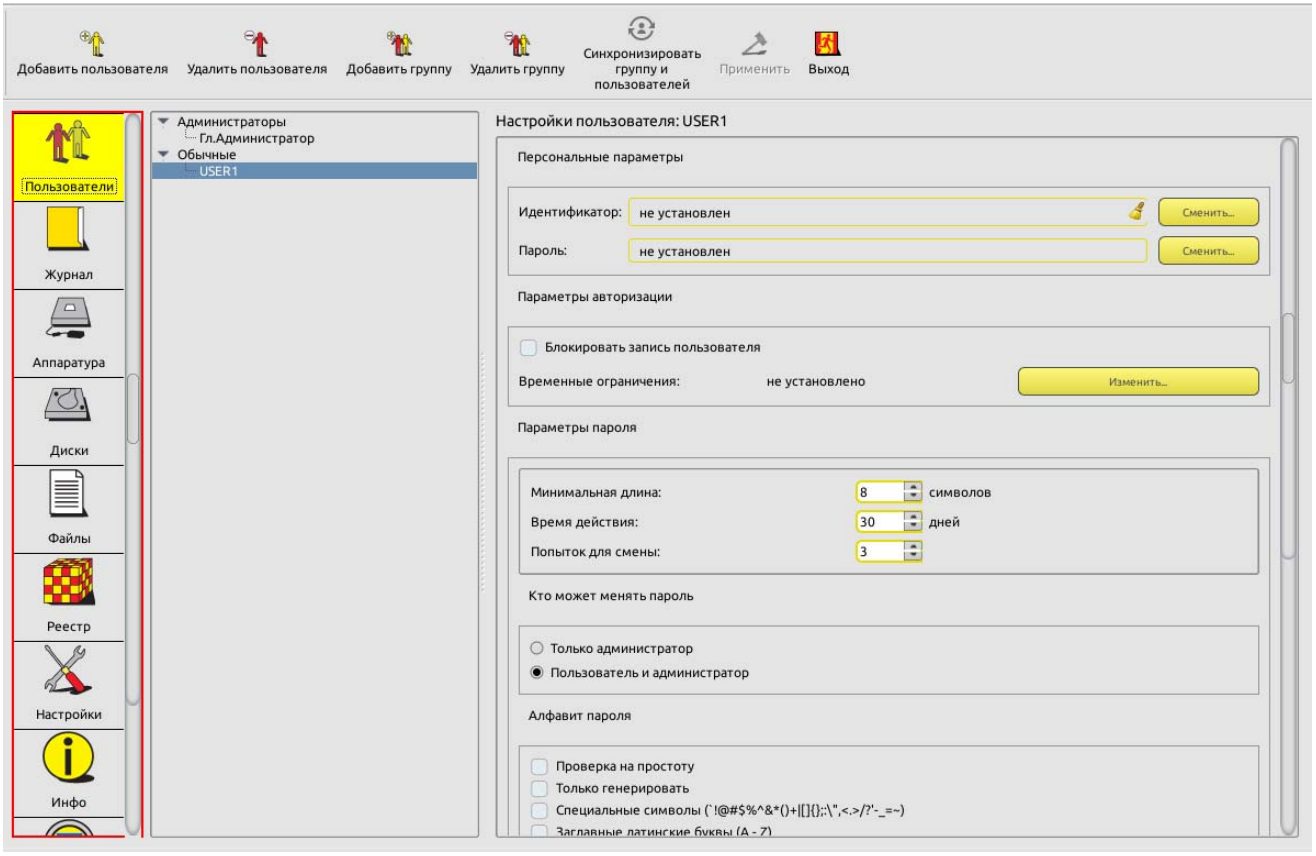

Рисунок 21 – Параметры пользователей в группе «Обычные» (для моделей Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019)

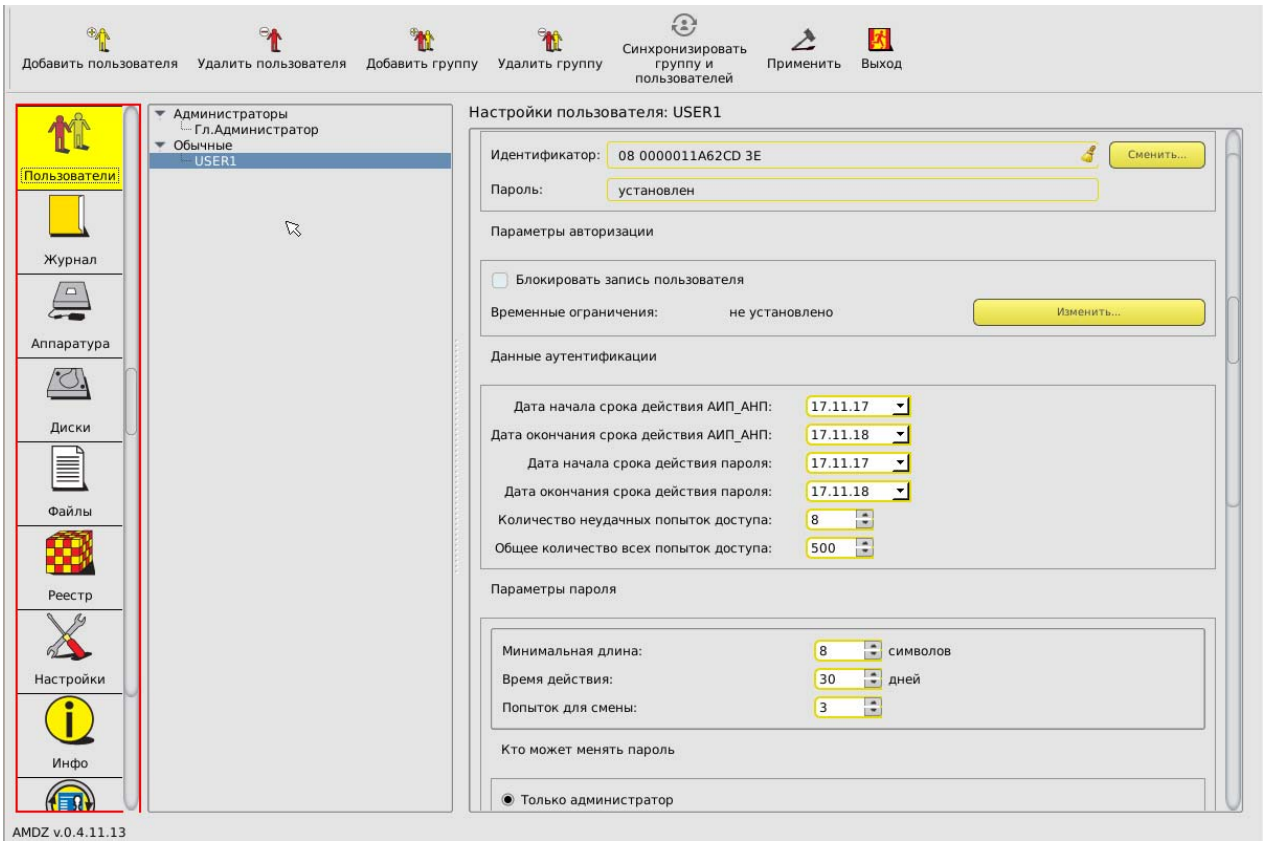

Рисунок 22 - Параметры пользователей в группе «Обычные» (для моделей Аккорд-АМДЗ» ТУ 4012-054-11443195-2013)

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

Настройки параметров авторизации пользователей группы «Обычные» в части режима блокировки аналогичны настройкам соответствующих параметров авторизации пользователей группы «Администраторы».

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 23).

Рисунок 23 - 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. Данные аутентификации

ВНИМАНИЕ! Данный пункт распространяется только на модели «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013.

Процедура настройки данных аутентификации для учетных записей пользователей из группы «Обычные»:

- является обязательной (для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013) и может быть выполнена либо на этапе настройки общих параметров группы «Обычные», либо на этапе настройки каждой учетной записи (в рамках настоящего пункта Руководства);
- аналогична процедуре настройке данных аутентификации для учетной записи «Гл. Администратор» (см. 3.2.2).

3.3.5.4. Параметры пароля

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

3.3.5.5. Время действия

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

3.3.5.6. 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 выполнить процедуру установки параметров учетной записи созданного администратора. Данная процедура аналогична соответствующим процедурам, выполняемым при настройке параметров учетной записи «Гл. Администратор» (см. 3.2).

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

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 выполнить процедуру установки параметров учетной записи созданного пользователя. Данная процедура аналогична соответствующим процедурам, выполняемым при настройке параметров учетной записи «Гл. Администратор» (см. 3.2).

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

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 среды администрирования 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 подразделах 3.3.2 и 3.3.3.

3.8. Удаление группы пользователей

Для выполнения процедуры удаления группы пользователей необходимо в главном окне среды администрирования 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. Синхронизация параметров групп и пользователей

Синхронизация может понадобиться при изменении параметров группы и последующем присвоении этих параметров всем пользователям, входящим в данную группу.

Для выполнения синхронизации параметров следует в главном окне среды администрирования выбрать из списка группу пользователей, параметры которой необходимо присвоить всем пользователям внутри группы, и нажать кнопку <Синхронизировать группу и пользователей> на панели инструментов (рисунок 1).

Доступна синхронизация всех общих параметров группы, кроме параметров из группы элементов «Данные аутентификации» (для моделей «Аккорд-АМДЗ» ТУ 4012-054-11443195-2013, подробнее о данных аутентификации см. 3.2.2).

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 среды администрирования нужно выбрать объект администрирования <Аппаратура> и нажать <Enter>. На экран выводится окно контроля аппаратуры (рисунок 24).

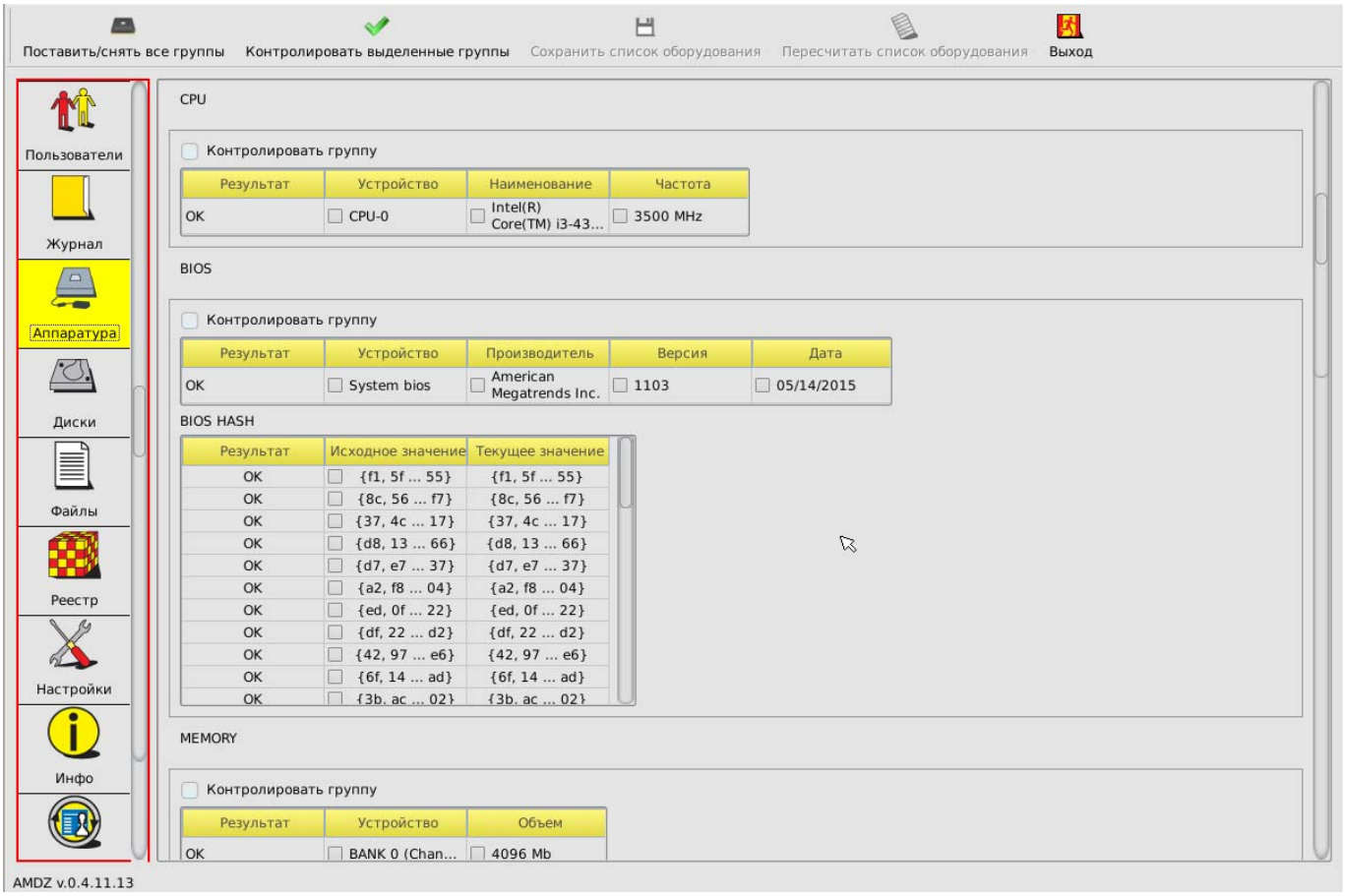

Рисунок 24 - Окно контроля аппаратной части компьютера

В данном окне выводится список классов контролируемых устройств, содержащий отдельные устройства и их параметры.

Установкой соответствующего флага можно включить/исключить в процедуру контроля любой класс или устройство.

Имеется возможность, зажав левую кнопку мыши, выделить несколько объектов (в том числе из разных групп) и установить их на контроль посредством нажатия кнопки <Контролировать выделенные группы> на панели инструментов или при помощи соответствующего пункта контекстного меню, вызываемого щелчком правой кнопкой мыши.

Внесенные изменения подтверждаются нажатием кнопки <Сохранить список оборудования> на панели инструментов.

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.

Подключение USB-устройств с VID «17e4», «072» не считается нарушением конфигурации оборудования.

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 среды администрирования на экран выводится окно контроля служебных областей дисков (рисунок 25). 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>.

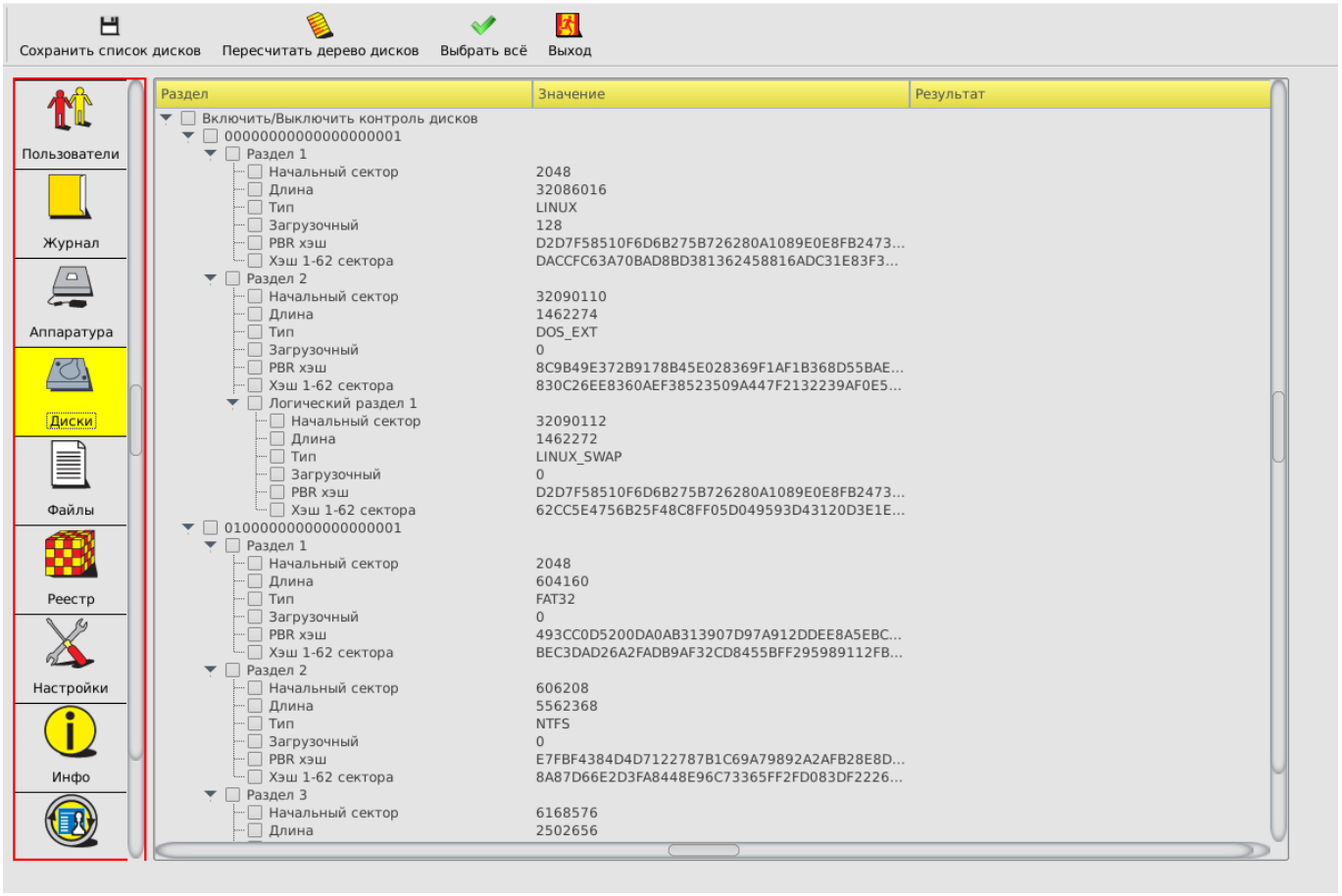

Рисунок 25 - Окно контроля служебных областей диска

3.10.3. Контроль целостности файлов

После выбора объекта администрирования <Файлы> в левой панели на экран выводится окно контроля файлов (рисунок 26). СЗИ «Аккорд-АМДЗ» обеспечивает контроль целостности программ и данных до загрузки ОС, защиту от внедрения разрушающих программных воздействий. 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.

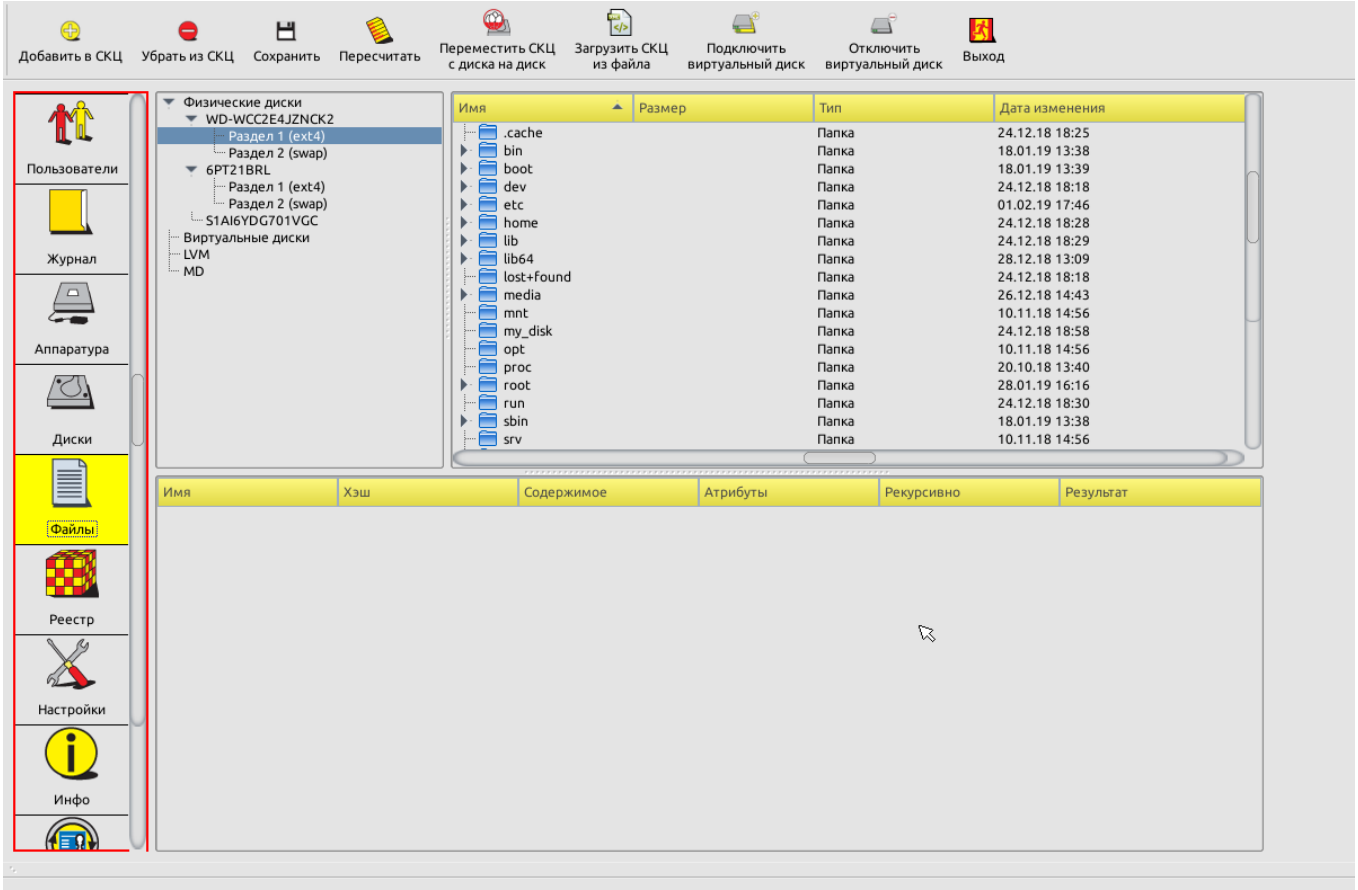

Рисунок 26 - Окно контроля целостности файлов

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 26);
- 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 27).

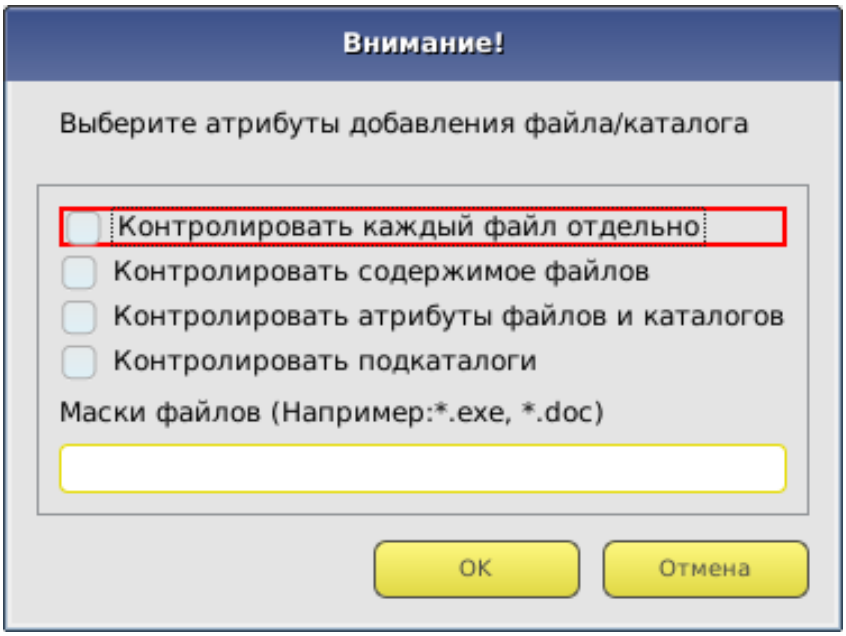

Рисунок 27 – Окно выбора атрибутов добавления каталога

По кнопке <OK> выбранный каталог будет добавлен в список контроля целостности (рисунок 28).

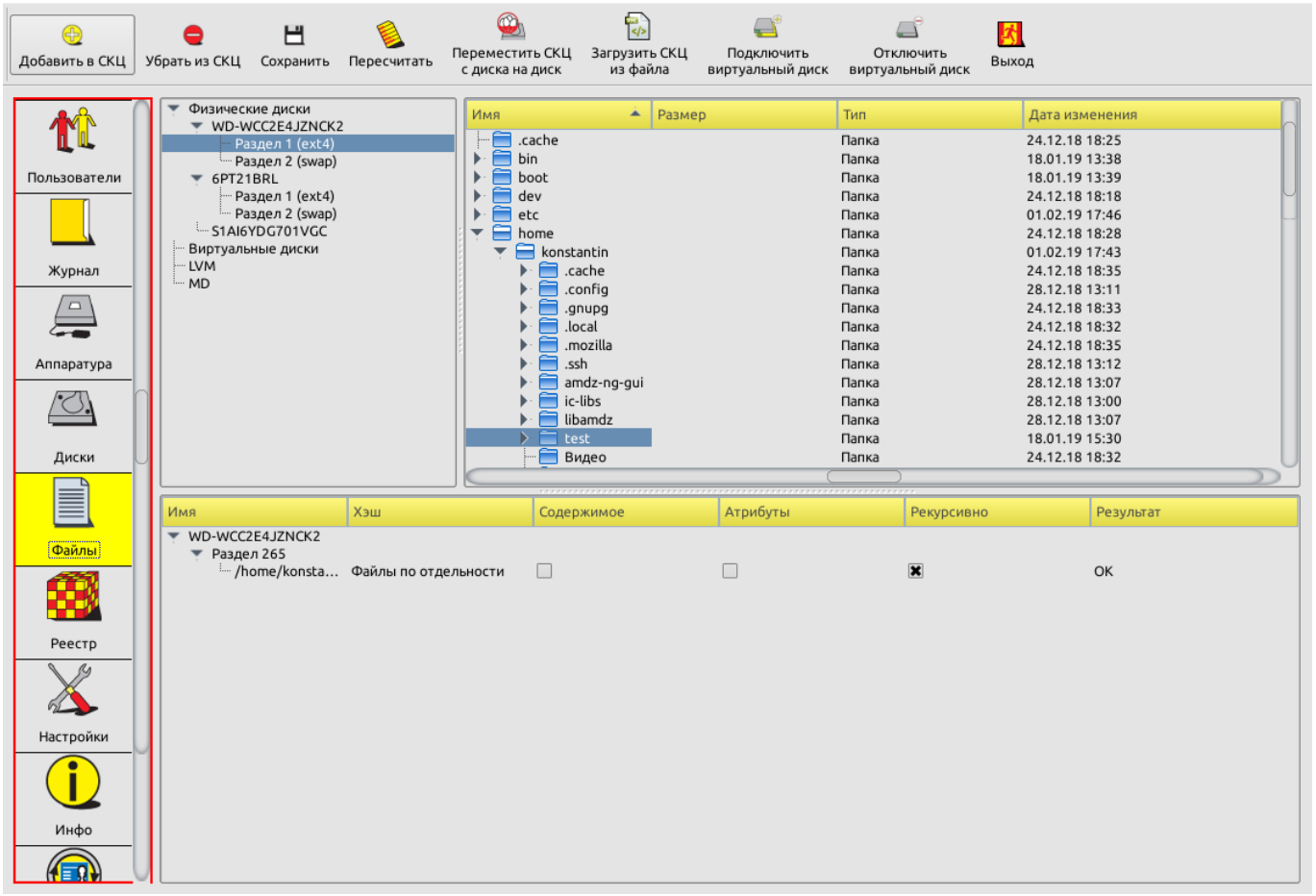

Рисунок 28 – Список контроля целостности с добавленным в него каталогом

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 29).

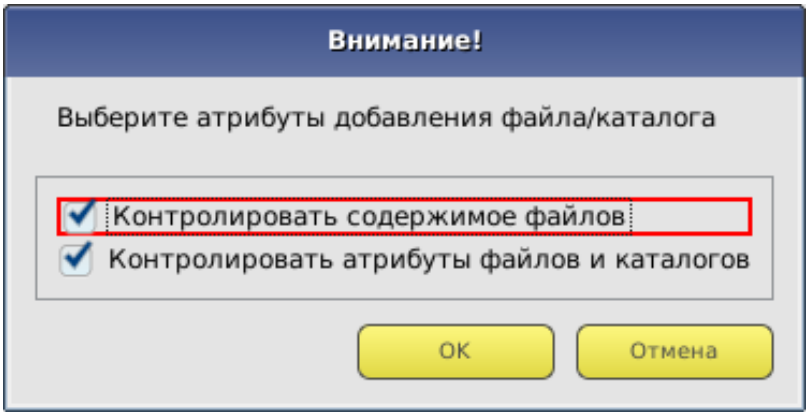

Рисунок 29 – Окно выбора атрибутов добавления файла

По кнопке <OK> выбранный файл будет добавлен в список контроля целостности (рисунок 30).

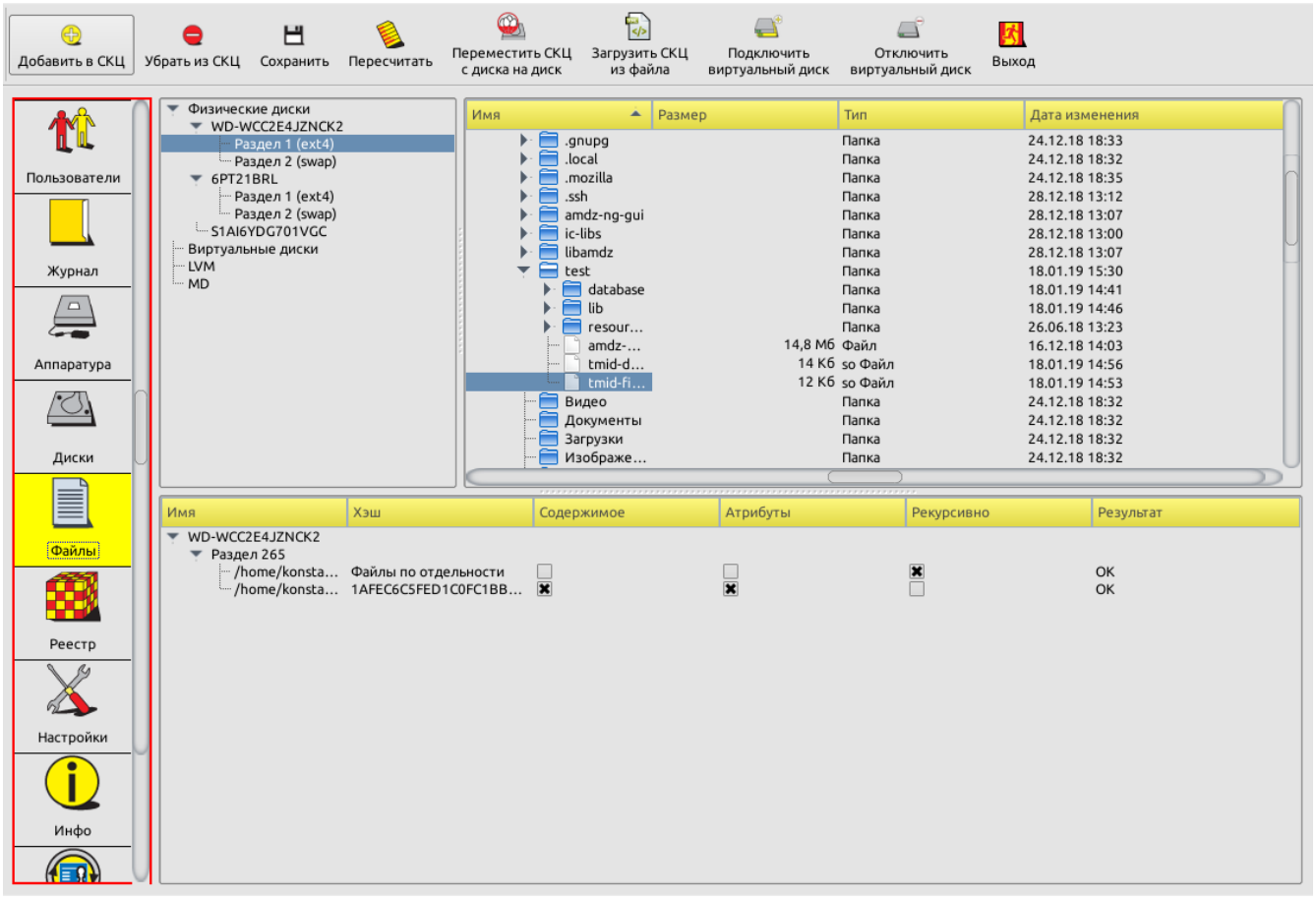

Рисунок 30 – Список контроля целостности с добавленным в него файлом

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 среду администрирования, может выполнить операцию проверки в разделе <Файлы> и выявить измененные файлы.

ВНИМАНИЕ! Если требуется внести изменения в списке контроля целостности файлов (например, добавить или удалить файлы/каталоги в СКЦ), в котором ранее были обнаружены нарушения, следует **сначала выполнить**

пересчет КС в «старом» списке (посредством нажатия кнопки <Пересчитать>), затем выполнить необходимые изменения и нажать кнопку <Сохранить>.

Примечание: *Количество файлов, которое можно установить на контроль, зависит от операционной системы и от длины пути к каталогу, где находятся файлы. Среднее количество составляет 1200-1500 файлов. Списки файлов различных ОС семейства Windows, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»), приведены в Приложениях 3 - 9 к настоящему Руководству.*

В СЗИ «Аккорд-АМДЗ» реализована возможность установки файлов на контроль с использованием шаблонов. Пользователь может выбрать стандартный шаблон с рекомендуемым списком контроля целостности файлов или использовать собственный шаблон, прописав в нем необходимые файлы и обозначив флаги контроля. Списки контролируемых файлов, входящих в стандартные шаблоны, а также рекомендации по созданию новых шаблонов описаны в Приложениях 10 – 17 к настоящему Руководству.

При необходимости использования шаблона для составления списка контроля целостности файлов следует нажать кнопку <Загрузить СКЦ из файла>. В появившемся окне выбора верхнее поле Выбрать файл раскрывает список стандартных шаблонов (рисунок 31). Необходимый шаблон загружается по кнопке <Выбрать файл>. Нижнее поле позволяет выбрать шаблон, созданный пользователем. При нажатии кнопки <ОК> шаблон добавляется в СКЦ (рисунок 30).

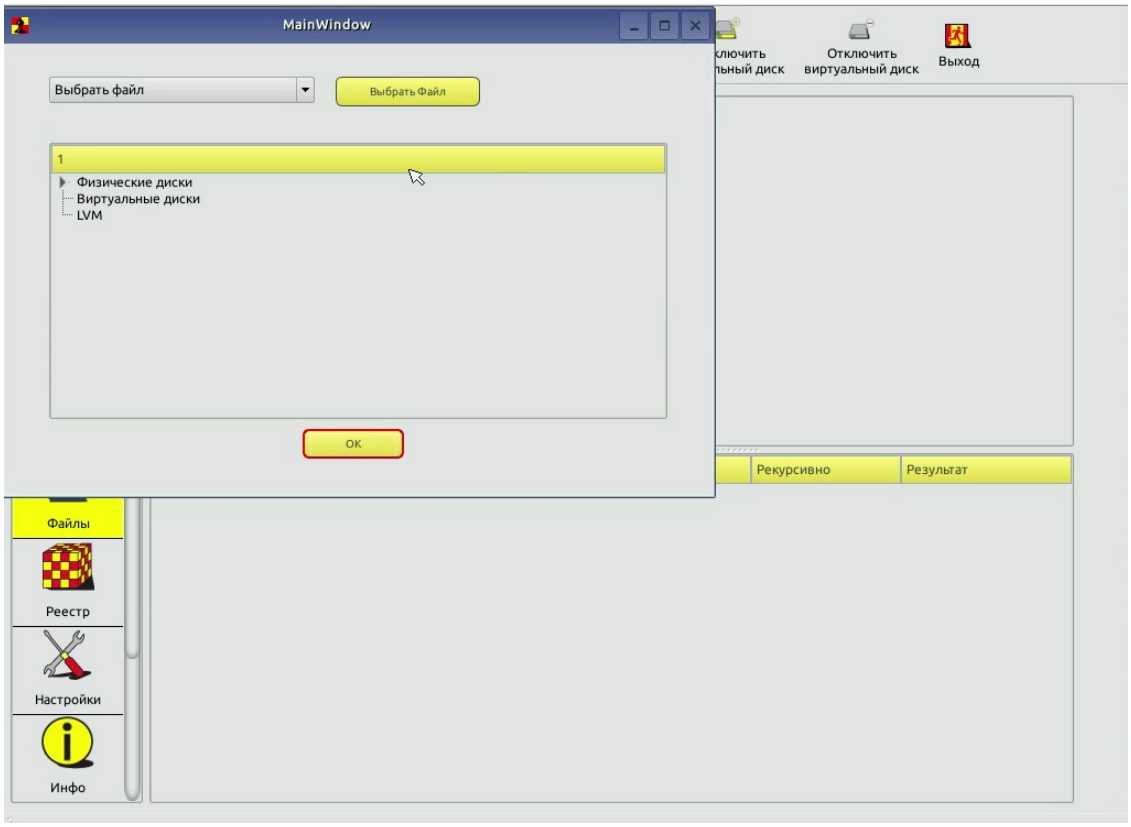

Рисунок 31 - Выбор шаблона при нажатии кнопки <Загрузить СКЦ из файла>

3.10.4. Контроль целостности реестра Windows

Данная функция позволяет контролировать целостность разделов реестра Windows 95/98/ NT/ 2000/ XP/ Vista/ 2008/ 2008 R2/ 7/ 8/ 8.1/ 2012/ 2012 R2.

После выбора объекта администрирования <Реестр> в левой панели на экран выводится окно со списком контролируемых реестров. В начальный момент список пуст. Для добавления записей в список следует нажать кнопку <Обзор> и в появившемся далее окне со списком логических разделов жесткого диска данного компьютера выбрать тот раздел, в котором установлена ОС. В окне контроля целостности реестра появится дерево каталогов данного раздела (рисунок 32).

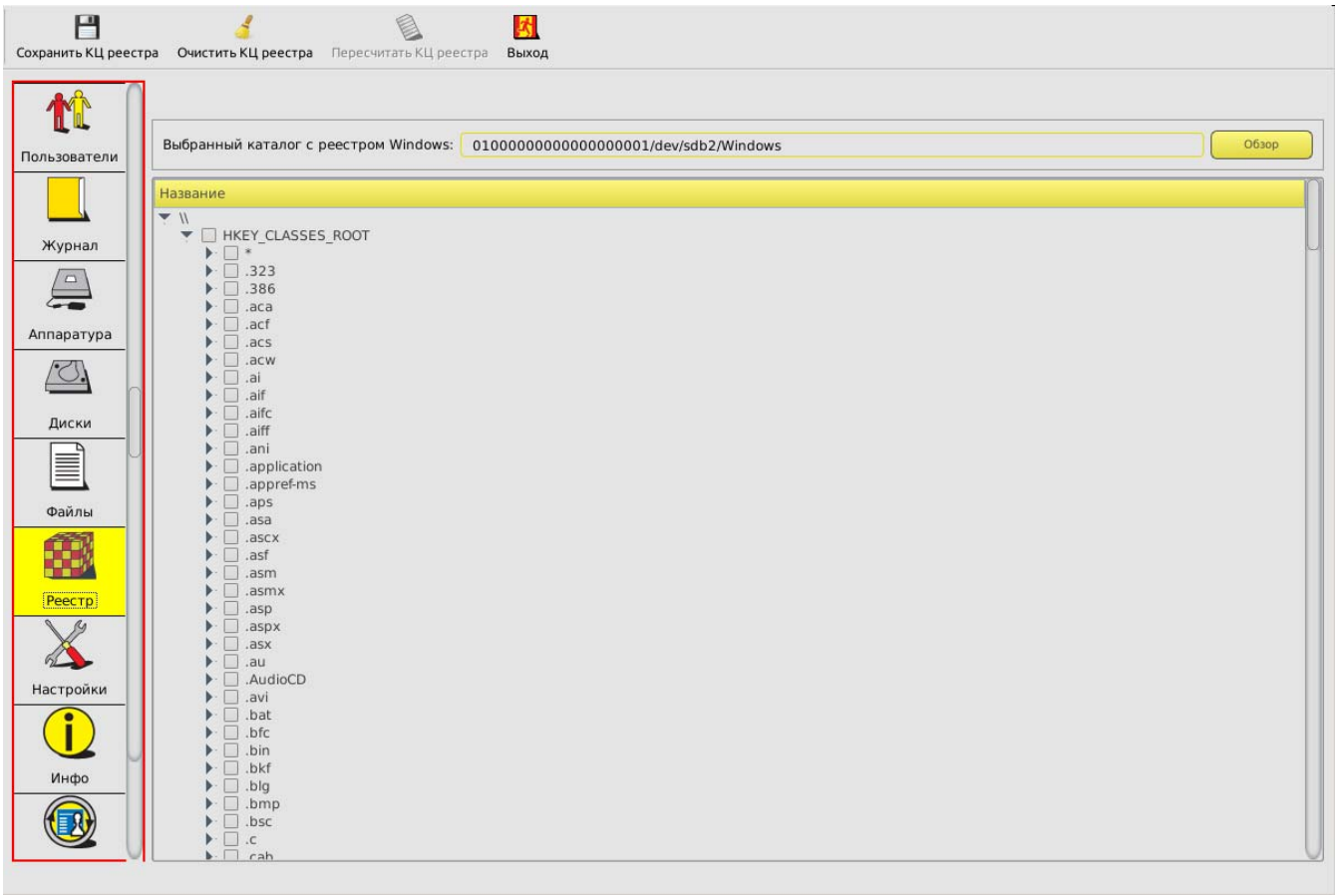

Рисунок 32 - – Информация о состоянии реестра

Для добавления ветки реестра в список контролируемых комплексом объектов следует выбрать ее из списка, установить напротив нее галочку и нажать кнопку <Сохранить КЦ реестра> (рисунок 33).

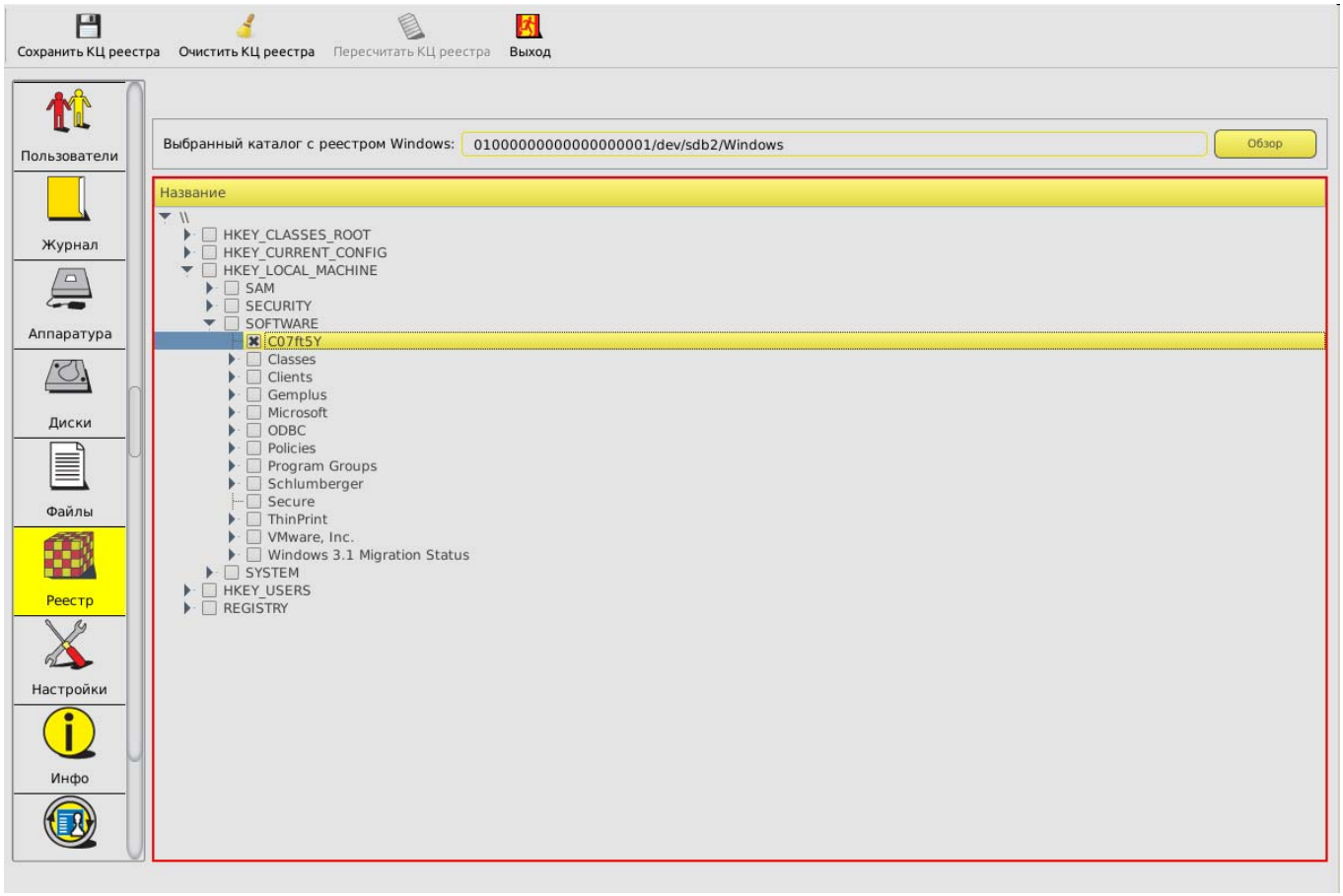

Рисунок 33 - Постановка ветви реестра на контроль целостности

В случае нарушения целостности какой-либо ветки реестра на вкладке «Реестр» все нарушения выделяются цветом.

Для перерасчета контрольных сумм списка контролируемых веток системного реестра следует нажать кнопку <Пересчитать КЦ реестра>.

После перерасчета КЦ необходимо выполнить сохранение новых КС, нажав на кнопку <Сохранить КЦ реестра>.

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 всех попытках несанкционированного доступа к компьютеру.

Размер энергонезависимой памяти, в которой размещается системный журнал, составляет 256 Кбайт. Такой объем памяти позволяет вместить в журнале не менее 1010 записей. При штатной работе «Аккорд-АМДЗ» (когда в системе отсутствуют серийные нарушения целостности файлов/реестра и не используется чрезмерно глубокая вложенность файлов в каталогах) количество записей в журнале может быть больше этого значения в десятки или сотни раз.

Для просмотра журнала следует в главном окне среды администрирования выбрать объект администрирования <Журнал>. На экран выводится окно системного журнала (рисунок 34). Подробнее об основных параметрах, фиксируемых в журнале, и их обозначениях см. Приложение 1.

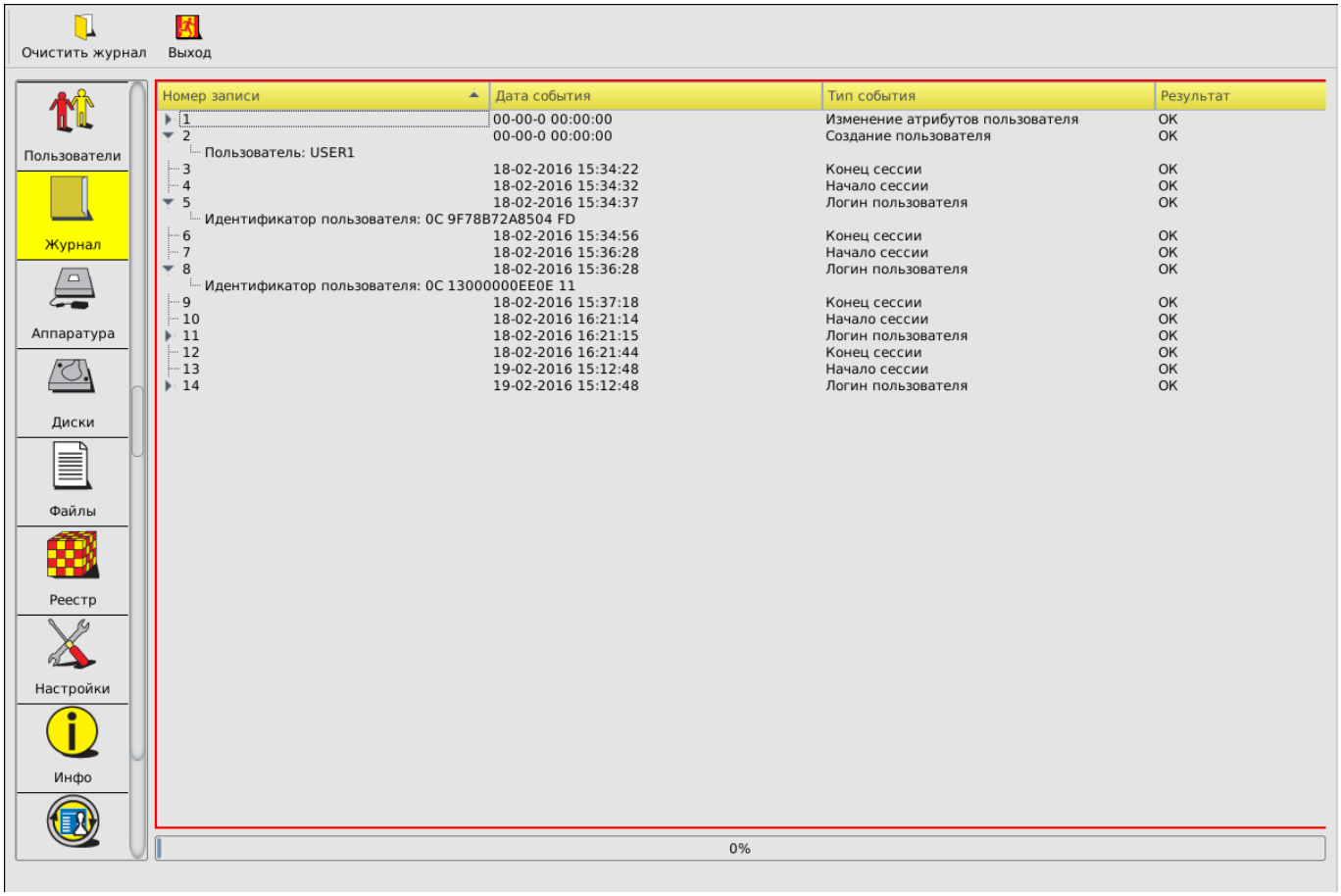

Рисунок 34 - Системный журнал контроллера

Если заполнение журнала превышает 85%, при загрузке компьютера выдается предупреждение, но загрузка продолжается. Если заполнение журнала превышает 95%, то загрузка для пользователя блокируется, и требуется вмешательство администратора.

Для очистки журнала служит кнопка <Очистить журнал> (рисунок 34).

3.12.Общие настройки комплекса

Редактирование общих настроек комплекса выполняется администратором комплекса, обладающим правами на изменение настроек комплекса «Аккорд-АМДЗ» (см. п. 3.3.4.7).

Для изменения общих настроек комплекса необходимо нажать кнопку <Настройки> в меню выбора объектов администрирования. На экран выводится окно с настройками комплекса (рисунок 35, рисунок 36).

В настройках комплекса установлены следующие разделы:

- данные конфигурации;
- режим запуска ACRUN;

- сторожевой таймер.

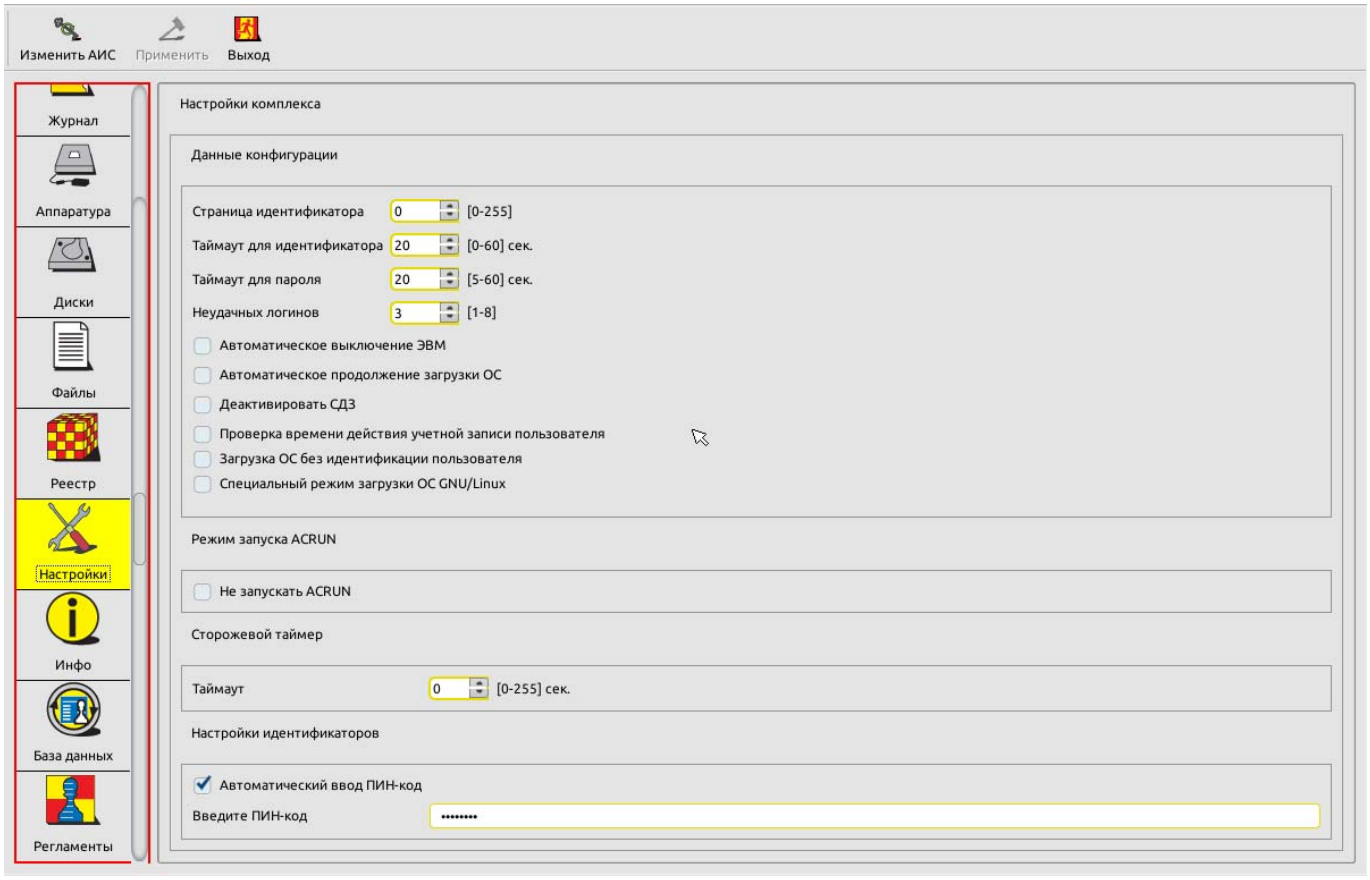

Рисунок 35 - Общие настройки комплекса (для моделей «Аккорд-АМДЗ ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019)

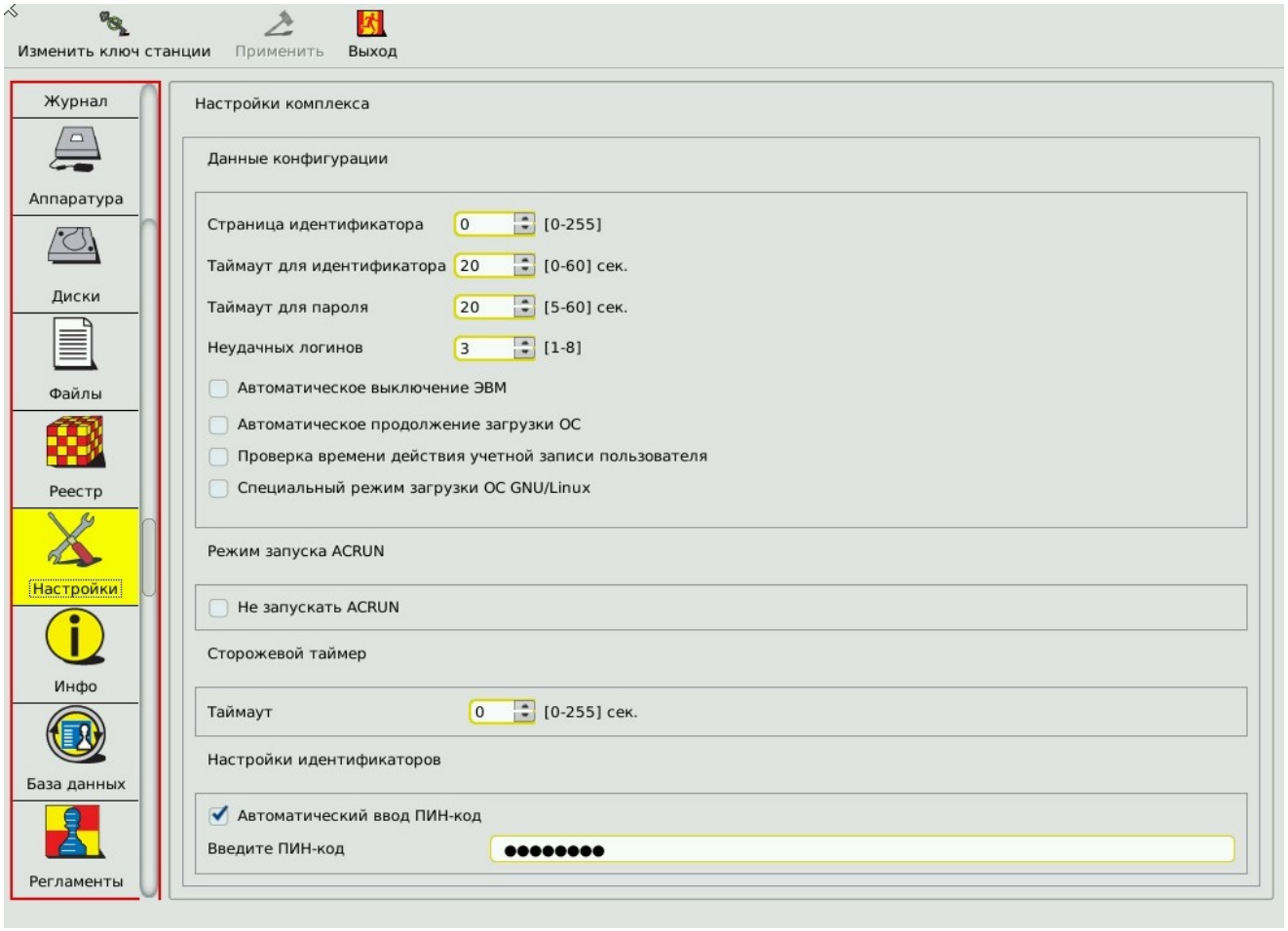

Рисунок 36 - Общие настройки комплекса (для моделей «Аккорд-АМДЗ ТУ 4012-054-11443195-2013)

3.12.1. Данные конфигурации

Для настроек данных конфигурации установлены следующие параметры:

- страница идентификатора;
- таймаут для идентификатора;
- таймаут для пароля;
- количество неудачных логинов;
- автоматическое выключение ЭВМ;
- автоматическое продолжение загрузки ОС;
- проверка времени действия учетной записи пользователя;
- деактивировать Аккорд-АМДЗ (для моделей «Аккорд-АМДЗ ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019);
- загрузка ОС без идентификации пользователя (для моделей «Аккорд-АМДЗ ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019);
- специальный режим загрузки ОС GNU/Linux (для моделей ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019 начиная с версии 0.3.11.x, для моделей «Аккорд-АМДЗ ТУ 4012-054-11443195-2013 начиная с версии 0.4.11.x).

«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. При выставлении параметра «Таймаут для идентификатора» в значение «0» таймер игнорируется[1].

Параметр «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.

Если в настройках конфигурации установлен параметр «Автоматическое выключение ЭВМ», то если по истечении заданного интервала времени (за данный интервал времени отвечает параметр «Таймаут для идентификатора») идентификатор пользователя не был предъявлен, компьютер автоматически выключается[2].

Установка параметра «Автоматическое продолжение загрузки ОС» позволяет автоматически продолжать загрузку компьютера без нажатия кнопки <Продолжить загрузку> в том случае, если в процессе выполнения процедуры контроля целостности не было выявлено нарушений.

Установка параметра «Деактивировать Аккорд-АМДЗ» (для моделей «Аккорд-АМДЗ ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019) позволяет деактивировать комплекс без механических операций вскрытия и установки/извлечения компонентов. Подробнее о способах программной активации/деактивации СЗИ НСД «Аккорд-АМДЗ» см. раздел 5.

Установка параметра «Проверка времени действия учетной записи пользователя» позволяет учитывать настройки параметра «Время действия» для учетных записей пользователей (подробнее о настройке параметра «Время действия» см. 3.3.2.5).

Если в настройках конфигурации установлен параметр «Загрузка ОС без идентификации пользователя» (для моделей «Аккорд-АМДЗ ТУ 4012-038-

---

[1)] Для моделей «Аккорд-АМДЗ» с ФПО версии 0.3.9.11 (0.4.9.11) и выше – на базе всех контроллеров

[2)] Для моделей «Аккорд-АМДЗ», разработанных по ТУ 4012-054-11443195-2013, в этом случае выполняется завершение работы ПО «Аккорд-АМДЗ» (все сервисы и службы «Аккорд-АМДЗ» останавливаются, драйверы завершают работу), работа с ОС компьютера невозможна. Однако для полного выключения компьютера (выключения питания) необходимо нажать на системном блоке кнопку «Выключение» («Power»)

11443195-2011 и ТУ 26.20.40.140-079-37222406-2019), то в процессе загрузки компьютера с установленным комплексом «Аккорд-АМДЗ» выполнение процедур идентификации и аутентификации пользователя не требуется, но загрузка ОС осуществляется только после успешного завершения всех контрольных процедур (установленных в рамках подраздела 3.10).

Параметр «Специальный режим загрузки ОС GNU/Linux» позволяет активировать специальный режим загрузки ОС.

3.12.2. Установка специального режима загрузки ОС GNU/Linux

В «Аккорд-АМДЗ» (ТУ 4012-054-11443195-2013 начиная с версии 0.4.11.x, ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019 начиная с версии 0.3.11.x) имеется возможность установки специального режима загрузки ОС GNU/Linux.

В данном подходе загрузка передается не загрузчику на диск, а напрямую ядру ОС Linux. Это позволяет, в частности, повысить защищенность процесса загрузки за счет минимизации количества промежуточных звеньев, безопасность которых необходимо обеспечить.

Если данный режим включен, то после успешной проверки целостности среды выполняется проверка целостности ядра, RAM-диска и файла конфигурации, далее «Аккорд-АМДЗ» передает управление выбранному ядру ОС, минуя передачу управления дисками.

Для автоматической загрузки GNU Linux системы после процедур контроля целостности «Аккорд-АМДЗ» необходимо выполнить предварительную настройку конфигурационного файла ACBOOT.

ВНИМАНИЕ! Настройка должна быть произведена до установки контроллера «Аккорд-АМДЗ»!

Для активации данного режима следует:

1. Создать или скопировать заранее подготовленный файл конфигурации с именем ACBOOT в корневой каталог загрузочного раздела (раздел жесткого диска, на котором находится ядро ОС и штатный загрузчик). В общем случае переход в него выполняется командой “cd /” в консоли операционной системы. При использовании LVM файл необходимо создать в каталоге /boot).

Данный файл рекомендуется устанавливать на контроль в «Аккорд-АМДЗ». В файле необходимо прописать следующие параметры:

- в первой строке – имя ядра linux (полный путь к файлу в разделе);
- во второй строке – имя initrd (полный путь к файлу в разделе);
- в третьей строке – параметры ядра, передающиеся при загрузке.

В случае использования загрузчика grub2, что верно для большинства дистрибутивов, необходимые значения можно найти в файле menu.list.

Пример настройки:

Файл menu.list:

```
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Atlix-grsec (2.6.54.44-4.atl3.x86_64.grsec)
root (hd0,0)
kernel /vmlinuz-2.6.54.44-4.atl3.x86_64.grsec ro root=/dev/mapper/VolGroup-lv_root LANG=ru_RU.UTF-8 rd_NO_LUKS rd_NO_MD rd_LVM_LV=VolGroup/lv_swap rd_LVM_LV=VolGroup/lv_root KEYBOARDTYPE=pc KEYTABLE=ru rd_NO_DM
initrd /initramfs-2.6.54.44-4.atl3.x86_64.grsec.img
```

В этом случае файл ACBOOT будет иметь следующее содержание:

```
/vmlinuz-2.6.54.44-4.atl3.x86_64.grsec
/initramfs-2.6.54.44-4.atl3.x86_64.grsec.img
ro root=/dev/mapper/VolGroup-lv_root LANG=ru_RU.UTF-8 rd_NO_LUKS rd_NO_MD rd_LVM_LV=VolGroup/lv_swap rd_LVM_LV=VolGroup/lv_root KEYBOARDTYPE=pc KEYTABLE=ru rd_NO_DM
```

(третью строку менять не нужно)

Первый способ

Для создания файла необходимо перейти в директорию grub /boot/grub и открыть в ней с помощью текстового редактора файл grub.cfg.

```
nano /boot/grub/grub.cfg
```

После этого необходимо найти строчку, по которой осуществлялась загрузка. В нашем случае это 'AstraLinuxSE GNU/Linux, with Linux 4.2.0-23-generic'. В файле данный блок в нашем случае выглядит следующим образом:

```
menuentry 'AstraLinuxSE GNU/Linux, with Linux 4.2.0-23-generic' --class astralinuxse --class gnu-linux --class gnu --class os --unr$
        load_video
        insmod gzio
        if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
        insmod part_msdos
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root  67ddae89-517a-49f4-b527-ace540889505
        else
          search --no-floppy --fs-uuid --set=root 67ddae89-517a-49f4-b527-ace540889505
        fi
        echo    'Loading Linux 4.2.0-23-generic ...'
        linux        /boot/vmlinuz-4.2.0-23-generic   root=UUID=67ddae89-517a-49f4-b527-ace540889505 ro  quiet splash
        echo    'Loading initial ramdisk ...'
        initrd  /boot/initrd.img-4.2.0-23-generic
```

Из данного блока нас интересуют последние 4 записи.

В соответствии с этими записями в нашем случае ACBOOT будет выглядеть следующим образом:

```
/boot/vmlinuz-4.2.0-23-generic
/boot/initrd.img-4.2.0-23-generic
```

```
root=UUID=67ddae89-517a-49f4-b527-ace540889505 ro  quiet splash
```

Второй способ

Помимо этого, в данном файле можно задавать адреса разделов вместо UUID для корневой директории (root). Для этого необходимо запустить blkid (запускать данную утилиту необходимо под учетной записью root). По результатам будет выдан список доступных разделов:

```
/dev/sda1: UUID="67ddae89-517a-49f4-b527-ace540889505" TYPE="ext4"
/dev/sda5: UUID="29f85fee-ff77-4ae2-ac25-b0ad191f8744" TYPE="swap"
```

В данном случае нас интересует первый раздел, поскольку UUID в нем соответствует UUID из конфигурации GRUB. Для нашего случая grub файл имеет следующее содержимое:

```
 /boot/vmlinuz-4.2.0-23-generic
/boot/initrd.img-4.2.0-23-generic
root=/dev/sda1  ro  quiet splash
```

Третий способ

Как и во втором случае, вместо UUID корневой директории можно задавать и метки. Для этого необходимо установить утилиту e2label, выполнив для этого команду:

```
apt-get install e2fsprogs
```

После этого следует запустить метку корневого раздела. В данном случае метка создается для раздела /dev/sda1, в предыдущем пункте было описано, как определить путь к корневому разделу. После этого следует установить метку для раздела (использовано название метки rootfs), выполнив команду:

e2label /dev/sda1 rootfs

Убедиться, что метка корректно установлена, можно через утилиты просмотра дисков (к примеру, gparted). Теперь файл ACBOOT будет выглядеть следующим образом

```
/boot/vmlinuz-4.2.0-23-generic
/boot/initrd.img-4.2.0-23-generic
root=LABEL=rootfs ro  quiet splash
```

2. На вкладке «Настройки» главного окна среды администрирования установить флаг «Специальный режим загрузки ОС GNU/Linux».

3. Установить на контроль файл конфигурации, ядро и initrd.

3.12.3. 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.

3.12.4. Сторожевой таймер

Параметр «Сторожевой таймер»[1] 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.

Действие сторожевого таймера в общем случае не распространяется на процедуры, связанные с выполнением настроек в BIOS компьютера. В зависимости от модели установленной в компьютере материнской платы сторожевой таймер может как срабатывать, так и не срабатывать при выполнении пользователем настроек в BIOS компьютера.

3.13.Информация о комплексе

На вкладке «Инфо» (рисунок 37) главного окна среды администрирования отображается следующая информация о комплексе:

- версия ПО «Аккорд-АМДЗ»;
- серийный номер контроллера «Аккорд-АМДЗ»;
- контрольные суммы основных компонентов.

[1)] На контроллерах «Аккорд-LE» данный функционал отсутствует

Рисунок 37 - Вкладка «Инфо» главного окна среды администрирования

3.14.Экспорт/импорт баз данных

3.14.1. 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. 3.14.2).

ВНИМАНИЕ! При выполнении процедур экспорта/импорта списков КЦ файлов следует учитывать сведения, указанные в 3.14.4.

3.14.2. 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. 3.14.3).

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».

3.14.3. Экспорт/импорт баз данных

Для того чтобы начать процедуру экспорта/импорта базы данных «Аккорд-АМДЗ», следует в главном окне среды администрирования перейти на вкладку «База данных» и в поле «Носитель» выбрать носитель, на который (с которого) будет выполняться экспорт (импорт) базы данных (рисунок 38).

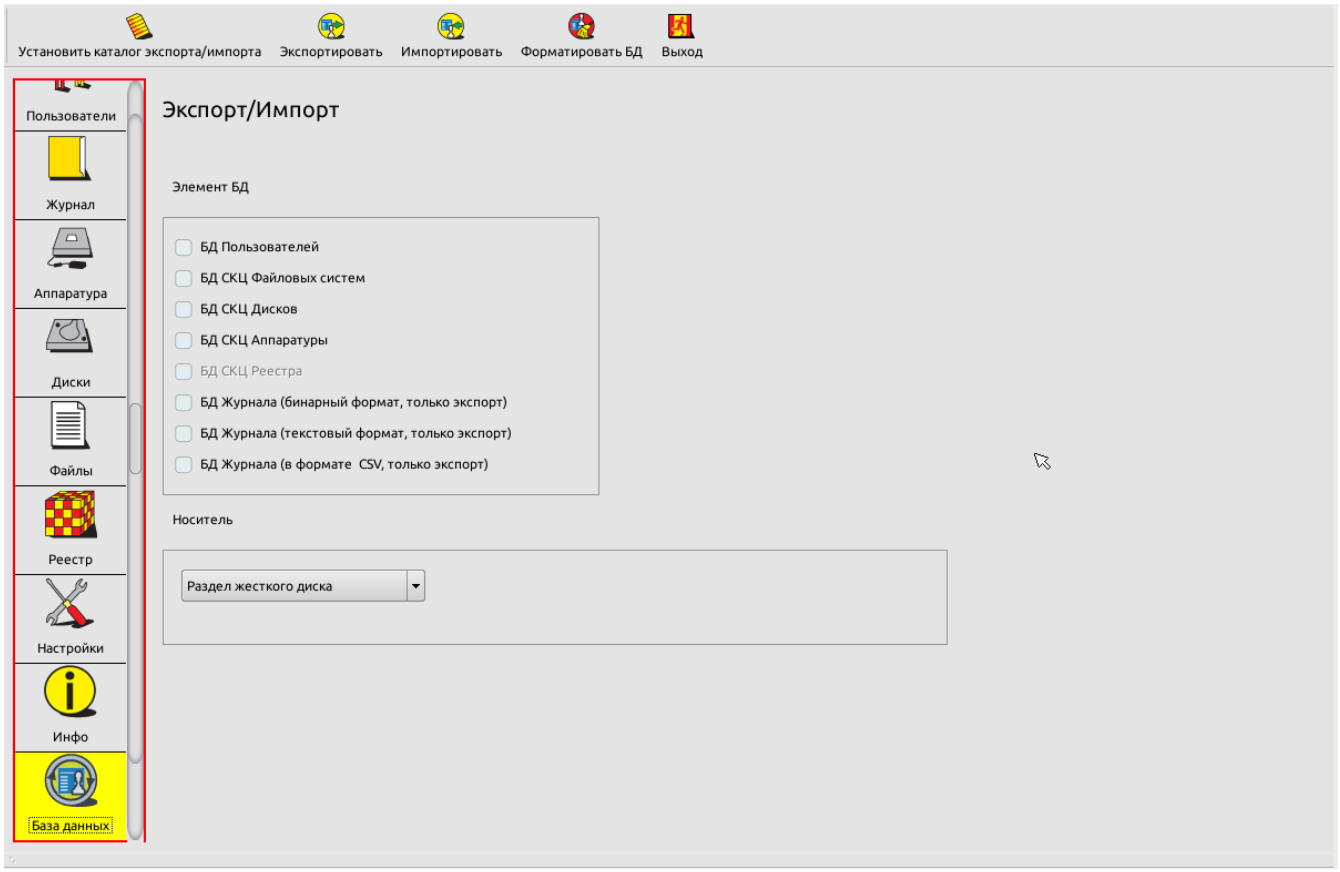

Рисунок 38 - Выбор носителя для экспорта базы пользователей

Далее, если в качестве носителя выбран раздел жесткого диска, 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 39).

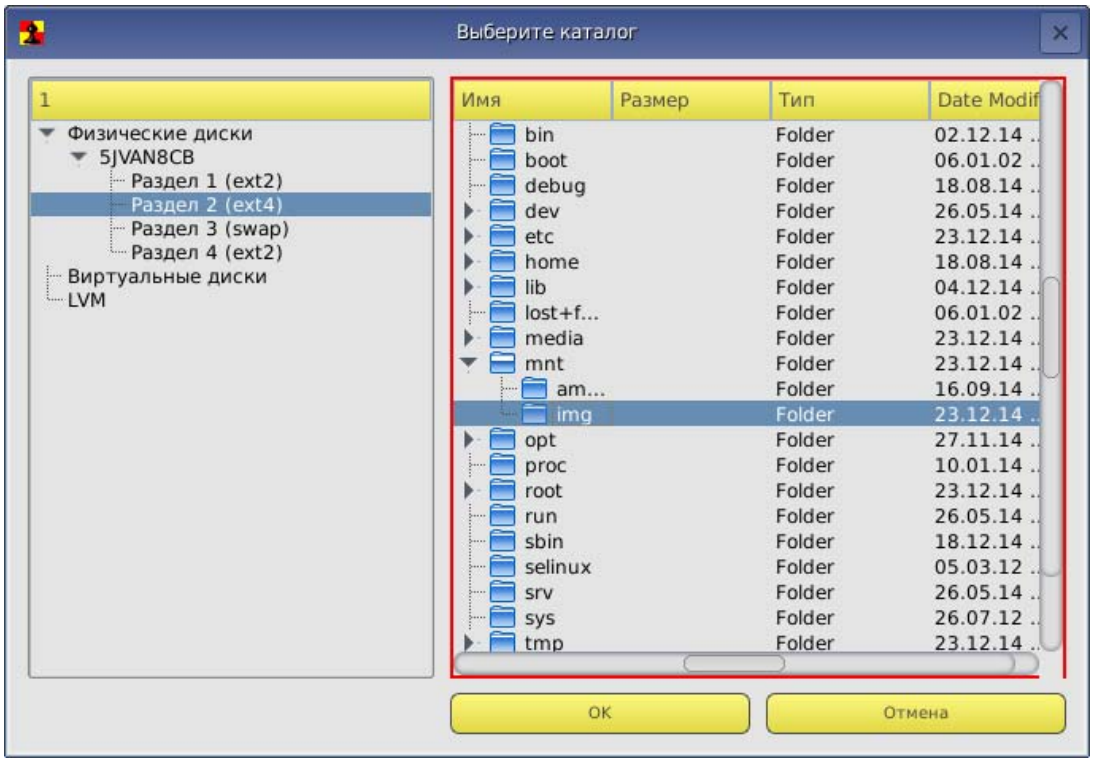

Рисунок 39 - Установка директории экспорта/импорта БД

После установки директории экспорта/импорта следует выбрать нужные элементы БД, указав их галочками, и нажать кнопку <Экспортировать>/<Импортировать> (рисунок 38).

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! После появления сообщения «Данные успешно импортированы» перезагрузка компьютера выполняется автоматически.

3.14.4. Особенности выполнения процедур экспорта/импорта списков КЦ файлов

Процедуры экспорта/импорта списков КЦ файлов имеют некоторые особенности и выполняются, как правило, в рамках следующих сценариев работы:

1. Создание СКЦ на одном компьютере и перенос его на аналогичные компьютеры. В рамках данного сценария следует выполнить:

а) экспорт/импорт СКЦ файлов;

б) изменение метки диска в СКЦ после выполнения процедуры импорта (подробнее об изменении метки диска см. 3.14.5).

2. Замена контроллера «Аккорд-АМДЗ» в компьютере. В рамках данного сценария достаточно выполнить экспорт на исходном контроллере «Аккорд-АМДЗ», а затем – импорт на новом.

3. Замена диска/переустановка ОС на компьютере. В рамках данного сценария достаточно изменить метку диска в СКЦ.

3.14.5. Изменение метки диска в списке КЦ файлов после выполнения процедуры импорта

Для изменения метки диска следует на вкладке «Файлы» главного окна среды администрирования нажать кнопку <Переместить СКЦ с диска на диск> (рисунок 26).

В появившимся окне необходимо указать метку диска от ПЭВМ с установленным «Аккорд-АМДЗ», с которой был производен экспорт, и нажать кнопку <ОК>.

Далее следует указать метку диска от ПЭВМ, на которую произведен импорт СКЦ, и нажать кнопку <ОК>.

Далее следует нажать кнопку <Сохранить> (на верхней панели вкладки «Файлы») и выполнить перезагрузку ПЭВМ (кнопка <Выход> на верхней панели вкладки «Файлы», затем – кнопка <Перезагрузить> в окне приветствия администратора).

Затем, при необходимости, следует выполнить пересчет КС с сохранением изменений (кнопки <Пересчитать> и <Сохранить> на верхней панели вкладки «Файлы»).

3.15. Форматирование баз данных контроллера

Процедура форматирования баз данных контроллера, вызываемая кнопкой <Форматировать БД> на вкладке «База данных» главного окна среды администрирования, позволяет администратору комплекса, обладающему правами на изменение персональных параметров пользователей, 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 «Аккорд-АМДЗ» нужно проверить работоспособность компьютера, а для этого нужно зарегистрировать идентификатор для учетной записи «Гл.Администратор» и ввести пароль. Специалисту, который выполняет проверку, придется для каждого компьютера регистрировать отдельный идентификатор и прикладывать к нему памятку 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 следует на вкладке «База данных» главного окна среды администрирования нажать кнопку <Форматировать БД> (рисунок 38).

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).

3.16.Регламентные проверки

В работе «Аккорд-АМДЗ» предусмотрена возможность выполнения процедур самотестирования.

На вкладке «Регламенты» (рисунок 40) главного окна среды администрирования можно выполнить следующие регламентные проверки в рамках самотестирования комплекса «Аккорд-АМДЗ»:

- проверка физического генератора случайных чисел (ФГСЧ);
- проверка целостности ПО;
- проверка целостности данных;
- проверка блокировки.

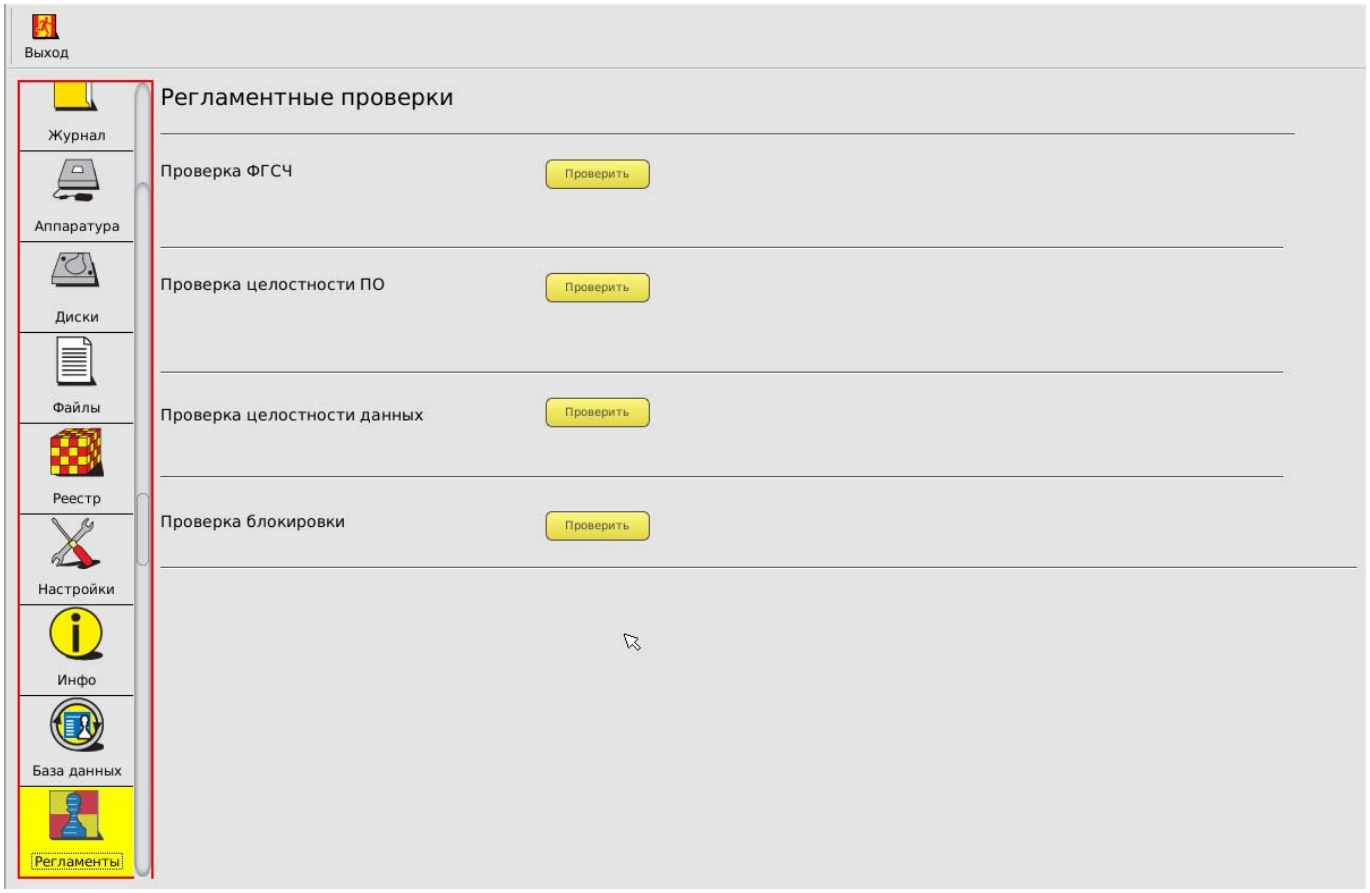

Рисунок 40 - Регламентные проверки

3.17.Выход из среды администрирования

Выход из среды 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/ 11443195.4012.054 98 / 37222406.26.20.40.140.079 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/ 11443195.4012.054 98/ 37222406.26.20.40.140.079 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

ВНИМАНИЕ! Данный пункт распространяется только на модели «Аккорд-АМДЗ» ТУ 4012-038-11443195-2011 и ТУ 26.20.40.140-079-37222406-2019.

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

Процедура деактивации комплекса может быть вызвана установкой галочки «Деактивировать Аккорд-АМДЗ» в разделе «Данные конфигурации» на вкладке «Настройки» (см. п. 3.12.1). Данная процедура выполняется администратором комплекса, обладающим правами на изменение настроек комплекса «Аккорд-АМДЗ» (см. п. 3.3.4.7).

Процедура активации комплекса может быть вызвана 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».

6. Загрузка с отчуждаемых носителей на СВТ с установленным «Аккорд-АМДЗ»

ВНИМАНИЕ! Данный пункт распространяется на контроллеры «Аккорд-АМДЗ» семейства GX.

По умолчанию, СЗИ НСД «Аккорд-АМДЗ» обеспечивает блокировку загрузки СВТ с отчуждаемых носителей.

Однако если политикой организации предусмотрена необходимость загрузки с отчуждаемого носителя (в особых случаях; например, для выполнения резервной копии жесткого диска СВТ, установки ОС, проверки на вирусы и т.п.), Администратору (пользователю, входящему в группу «Администраторы») предоставляется возможность загрузки со специально подготовленного отчуждаемого носителя.

Данная функциональность позволяет загружать различные дистрибутивы общего и специального назначения (например, на базе ОС GNU/Linux).

В рамках подготовки носителя выполняется процедура копирования на него необходимых образов ПО и подготовка файла для встроенного загрузчика. Подробные сценарии загрузки СВТ с установленным «Аккорд-АМДЗ» со специально подготовленных съемных носителей представлены в Приложении 18 к настоящему Руководству.

ВНИМАНИЕ! В процессе штатной работы на СВТ с установленным «Аккорд-АМДЗ» не рекомендуется устанавливать в качестве первого загрузочного устройства съемный носитель, поскольку в зависимости от типа СВТ и BIOS это может привести к невозможности загрузки компьютера как со съемного носителя (что является функцией безопасности «Аккорд-АМДЗ»), так и с жесткого диска компьютера.

7. 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 (495) 994-49-96

+7 (495) 994-49-97

+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. Сочетания клавиш, применяемые для работы в среде администрирования «Аккорд-АМДЗ»

Сочетание клавиш	Описание функциональности	Пояснения
Fn, где n - номер клавиши	Активация кнопки N на панели инструментов (верхняя панель главного окна среды администрирования). Счет слева направо	
Alt+n, где n - номер клавиши	Переход в пункт номер n меню выбора объектов администрирования (левая вертикальная панель главного окна среды администрирования). Счет сверху вниз	
Ctrl+Alt+Del	Перезагрузка	
Ctrl+I Alt+I Insert	Добавить пользователя	Доступно в меню «Пользователи»
Ctrl+D Alt+D	Удалить пользователя	Доступно в меню «Пользователи»
Escape	Выход из текущего элемента администрирования	
Ctrl+Enter	Смена пароля пользователя	Во время аутентификации
Ctrl+L	Вызов окна смены языка	Только в случае использования программных средств «Аккорд-АМДЗ» с возможностью выбора языка
Delete	Удалить файл из СКЦ	Доступно в меню «Файлы»
Alt+Shift+U	Обновить СКЦ оборудования Обновить СКЦ файлов Обновить СКЦ дисков	Доступно в меню «Оборудование», «Файлы» и «Диски» соответственно
Tab	Переключение между элементами интерфейса	
space	Активация графического объекта	

Приложение 3. Список файлов ОС Windows XP, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»)

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

\NTLDR
\NTDETECT.COM
\BOOT.INI
\Windows\System32\CSRSS.EXE
\Windows\System32\HAL.DLL
\Windows\System32\KERNEL32.DLL
\Windows\System32\LSASRV.DLL
\Windows\System32\LSASS.EXE
\Windows\System32\NTDLL.DLL
\Windows\System32\NTOSKRNL.EXE
\Windows\System32\PSAPI.DLL
\Windows\System32\REGAPI.DLL
\Windows\System32\RUNDLL32.EXE
\Windows\System32\SECUR32.DLL
\Windows\System32\SERVICES.EXE
\Windows\System32\SMSS.EXE
\Windows\System32\CTFMON.EXE
\Windows\System32\SVCHOST.EXE
\Windows\System32\USERINIT.EXE
\Windows\System32\USER32.DLL
\Windows\System32\WINLOGON.EXE

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

\NTLDR
\NTDETECT.COM
\BOOT.INI
\WINDOWS\SYSTEM32\CSRSS.EXE
\WINDOWS\SYSTEM32\HAL.DLL
\WINDOWS\SYSTEM32\KERNEL32.DLL
\WINDOWS\SYSTEM32\LSASRV.DLL
\WINDOWS\SYSTEM32\LSASS.EXE
\WINDOWS\SYSTEM32\NTDLL.DLL
\WINDOWS\SYSTEM32\NTOSKRNL.EXE
\WINDOWS\SYSTEM32\PSAPI.DLL
\WINDOWS\SYSTEM32\REGAPI.DLL
\WINDOWS\SYSTEM32\RUNDLL32.EXE
\WINDOWS\SYSTEM32\SECUR32.DLL
\WINDOWS\SYSTEM32\SERVICES.EXE
\WINDOWS\SYSTEM32\SMSS.EXE
\WINDOWS\SYSTEM32\CTFMON.EXE
\WINDOWS\SYSTEM32\SVCHOST.EXE
\WINDOWS\SYSTEM32\USERINIT.EXE
\WINDOWS\SYSTEM32\USER32.DLL
\WINDOWS\SYSTEM32\WINLOGON.EXE

Приложение 4. 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\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\memtest.exe

Приложение 5. Список файлов ОС Windows 8.1 u3, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»)

Список файлов ОС Windows 8.1 u3 x32, рекомендованный к контролю на аппаратном уровне.

\Windows\explorer.exe
\Windows\system32\audiodg.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\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\kernel32.dll
\Windows\System32\KernelBase.dll
\Windows\System32\LogonUI.exe
\Windows\System32\lsasrv.dll
\Windows\system32\lsass.exe
\Windows\System32\ntdll.dll
\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
<диск с каталогом Boot>\Boot\memtest.exe

Список файлов ОС Windows 8.1 u3 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\wdmaud.drv
\Windows\System32\drivers\ACPI.sys
\Windows\System32\drivers\afd.sys
\Windows\System32\drivers\atapi.sys
\Windows\System32\drivers\ataport.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\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\dwm.exe
\Windows\System32\gdi32.dll
\Windows\System32\hal.dll
\Windows\System32\kernel32.dll
\Windows\System32\KernelBase.dll
\Windows\System32\LogonUI.exe
\Windows\System32\lsasrv.dll
\Windows\System32\lsass.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\memtest.exe

Приложение 6. Список файлов ОС Windows 10, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»)

Список файлов ОС Windows 10 x32, рекомендованный к контролю на аппаратном уровне.

\Windows\explorer.exe
\Windows\system32\audiodg.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\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\kernel32.dll
\Windows\System32\KernelBase.dll
\Windows\System32\LogonUI.exe
\Windows\System32\lsasrv.dll
\Windows\system32\lsass.exe
\Windows\System32\ntdll.dll
\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\taskhostw.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\memtest.exe

Список файлов ОС Windows 10 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\wdmaud.drv
\Windows\System32\drivers\ACPI.sys
\Windows\System32\drivers\afd.sys
\Windows\System32\drivers\atapi.sys
\Windows\System32\drivers\ataport.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\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\dwm.exe
\Windows\System32\gdi32.dll
\Windows\System32\hal.dll
\Windows\System32\kernel32.dll
\Windows\System32\KernelBase.dll
\Windows\System32\LogonUI.exe
\Windows\System32\lsasrv.dll
\Windows\System32\lsass.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\taskhostw.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\memtest.exe

Приложение 7. Список файлов ОС Windows Server 2008 R2, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»)

Файлы ОС, целостность которых рекомендуется контролировать с помощью аппаратного контроллера «Аккорд-АМДЗ»:

\Windows\explorer.exe
\Windows\System32\CLFS.SYS
\Windows\System32\csrsrv.dll
\Windows\System32\gdi32.dll
\Windows\System32\hal.dll
\Windows\System32\kernel32.dll
\Windows\System32\KernelBase.dll
\Windows\System32\lsasrv.dll
\Windows\System32\ntdll.dll
\Windows\System32\ntoskrnl.exe
\Windows\System32\services.exe
\Windows\System32\user32.dll
\Windows\System32\vmms.exe
\Windows\System32\wdmaud.drv
\Windows\System32\win32k.sys
\Windows\System32\Drivers\ACPI.sys
\Windows\System32\Drivers\ataport.SYS
\Windows\System32\Drivers\cdrom.sys
\Windows\System32\Drivers\CLASSPNP.SYS
\Windows\System32\Drivers\cng.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\HDAudBus.sys
\Windows\System32\Drivers\HIDCLASS.SYS
\Windows\System32\Drivers\HIDPARSE.SYS
\Windows\System32\Drivers\HTTP.sys
\Windows\System32\Drivers\hvboot.sys
\Windows\System32\Drivers\i8042prt.sys
\Windows\System32\Drivers\igdkmd64.sys
\Windows\System32\Drivers\intelppm.sys
\Windows\System32\Drivers\iusb3hub.sys
\Windows\System32\Drivers\luafv.sys
\Windows\System32\Drivers\mouclass.sys
\Windows\System32\Drivers\mouhid.sys
\Windows\System32\Drivers\mountmgr.sys
\Windows\System32\Drivers\msahci.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\partmgr.sys
\Windows\System32\Drivers\PCIIDEX.SYS
\Windows\System32\Drivers\portcls.sys
\Windows\System32\Drivers\rdbss.sys
\Windows\System32\Drivers\spsys.sys
\Windows\System32\Drivers\storport.sys
\Windows\System32\Drivers\tcpip.sys
\Windows\System32\Drivers\usbehci.sys
\Windows\System32\Drivers\usbhub.sys
\Windows\System32\Drivers\USBPORT.SYS
\Windows\System32\Drivers\volmgr.sys
\Windows\System32\Drivers\volsnap.sys
\Windows\System32\Drivers\watchdog.sys
\Windows\System32\Drivers\Wdf01000.sys
\Windows\System32\Drivers\wfplwf.sys

Приложение 8. Список файлов ОС Windows Server 2012 R2, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»)

Список файлов ОС Windows Server 2012 R2, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»).

\Windows\explorer.exe
\Windows\system.ini
\Windows\win.ini
\Windows\system32\alg.exe
\Windows\system32\autochk.exe
\Windows\system32\CLFS.SYS
\Windows\system32\cmd.exe
\Windows\system32\csrss.exe
\Windows\system32\dllhost.exe
\Windows\system32\drivers\1394ohci.sys
\Windows\system32\drivers\3ware.sys
\Windows\system32\drivers\ACPI.sys
\Windows\system32\drivers\acpiex.sys
\Windows\system32\drivers\acpipagr.sys
\Windows\system32\drivers\acpipmi.sys
\Windows\system32\drivers\acpitime.sys
\Windows\system32\drivers\adp80xx.sys
\Windows\system32\drivers\afd.sys
\Windows\system32\drivers\agilevpn.sys
\Windows\system32\drivers\AGP440.sys
\Windows\system32\drivers\ahcache.sys
\Windows\system32\drivers\amdk8.sys
\Windows\system32\drivers\amdppm.sys
\Windows\system32\drivers\amdsata.sys
\Windows\system32\drivers\amdsbs.sys
\Windows\system32\drivers\amdxata.sys
\Windows\system32\drivers\appid.sys
\Windows\system32\drivers\arcsas.sys
\Windows\system32\drivers\asyncmac.sys
\Windows\system32\drivers\atapi.sys
\Windows\system32\drivers\BasicDisplay.sys
\Windows\system32\drivers\BasicRender.sys
\Windows\system32\drivers\beep.sys
\Windows\system32\drivers\bfadfcoei.sys
\Windows\system32\drivers\bfadi.sys
\Windows\system32\drivers\bowser.sys
\Windows\system32\drivers\bowser.sys
\Windows\system32\drivers\bridge.sys
\Windows\system32\drivers\bxfcoe.sys
\Windows\system32\drivers\bxois.sys
\Windows\system32\drivers\bxvbda.sys
\Windows\system32\drivers\cdfs.sys
\Windows\system32\drivers\cdrom.sys
\Windows\system32\drivers\cht4vx64.sys

\Windows\system32\drivers\CmBatt.sys
\Windows\system32\drivers\cng.sys
\Windows\system32\drivers\CompositeBus.sys
\Windows\system32\drivers\condrv.sys
\Windows\system32\drivers\dfsc.sys
\Windows\system32\drivers\disk.sys
\Windows\system32\drivers\dmvsc.sys
\Windows\system32\drivers\dxgkrnl.sys
\Windows\system32\drivers\E1G6032E.sys
\Windows\system32\drivers\elxfcoe.sys
\Windows\system32\drivers\elxstor.sys
\Windows\system32\drivers\errdev.sys
\Windows\system32\drivers\evbda.sys
\Windows\system32\drivers\exfat.sys
\Windows\system32\drivers\fastfat.sys
\Windows\system32\drivers\fcvsc.sys
\Windows\system32\drivers\fdc.sys
\Windows\system32\drivers\fileinfo.sys
\Windows\system32\drivers\filetrace.sys
\Windows\system32\drivers\flpydisk.sys
\Windows\system32\drivers\fltmgr.sys
\Windows\system32\drivers\Fs_Rec.sys
\Windows\system32\drivers\fsdepends.sys
\Windows\system32\drivers\fxppm.sys
\Windows\system32\drivers\GAGP30KX.SYS
\Windows\system32\drivers\hdaudbus.sys
\Windows\system32\drivers\hidbatt.sys
\Windows\system32\drivers\hidusb.sys
\Windows\system32\drivers\HpSAMD.sys
\Windows\system32\drivers\http.sys
\Windows\system32\drivers\hwpolicy.sys
\Windows\system32\drivers\hyperkbd.sys
\Windows\system32\drivers\HyperVideo.sys
\Windows\system32\drivers\i8042prt.sys
\Windows\system32\drivers\iaStorAV.sys
\Windows\system32\drivers\iaStorV.sys
\Windows\system32\drivers\ibbus.sys
\Windows\system32\drivers\intelide.sys
\Windows\system32\drivers\intelppm.sys
\Windows\system32\drivers\ipfltdrv.sys
\Windows\system32\drivers\IPMIDrv.sys
\Windows\system32\drivers\ipnat.sys
\Windows\system32\drivers\isapnp.sys
\Windows\system32\drivers\kbdclass.sys
\Windows\system32\drivers\kbdhid.sys
\Windows\system32\drivers\kdnic.sys
\Windows\system32\drivers\ksecdd.sys
\Windows\system32\drivers\ksecpkg.sys
\Windows\system32\drivers\ksthunk.sys
\Windows\system32\drivers\lltdio.sys
\Windows\system32\drivers\lsi_sas.sys
\Windows\system32\drivers\lsi_sas2.sys
\Windows\system32\drivers\lsi_sas3.sys
\Windows\system32\drivers\lsi_sss.sys
\Windows\system32\drivers\luafv.sys

\Windows\system32\drivers\megasas.sys
\Windows\system32\drivers\megasr.sys
\Windows\system32\drivers\mlx4_bus.sys
\Windows\system32\drivers\modem.sys
\Windows\system32\drivers\monitor.sys
\Windows\system32\drivers\mouclass.sys
\Windows\system32\drivers\mouhid.sys
\Windows\system32\drivers\mountmgr.sys
\Windows\system32\drivers\mpsdrv.sys
\Windows\system32\drivers\mrxsmb.sys
\Windows\system32\drivers\mrxsmb10.sys
\Windows\system32\drivers\mrxsmb20.sys
\Windows\system32\drivers\msfs.sys
\Windows\system32\drivers\msgpioclx.sys
\Windows\system32\drivers\mshidkmdf.sys
\Windows\system32\drivers\mshidumdf.sys
\Windows\system32\drivers\msisadrv.sys
\Windows\system32\drivers\msiscsi.sys
\Windows\system32\drivers\mskssrv.sys
\Windows\system32\drivers\MsLbfoProvider.sys
\Windows\system32\drivers\mspclock.sys
\Windows\system32\drivers\mspqm.sys
\Windows\system32\drivers\msrpc.sys
\Windows\system32\drivers\mssmbios.sys
\Windows\system32\drivers\mstee.sys
\Windows\system32\drivers\MTConfig.sys
\Windows\system32\drivers\mup.sys
\Windows\system32\drivers\mvumis.sys
\Windows\system32\drivers\ndfltr.sys
\Windows\system32\drivers\NDIS.SYS
\Windows\system32\drivers\ndiscap.sys
\Windows\system32\drivers\NdisImPlatform.sys
\Windows\system32\drivers\ndistapi.sys
\Windows\system32\drivers\ndisuio.sys
\Windows\system32\drivers\NdisVirtualBus.sys
\Windows\system32\drivers\ndiswan.sys
\Windows\system32\drivers\ndproxy.sys
\Windows\system32\drivers\netbios.sys
\Windows\system32\drivers\netbt.sys
\Windows\system32\drivers\netvsc63.sys
\Windows\system32\drivers\npfs.sys
\Windows\system32\drivers\npsvctrig.sys
\Windows\system32\drivers\nsiproxy.sys
\Windows\system32\drivers\Ntfs.sys
\Windows\system32\drivers\null.sys
\Windows\system32\drivers\NV_AGP.SYS
\Windows\system32\drivers\nvraid.sys
\Windows\system32\drivers\nvstor.sys
\Windows\system32\drivers\pacer.sys
\Windows\system32\drivers\parport.sys
\Windows\system32\drivers\partmgr.sys
\Windows\system32\drivers\pci.sys
\Windows\system32\drivers\pciide.sys
\Windows\system32\drivers\pcmcia.sys
\Windows\system32\drivers\pcw.sys

\Windows\system32\drivers\pdc.sys
\Windows\system32\drivers\PEAuth.sys
\Windows\system32\drivers\processr.sys
\Windows\system32\drivers\ql2300i.sys
\Windows\system32\drivers\ql40xx2i.sys
\Windows\system32\drivers\qlfcoei.sys
\Windows\system32\drivers\rasacd.sys
\Windows\system32\drivers\rasl2tp.sys
\Windows\system32\drivers\raspppoe.sys
\Windows\system32\drivers\raspptp.sys
\Windows\system32\drivers\rassstp.sys
\Windows\system32\drivers\rdbss.sys
\Windows\system32\drivers\rdpbus.sys
\Windows\system32\drivers\rdpdr.sys
\Windows\system32\drivers\rdpvideominiport.sys
\Windows\system32\drivers\refs.sys
\Windows\system32\drivers\rspndr.sys
\Windows\system32\drivers\sacdrv.sys
\Windows\system32\drivers\sbp2port.sys
\Windows\system32\drivers\scfilter.sys
\Windows\system32\drivers\sdbus.sys
\Windows\system32\drivers\sdstor.sys
\Windows\system32\drivers\secdrv.sys
\Windows\system32\drivers\SerCx.sys
\Windows\system32\drivers\SerCx2.sys
\Windows\system32\drivers\serenum.sys
\Windows\system32\drivers\serial.sys
\Windows\system32\drivers\sermouse.sys
\Windows\system32\drivers\sfloppy.sys
\Windows\system32\drivers\sisraid2.sys
\Windows\system32\drivers\sisraid4.sys
\Windows\system32\drivers\smbdirect.sys
\Windows\system32\drivers\spaceport.sys
\Windows\system32\drivers\SpbCx.sys
\Windows\system32\drivers\srv.sys
\Windows\system32\drivers\srv2.sys
\Windows\system32\drivers\srvnet.sys
\Windows\system32\drivers\stexstor.sys
\Windows\system32\drivers\storahci.sys
\Windows\system32\drivers\stornvme.sys
\Windows\system32\drivers\storvsc.sys
\Windows\system32\drivers\storvsp.sys
\Windows\system32\drivers\swenum.sys
\Windows\system32\drivers\tcpip.sys
\Windows\system32\drivers\tcpipreg.sys
\Windows\system32\drivers\tdx.sys
\Windows\system32\drivers\terminpt.sys
\Windows\system32\drivers\tpm.sys
\Windows\system32\drivers\TsUsbFlt.sys
\Windows\system32\drivers\TsUsbGD.sys
\Windows\system32\drivers\tsusbhub.sys
\Windows\system32\drivers\tunnel.sys
\Windows\system32\drivers\UAGP35.SYS
\Windows\system32\drivers\uaspstor.sys
\Windows\system32\drivers\UCX01000.SYS

\Windows\system32\drivers\udfs.sys
\Windows\system32\drivers\uefi.sys
\Windows\system32\drivers\ULIAGPKX.SYS
\Windows\system32\drivers\umbus.sys
\Windows\system32\drivers\umpass.sys
\Windows\system32\drivers\usbccgp.sys
\Windows\system32\drivers\usbehci.sys
\Windows\system32\drivers\usbhub.sys
\Windows\system32\drivers\USBHUB3.SYS
\Windows\system32\drivers\usbohci.sys
\Windows\system32\drivers\usbprint.sys
\Windows\system32\drivers\USBSTOR.SYS
\Windows\system32\drivers\usbuhci.sys
\Windows\system32\drivers\USBXHCI.SYS
\Windows\system32\drivers\vdrvroot.sys
\Windows\system32\drivers\VerifierExt.sys
\Windows\system32\drivers\vhdmp.sys
\Windows\system32\drivers\viaide.sys
\Windows\system32\drivers\Vid.sys
\Windows\system32\drivers\volmgr.sys
\Windows\system32\drivers\volmgrx.sys
\Windows\system32\drivers\volsnap.sys
\Windows\system32\drivers\vpci.sys
\Windows\system32\drivers\vpcivsp.sys
\Windows\system32\drivers\vsmraid.sys
\Windows\system32\drivers\VSTXRAID.SYS
\Windows\system32\drivers\wacompen.sys
\Windows\system32\drivers\Wdf01000.sys
\Windows\system32\drivers\wfplwfs.sys
\Windows\system32\drivers\wimmount.sys
\Windows\system32\drivers\winmad.sys
\Windows\system32\drivers\winnat.sys
\Windows\system32\drivers\winverbs.sys
\Windows\system32\drivers\wmiacpi.sys
\Windows\system32\drivers\ws2ifsl.sys
\Windows\system32\drivers\wtlmdrv.sys
\Windows\system32\drivers\WUDFPf.sys
\Windows\system32\ieetwcollector.exe
\Windows\system32\Locator.exe
\Windows\system32\LogonUI.exe
\Windows\system32\lsass.exe
\Windows\system32\mmc.exe
\Windows\system32\msdtc.exe
\Windows\system32\msiexec.exe
\Windows\system32\ntoskrnl.exe
\Windows\system32\rsopprov.exe
\Windows\system32\rundll32.exe
\Windows\system32\smss.exe
\Windows\system32\snmptrap.exe
\Windows\system32\spoolsv.exe
\Windows\system32\sppsvc.exe
\Windows\system32\svchost.exe
\Windows\system32\Taskmgr.exe
\Windows\system32\TieringEngineService.exe

\Windows\system32\UI0Detect.exe
\Windows\system32\userinit.exe
\Windows\system32\vds.exe
\Windows\system32\VSSVC.exe
\Windows\system32\wbem\WmiApSrv.exe
\Windows\system32\win32k.sys
\Windows\system32\winload.exe
\Windows\system32\winlogon.exe
\Windows\system32\winresume.exe
\Windows\system32\winspool.drv

Приложение 9.
Список файлов СПО «ПИ ШИПКА» для ОС Windows, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»)

Список файлов СПО «ПИ ШИПКА» для 32х битных ОС Windows, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «Аккорд-АМДЗ»).

\WINDOWS\SYSTEM32\OSCIAPI.dll

Список файлов СПО «ПИ ШИПКА» для 64х битных ОС Windows, рекомендуемых для контроля целостности на аппаратном уровне при установке комплекса СЗИ НСД «АККОРД – Win64».

\WINDOWS\SYSTEM32\OSCIAPI.dll
\WINDOWS\SYSTEM32\syswow64\OSCIAPI.dll

Приложение 10.
Стандартный шаблон icl_WindowsXPx32.xml

Список файлов ОС Windows XP x32 для контроля целостности на аппаратном уровне.

NTLDR
NTDETCT.COM
BOOT.INI
WINDOWS/SYSTEM32/ACGINA.DLL
WINDOWS/SYSTEM32/ACRUNNT.EXE
WINDOWS/SYSTEM32/AZIAHLP.DLL
WINDOWS/SYSTEM32/CSRSS.EXE
WINDOWS/SYSTEM32/HAL.DLL
WINDOWS/SYSTEM32/KERNEL32.DLL
WINDOWS/SYSTEM32/LSASRV.DLL
WINDOWS/SYSTEM32/LSASS.EXE
WINDOWS/SYSTEM32/NTDLL.DLL
WINDOWS/SYSTEM32/NTOSKRNL.EXE
WINDOWS/SYSTEM32/PSAPI.DLL
WINDOWS/SYSTEM32/REGAPI.DLL
WINDOWS/SYSTEM32/RUNDLL32.DLL
WINDOWS/SYSTEM32/SECUR32.DLL
WINDOWS/SYSTEM32/SERVICES.EXE
WINDOWS/SYSTEM32/SMSS.EXE
WINDOWS/SYSTEM32/CTFMON.EXE
WINDOWS/SYSTEM32/SVCHOST.EXE
WINDOWS/SYSTEM32/TMATTACH.DLL
WINDOWS/SYSTEM32/TMDRV32.DLL
WINDOWS/SYSTEM32/USERINIT.EXE
WINDOWS/SYSTEM32/USER32.DLL
WINDOWS/SYSTEM32/WINLOGON.EXE

Приложение 11.
Стандартный шаблон icl_WindowsXPx64.xml

Список файлов ОС Windows XP x64 для контроля целостности на аппаратном уровне.

NTLDR
NTDETCT.COM
BOOT.INI
WINDOWS/SYSTEM32/ACGINA.DLL
WINDOWS/SYSTEM32/ACRUNNT.EXE
WINDOWS/SYSTEM32/AZIAHLP.DLL
WINDOWS/SYSTEM32/CSRSS.EXE
WINDOWS/SYSTEM32/HAL.DLL
WINDOWS/SYSTEM32/KERNEL32.DLL
WINDOWS/SYSTEM32/LSASRV.DLL
WINDOWS/SYSTEM32/LSASS.EXE
WINDOWS/SYSTEM32/NTDLL.DLL
WINDOWS/SYSTEM32/NTOSKRNL.EXE
WINDOWS/SYSTEM32/PSAPI.DLL
WINDOWS/SYSTEM32/REGAPI.DLL
WINDOWS/SYSTEM32/RUNDLL32.DLL
WINDOWS/SYSTEM32/SECUR32.DLL
WINDOWS/SYSTEM32/SERVICES.EXE
WINDOWS/SYSTEM32/SMSS.EXE
WINDOWS/SYSTEM32/CTFMON.EXE
WINDOWS/SYSTEM32/SVCHOST.EXE
WINDOWS/SYSTEM32/TMATTACH.DLL
WINDOWS/SYSTEM32/TMDRV32.DLL
WINDOWS/SYSTEM32/TMDRV64.DLL
WINDOWS/SYSTEM32/USERINIT.EXE
WINDOWS/SYSTEM32/USER32.DLL
WINDOWS/SYSTEM32/WINLOGON.EXE

Приложение 12.
Стандартный шаблон icl_Windows7x32.xml

Список файлов ОС Windows 7 x32 для контроля целостности 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
WINDOWS/SYSTEM32/ACCORD.SCR
WINDOWS/SYSTEM32/ACGINA.DLL
WINDOWS/SYSTEM32/ACRUNNT.EXE
WINDOWS/SYSTEM32/ACRUNVDD.DLL
WINDOWS/SYSTEM32/ACRUNVDD.EXE
WINDOWS/SYSTEM32/ACUSRMOD.DLL
WINDOWS/SYSTEM32/AZIAHLP.DLL
WINDOWS/SYSTEM32/DRIVERS/ACBOOT.SYS
WINDOWS/SYSTEM32/DRIVERS/ACLOCK2K.SYS
WINDOWS/SYSTEM32/DRIVERS/ACRUN.SYS
WINDOWS/SYSTEM32/DRIVERS/ACXALLOW.SYS

WINDOWS/SYSTEM32/DRIVERS/ACXLMSRV.SYS
WINDOWS/SYSTEM32/PSAPI.DLL
WINDOWS/SYSTEM32/TMATTACH.DLL
WINDOWS/SYSTEM32/TMDRV32.DLL

Приложение 13. Стандартный шаблон icl_Windows7x32_bootdisk.xml

Список файлов загрузочного диска ОС Windows 7 x32 для контроля целостности на аппаратном уровне.

Boot/BOOTSTAT.DAT
Boot/memtest.exe

Приложение 14. Стандартный шаблон icl_Windows7x64.xml

Список файлов ОС Windows 7 x64 для контроля целостности 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
ACCORD.X64/ACCORD.INI
ACCORD.X64/ACTSKMNG.EXE
ACCORD.X64/ACTSKMNG.INI

ACCORD.X64/ACUSRM64.DLL
ACCORD.X64/ACUSRMOD.DLL
ACCORD.X64/PSAPI.DLL
WINDOWS/SYSTEM32/ACCORD.SCR
WINDOWS/SYSTEM32/ACGINA.DLL
WINDOWS/SYSTEM32/ACRUNNT.EXE
WINDOWS/SYSTEM32/ACUSRM64.DLL
WINDOWS/SYSTEM32/AZIAH64.DLL
WINDOWS/SYSTEM32/DRIVERS/ACBOOT.SYS
WINDOWS/SYSTEM32/DRIVERS/ACLOCK2K.SYS
WINDOWS/SYSTEM32/DRIVERS/ACRUN.SYS
WINDOWS/SYSTEM32/DRIVERS/ACXLMSRV.SYS
WINDOWS/SYSTEM32/TMATT64.DLL
WINDOWS/SYSTEM32/TMDRV64.DLL
WINDOWS/SYSWOW64/ACUSRMOD.DLL
WINDOWS/SYSWOW64/AZIAHLP.DLL
WINDOWS/SYSWOW64/TMATTACH.DLL
WINDOWS/SYSWOW64/TMDRV32.DLL

Приложение 15.
Стандартный шаблон icl_Windows7x64_bootdisk.xml

Список файлов загрузочного диска ОС Windows 7 x64 для контроля целостности на аппаратном уровне.

Boot/memtest.exe

Приложение 16. Стандартный шаблон icl_WindowsServer2008R2x64.xml

Список файлов ОС Windows Server 2008 R2 x64 для контроля целостности на аппаратном уровне.

Windows/explorer.exe
Windows/System32/CLFS.SYS
Windows/System32/csrsrv.dll
Windows/System32/gdi32.dll
Windows/System32/hal.dll
Windows/System32/kernel32.dll
Windows/System32/KernelBase.dll
Windows/System32/lsasrv.dll
Windows/System32/ntdll.dll
Windows/System32/ntoskrnl.exe
Windows/System32/services.exe
Windows/System32/user32.dll
Windows/System32/vmms.exe
Windows/System32/wdmaud.drv
Windows/System32/win32k.sys
Windows/System32/Drivers/ACPI.sys
Windows/System32/Drivers/ataport.SYS
Windows/System32/Drivers/cdrom.sys
Windows/System32/Drivers/CLASSPNP.SYS
Windows/System32/Drivers/cng.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/HDAudBus.sys
Windows/System32/Drivers/HIDCLASS.SYS
Windows/System32/Drivers/HIDPARSE.SYS
Windows/System32/Drivers/HTTP.sys
Windows/System32/Drivers/hvboot.sys
Windows/System32/Drivers/i8042prt.sys
Windows/System32/Drivers/igdkmd64.sys
Windows/System32/Drivers/intelppm.sys
Windows/System32/Drivers/iusb3hub.sys
Windows/System32/Drivers/luafv.sys
Windows/System32/Drivers/mouclass.sys
Windows/System32/Drivers/mouhid.sys
Windows/System32/Drivers/mountmgr.sys

Windows/System32/Drivers/msahci.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/partmgr.sys
Windows/System32/Drivers/PCIIDEX.SYS
Windows/System32/Drivers/portcls.sys
Windows/System32/Drivers/rdbss.sys
Windows/System32/Drivers/spsys.sys
Windows/System32/Drivers/storport.sys
Windows/System32/Drivers/tcpip.sys
Windows/System32/Drivers/usbehci.sys
Windows/System32/Drivers/usbhub.sys
Windows/System32/Drivers/USBPORT.SYS
Windows/System32/Drivers/volmgr.sys
Windows/System32/Drivers/volsnap.sys
Windows/System32/Drivers/watchdog.sys
Windows/System32/Drivers/Wdf01000.sys
Windows/System32/Drivers/wfplwf.sys
Accord.x64/AcBoot.sys
Accord.x64/AcChgPas.exe
Accord.x64/Accord.dat
Accord.x64/Accord.ini
Accord.x64/Accord.scr
Accord.x64/Aced32.exe
Accord.x64/AcEd32n.hlp
Accord.x64/Acgina.dll
Accord.x64/AcLock2k.sys
Accord.x64/AcPrnCfg.exe
Accord.x64/AcProc.exe
Accord.x64/acrun.sys
Accord.x64/AcRunNT.exe
Accord.x64/AcRunTI.exe
Accord.x64/AcSetup.exe
Accord.x64/AcSync.exe
Accord.x64/AcTskMng.exe
Accord.x64/AcTskMng.ini
Accord.x64/AcTskMng64.dll
Accord.x64/AcUsrM64.dll
Accord.x64/AcUsrMod.dll
Accord.x64/AcWs32.prd

Accord.x64/AcXLmSrv.sys
Accord.x64/AmzToNT.dll
Accord.x64/aziah64.dll
Accord.x64/AzIaHlp.dll
Accord.x64/azlog.dll
Accord.x64/CSTm64.dll
Accord.x64/CSTMDrv.dll
Accord.x64/Eds32.dll
Accord.x64/EDS64.dll
Accord.x64/KeyToTm.exe
Accord.x64/LogBase.exe
Accord.x64/Logtoprd.exe
Accord.x64/LogView.exe
Accord.x64/MakePrc.exe
Accord.x64/Psapi.dll
Accord.x64/RdpTm64.dll
Accord.x64/RdpTmDrv.dll
Accord.x64/ReadPrd.exe
Accord.x64/System32.hsh
Accord.x64/Test.act
Accord.x64/TmAtt64.dll
Accord.x64/TmAttach.dll
Accord.x64/tmdrv32.dll
Accord.x64/TmDrv32_1.dll
Accord.x64/TmDrv64.dll
Accord.x64/TmDrv64_1.dll
Accord.x64/TmExp64.exe
Accord.x64/tmexplor.exe
Accord.x64/UsrToAz.dll
Accord.x64/VcTm64.dll
Accord.x64/VCTmDrv.dll
Accord.x64/Identifiers/AcIdCfg.exe
Accord.x64/Identifiers/Cards/TmDrv32.dll
Accord.x64/Identifiers/Cards/TmDrv64.dll
Accord.x64/Identifiers/Cards_New/TmDrv32.dll
Accord.x64/Identifiers/Cards_New/TmDrv64.dll
Accord.x64/Identifiers/eToken/TmDrv32.dll
Accord.x64/Identifiers/eToken/TmDrv64.dll
Accord.x64/Identifiers/Shipka/TmDrv32.dll
Accord.x64/Identifiers/Shipka/TmDrv64.dll
Accord.x64/Identifiers/TM/TmDrv32.dll
Accord.x64/Identifiers/TM/TmDrv64.dll
Accord.x64/Identifiers/TM-USB/tmdrv32.dll
Accord.x64/Identifiers/TM-USB/TmDrv64.dll

Accord.x64/Identifiers/Virtual/TmDrv32.dll
Accord.x64/Identifiers/Virtual/TmDrv64.dll
Accord.x64/ScreenSaver/String/Accord.scr
Accord.x64/VISTA/AcGina.dll
Accord.x64/VISTA/cp.reg

Приложение 17.
Описание формирования пользователем шаблона СКЦ

При необходимости формирования шаблона с произвольным списком контролируемых файлов пользователь должен учитывать следующие моменты:

1. Файл шаблона имеет расширение .xml
2. Начинается файл с открывающего тэга
   <request type="import" formatversion="0.1">
   и заканчивается закрывающим тэгом
   </request>
3. Каждый файл описывается внутри пары тэгов <file> (открывающий) и </file> (закрывающий)
4. Путь к файлу указывается внутри пары тэгов <path> (открывающий) и </path> (закрывающий)
5. После указания пути к файлу следуют флаги контроля, описанные в виде тэга <flags controldata="1" controlattrs="1" /> Флаг controldata отвечает за контроль содержимого файла и при необходимости его контроля имеет значение «1» Флаг controlattrs отвечает за контроль атрибутов файла и при необходимости их контроля имеет значение «1»

Пример шаблона файла .xml
(контролируемые файлы Windows/Explorer.exe и Windows/System32/audiodg.exe)

```
<request type="import" formatversion="0.1">
	<file>
		<path>
			Windows/Explorer.exe
		</path>
			<flags controldata="1" controlattrs="1" />
	</file>
	<file>
		<path>
			Windows/System32/audiodg.exe
		</path>
			<flags controldata="1" controlattrs="1" />
	</file>
</request>
```

Приложение 18. Сценарии загрузки СВТ с установленным «Аккорд-АМДЗ» со специально подготовленного USB-носителя

I. Продолжение загрузки для clonzilla

Пошаговая инструкция:

1. Скачать образ clonzilla.

2. На USB-носителе, который предполагается сделать загрузочным, создать раздел нужного размера (см. размер образа ОС), отформатированный в FAT32.

3. Скачать с официального сайта утилиту unetbootin (файл unetbootin-linux-625.bin).

4. Задать текущему пользователю права на исполнение файла с утилитой.

5. Запустить утилиту.

6. Выбрать нужный образ и нужный USB-носитель в соответствующих меню. Записать образ на USB-носитель.

7. Монтировать USB-носитель.

8. Создать в корневом каталоге USB-носителя файл с именем ACCORD_BOOT_PARAMS.

9. Вновь созданный файл должен содержать три строки:

а) путь до ядра Linux;

б) путь до Initrd;

в) список параметров командной строки в кавычках.

Указанную информацию можно получить из файла syslinux.cfg, находящегося на USB-носителе. Если в этом файле существует несколько вариантов конфигурации загрузки, следует выбрать из них необходимый.

Пример:

в файле syslinux.cfg указана следующая информация:

```
label unetbootindefault
menu label Default
kernel /ubnkern
append initrd=/ubninit vga=788 --- quiet
```

Следовательно, в файл ACCORD_BOOT_PARAMS следует записать:

```
/ubnkern
/ubninit
"vga=788 --- quiet"
```

10. Размонтировать каталог монтирования.

11. Выполнить перезагрузку. Загрузочный USB-носитель должен быть вставлен в компьютер, «Аккорд-АМДЗ» должен находиться в рабочем режиме.

12. После прохождения процедуры идентификации/аутентификации и контроля целостности в окне приветствия администратора следует нажать кнопку <Продолжить загрузку>.

13. В появившемся далее окне следует выбрать указанный выше USB-носитель в категории «Другое загрузочное устройство».

14. Готово!

II. Установка ОС Linux (например, Debian8)

Пошаговая инструкция:

1. Скачать образ ОС Linux.

2. На USB-носителе, который предполагается сделать загрузочным, создать раздел нужного размера (см. размер образа ОС), отформатированный в FAT32.

3. Скачать с официального сайта утилиту unetbootin (файл unetbootin-linux-625.bin).

4. Задать текущему пользователю права на исполнение файла с утилитой.

5. Запустить утилиту.

6. Выбрать нужный образ и нужный USB-носитель в соответствующих меню. Записать образ на USB-носитель.

7. Монтировать USB-носитель.

8. Создать в корневом каталоге USB-носителя файл с именем ACCORD_BOOT_PARAMS.

9. Вновь созданный файл должен содержать три строки:

а) путь до ядра Linux;

б) путь до Initrd;

в) список параметров командной строки в кавычках.

Указанную информацию можно получить из файла syslinux.cfg, находящегося на USB-носителе. Если в этом файле существует несколько вариантов конфигурации загрузки, следует выбрать из них необходимый.

Пример: в файле syslinux.cfg указана следующая информация:

```
label unetbootindefault
menu label Default
kernel /ubnkern
append initrd=/ubninit vga=788 --- quiet
```

Следовательно, в файл ACCORD_BOOT_PARAMS следует записать:

```
/ubnkern
/ubninit
"vga=788 --- quiet"
```

10. Размонтировать каталог монтирования.

11. Выполнить перезагрузку. Загрузочный USB-носитель должен быть вставлен в компьютер, «Аккорд-АМДЗ» должен находиться в рабочем режиме.

12. После прохождения процедуры идентификации/аутентификации и контроля целостности в окне приветствия администратора следует нажать кнопку <Продолжить загрузку>.

13. В появившемся далее окне следует выбрать указанный выше USB-носитель в категории «Другое загрузочное устройство».

14. Выполнить установку ОС в соответствии с инструкциями мастера установки Linux.

15. Готово!

III. Загрузка с live-CD (например, Xubuntu)

Пошаговая инструкция:

1. Скачать образ live-CD.

2. На USB-носителе, который предполагается сделать загрузочным, создать раздел нужного размера (см. размер образа ОС), отформатированный в FAT32.

3. Скачать с официального сайта утилиту unetbootin (файл unetbootin-linux-625.bin).

4. Задать текущему пользователю права на исполнение файла с утилитой.

5. Запустить утилиту.

6. Выбрать нужный образ и нужный USB-носитель в соответствующих меню. Записать образ на USB-носитель.

7. Монтировать USB-носитель.

8. Создать в корневом каталоге USB-носителя файл с именем ACCORD_BOOT_PARAMS.

9. Вновь созданный файл должен содержать три строки:

а) путь до ядра Linux;

б) путь до Initrd;

в) список параметров командной строки в кавычках.

Указанную информацию можно получить из файла syslinux.cfg, находящегося на USB-носителе. Если в этом файле существует несколько вариантов конфигурации загрузки, следует выбрать из них необходимый.

Пример: в файле syslinux.cfg указана следующая информация:

```
label unetbootindefault
menu label Default
kernel /ubnkern
append initrd=/ubninit vga=788 --- quiet
```

Следовательно, в файл ACCORD_BOOT_PARAMS следует записать:

```
/ubnkern
/ubninit
"vga=788 --- quiet"
```

10. Размонтировать каталог монтирования.

11. Выполнить перезагрузку. Загрузочный USB-носитель должен быть вставлен в компьютер, «Аккорд-АМДЗ» должен находиться в рабочем режиме.

12. После прохождения процедуры идентификации/аутентификации и контроля целостности в окне приветствия администратора следует нажать кнопку <Продолжить загрузку>.

13. В появившемся далее окне следует выбрать указанный выше USB-носитель в категории «Другое загрузочное устройство».

14. Готово!

IV. Проверка на вирусы (при помощи DrWeb LiveDisk)

Пошаговая инструкция:

1. Скачать антивирусную программу, поддерживающую запуск с live-CD. Например, DrWeb LiveDisk.

2. На USB-носителе, который предполагается сделать загрузочным, создать раздел нужного размера (см. размер образа ОС), отформатированный в FAT32.

3. Скачать с официального сайта утилиту unetbootin (файл unetbootin-linux-625.bin).

4. Задать текущему пользователю права на исполнение файла с утилитой.

5. Запустить утилиту.

6. Выбрать нужный образ и нужный USB-носитель в соответствующих меню. Записать образ на USB-носитель.

7. Монтировать USB-носитель.

8. Создать в корневом каталоге USB-носителя файл с именем ACCORD_BOOT_PARAMS.

9. Вновь созданный файл должен содержать три строки:

а) путь до ядра Linux;

б) путь до Initrd;

в) список параметров командной строки в кавычках.

Указанную информацию можно получить из файла syslinux.cfg (в данном случае необходимая информация содержалась в файле txt.cfg, на который ссылался файл syslinux.cfg), находящегося на USB-носителе. Если в этом файле существует несколько вариантов конфигурации загрузки, следует выбрать из них необходимый.

Пример: в файле syslinux.cfg указана следующая информация:

```
label unetbootindefault
menu label Default
kernel /ubnkernappend initrd=/ubninit vga=788 --- quiet
```

Следовательно, в файл ACCORD_BOOT_PARAMS следует должны записать:

```
/ubnkern
/ubninit
"vga=788 --- quiet"
```

10. Размонтировать каталог монтирования.

11. Выполнить перезагрузку. Загрузочный USB-носитель должен быть вставлен в компьютер, «Аккорд-АМДЗ» должен находиться в рабочем режиме.

12. После прохождения процедуры идентификации/аутентификации и контроля целостности в окне приветствия администратора следует нажать кнопку <Продолжить загрузку>.

13. В появившемся далее окне следует выбрать указанный выше USB-носитель в категории «Другое загрузочное устройство».

14. Готово!

Приложение 19. Описание механизма авторизации в СЗИ НСД «Аккорд-АМДЗ», поддерживающем режим загрузки BIOS UEFI

«Аккорд-АМДЗ» поддерживает режим загрузки UEFI-систем без использования опции совместимости CSM, но при работе в BIOS UEFI надо учитывать некоторые особенности, изложенные ниже.

Особенности настройки ПК

1. Необходима версия BIOS на английском языке.
2. Необходимо выключить режим «безопасной загрузки» ОС в BIOS:

   `Secure Boot>`**`disable`**
3. Режим работы ОС в BIOS необходимо установить в «Другие ОС» (Other OS):

   `Boot>Secure boot menu>OS type>`**`Other OS`**

Особенности аутентификации в «Аккорд-АМДЗ», поддерживающем режим загрузки BIOS UEFI

Работа с «Аккорд-АМДЗ», поддерживающим режим загрузки UEFI, имеет следующие особенности аутентификации:

1. Администраторы выполняют процедуру аутентификации дважды: в текстовом интерфейсе (рисунок 41) и, после успешного выполнения аутентификации, повторно – в графическом интерфейсе (рисунок 44).
2. Администраторы не имеют возможности продолжить загрузку компьютера. После отработки среды администрирования «Аккорд-АМДЗ» компьютер перезагружается.
3. Пользователи выполняют процедуру аутентификации только в текстовом интерфейсе (рисунок 41). При успешном выполнении процедуры аутентификации автоматически продолжается загрузка в ОС (рисунок 42).

Начало работы

Работа контроллера начинается с инициализации устройства и регистрации пользователя «Гл. Администратор» (супервизора). Для этого необходимо:

1. Предъявить идентификатор при запросе и ввести любой пароль (в дальнейшей работе эти данные не будут использоваться).

Рисунок 41 - Текстовый интерфейс UEFI АМДЗ (ввод пароля не отображается)

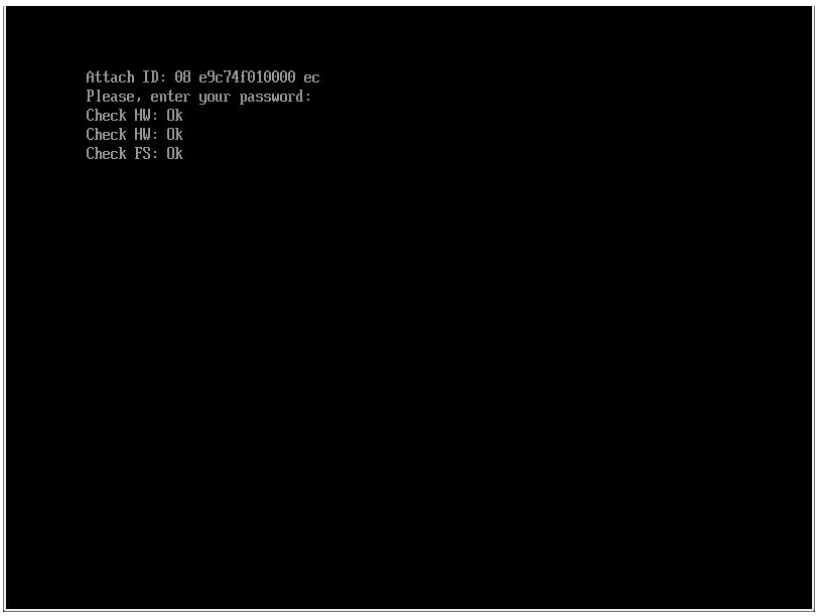

Рисунок 42 - Успешный логин пользователя

2. Дождаться старта среды администрирования, который сопровождается сообщением о необходимости зарегистрировать пользователя «Гл. Администратор» (рисунок 43), и нажать кнопку <OK>.

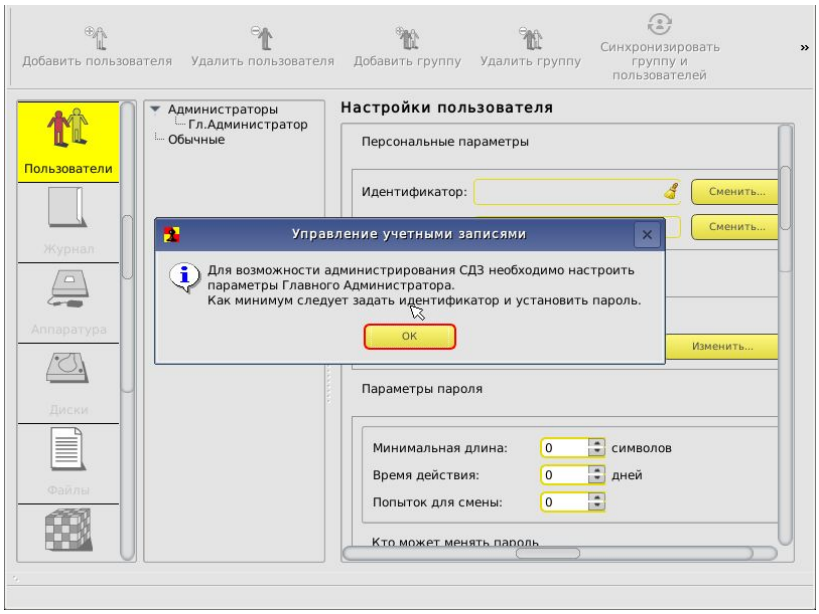

Рисунок 43 - Старт среды администрирования

3. Выбрать пользователя «Гл. Администратор» задать для его учетной записи необходимые параметры, назначить идентификатор и пароль (рисунок 44), после чего применить настройки (в случае необходимости создать группы, пользователей и настроить параметры их учетных записей, назначить идентификаторы и пароли).

4. Приступить к настройке КЦ файлов и аппаратуры (по необходимости, в соответствии с внутренними регламентами безопасности, принятыми в организации).

5. По окончании настройки осуществить выход из среды администрирования и выполнить перезагрузку компьютера.

Важно: В случае предъявления незарегистрированного идентификатора/неверного пароля происходит перезагрузка компьютера.

Важно: Продолжение загрузки в ОС возможно только пользователями, не состоящими в группе «Администраторы». Пользователи из группы «Администраторы» имеют возможность работать только в среде администрирования АМДЗ.

Важно: Возможен ввод идентификатора с клавиатуры. Для обеспечения этой возможности при назначении идентификатора в графическом режиме поле ввода выбирается курсором, с клавиатуры вводится комбинация букв и цифр, нажимается кнопка «Enter». После этого введенное значение преобразуется в 16-ричный номер ключа. В дальнейшем для получения доступа в текстовом интерфейсе в строке ввода идентификатора следует набирать ту же комбинацию.

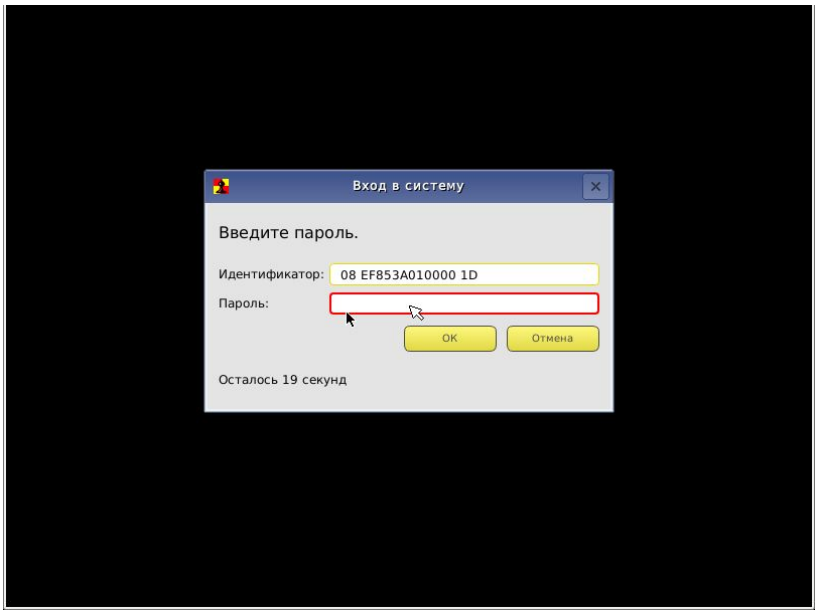

Рисунок 44 - Идентификация администратора в графическом интерфейсе

Контроль целостности оборудования и файлов

1. Установка файлов (рисунок 45) и аппаратуры (рисунок 46) на КЦ выполняется штатно.

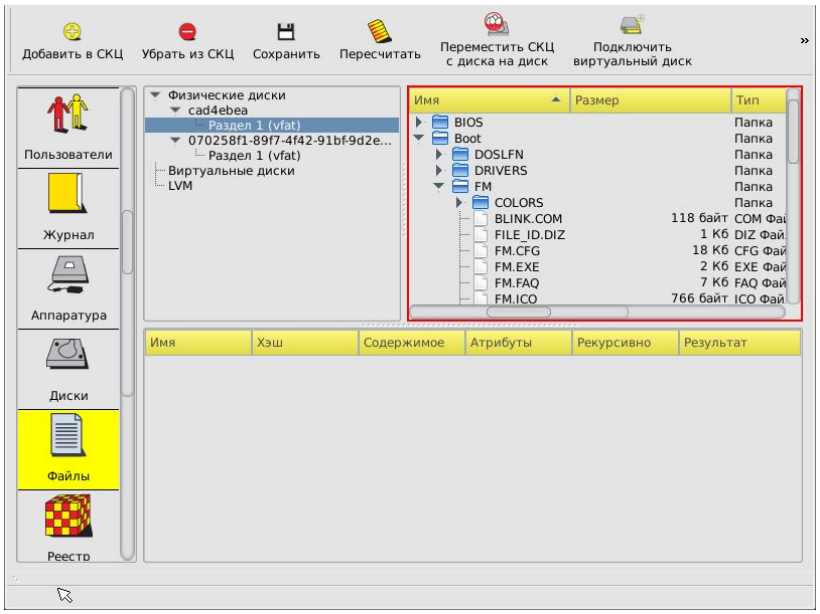

Рисунок 45 - Список дисков и файлов

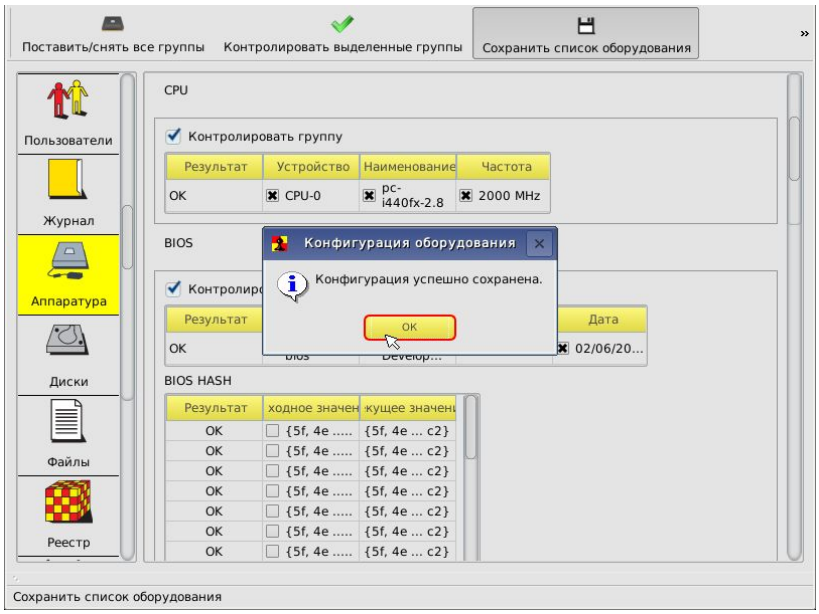

Рисунок 46 - Установка на контроль аппаратуры и сохранение конфигурации

2. В случае отсутствия нарушений КЦ, в окне приветствия администратора выдается сообщение об успешном выполнении процедур контроля (рисунок 47).

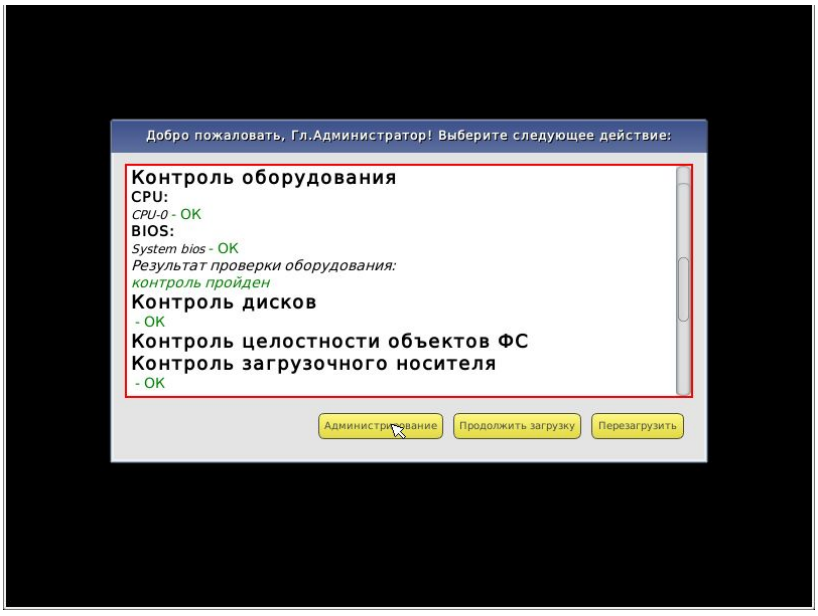

Рисунок 47 - КЦ без нарушений

3. При логине пользователя с нарушением КЦ файлов и/или аппаратуры выдается сообщение о первом непрошедшем контроль элементе из всего списка (рисунок 48). После чего выполняется перезагрузка компьютера.

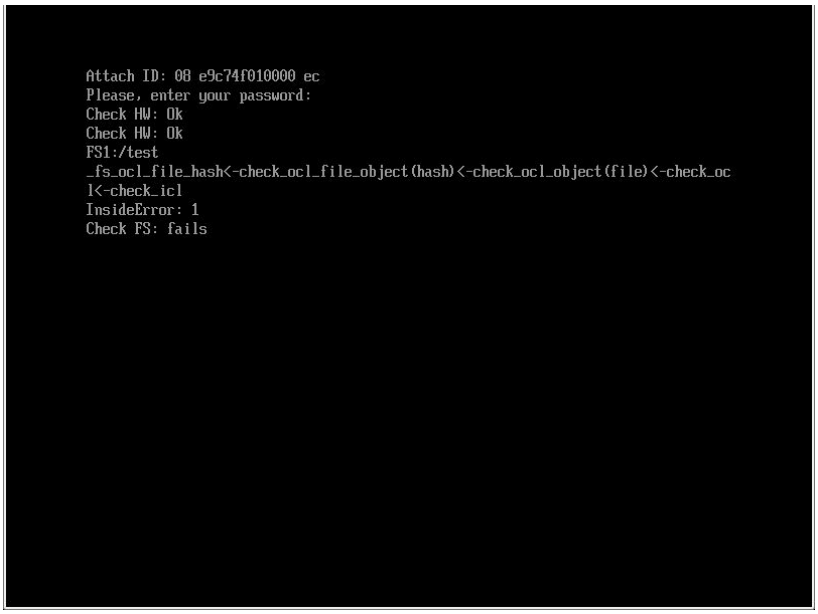

Рисунок 48 - Нарушение КЦ файлов

4. Для мониторинга и исправления ошибок необходимо выполнить аутентификацию в среде администрирования под учетной записью администратора. Будет получена ошибка, но начнется загрузка среды администрирования с выводом полного списка КЦ с указанием элементов, не прошедших контроль (рисунок 49).

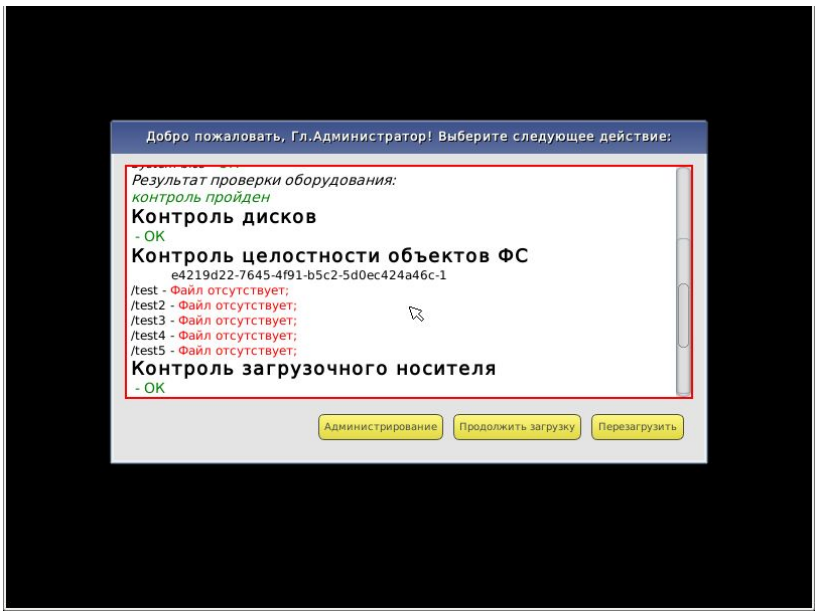

Рисунок 49 - Полный список файлов, не прошедших КЦ