ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «ИНАФ»

Руководство администратора

11443195.4012.046 90

Листов 61

Москва

2022

АННОТАЦИЯ

Настоящий документ является руководством администратора программно-аппаратного комплекса средств защиты информации от несанкционированного доступа «ИНАФ» (далее по тексту – «ИНАФ», комплекс, ПАК «ИНАФ», ПАК СЗИ НСД), являющегося средством доверенной загрузки.

В документе приведены основные функции и особенности эксплуатации ПАК «ИНАФ».

Перед установкой и эксплуатацией ПАК «ИНАФ» необходимо внимательно ознакомиться с комплектом эксплуатационной документации на комплекс, а также принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных средств комплекса должно дополняться общими мерами технической безопасности.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АБИ	Администратор безопасности информации
АС	Автоматизированная система
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПК	Персональный компьютер
ПО	Программное обеспечение
ПРД	Правила (политики) разграничения доступа
ПЭВМ	Персональная электронно-вычислительная машина
РС	Рабочая станция
СВТ	Средство вычислительной техники
СДЗ	Средство доверенной загрузки
СЗИ	Средство защиты информации
ТУ	Технические условия
ФПО	Функциональное программное обеспечение
ЭНП	Энергонезависимая память
BIOS	basic input/output system - «базовая система ввода-вывода»
MBR	master boot record - Главная загрузочная запись
RAM	Random access memory
USB	Universal serial bus

ПРИНЯТЫЕ ТЕРМИНЫ И ОБОЗНАЧЕНИЯ

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

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

Идентификатор – 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.

1. Общие сведения

1.1. Назначение комплекса

ПАК СЗИ НСД «ИНАФ» представляет собой программно-техническое средство, которое реализует функции по предотвращению несанкционированного доступа к программным и (или) техническим ресурсам средства вычислительной техники на этапе его загрузки в соответствии с требованиями документов «Профиль защиты средства доверенной загрузки уровня платы расширения четвертого класса защиты. ИТ.СДЗ.ПР4.ПЗ» и «Программно-аппаратный комплекс средств защиты информации от несанкционированного доступа «ИНАФ». Задание по безопасности» (11443195.4012.046 ЗБ).

ПАК СЗИ НСД «ИНАФ» предназначен для применения на IBM-совместимых ПК (автономных ПК, серверах и рабочих станциях локальной сети) и обеспечивает защиту устройств и информационных ресурсов от НСД, контроль целостности файлов и областей жестких дисков (в том числе и системных) при многопользовательском режиме эксплуатации.

ПАК СЗИ НСД «ИНАФ» обеспечивает нейтрализацию следующих основных угроз безопасности информации:

- несанкционированный доступ к информации за счет загрузки нештатной операционной системы и обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы;
- нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе;
- несанкционированный запуск ПО настроек BIOS;
- 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 позволяет обеспечить возможность доверенной загрузки[1] для ОС, поддерживающих файловые системы: FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, ReiserFS, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX.

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

ПАК СЗИ НСД «ИНАФ» обеспечивает:

- идентификацию и аутентификацию пользователей при входе в систему по персональному идентификатору пользователя и по паролю временного действия длиной от 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;
- идентификацию и аутентификацию пользователей при допуске к средствам настройки и администрирования ПАК «ИНАФ» по персональному идентификатору пользователя и по паролю 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;
- аппаратный контроль целостности технических, программных средств, условно-постоянной информации ПЭВМ до загрузки ОС, с реализацией пошагового алгоритма контроля;
- возможность доверенной загрузки операционной системы, а также системного и прикладного ПО при одновременной установке на дисках или в логических разделах диска ПЭВМ нескольких ОС;
- многопользовательский режим эксплуатации ПЭВМ с возможностью регистрации (в энергонезависимой памяти) до 1024 пользователей на одной ПЭВМ;
- администрирование, включающее:
    - регистрацию пользователей и их идентификаторов, генерацию пароля пользователя и определение его параметров;
    - построение списков объектов для контроля целостности и указание режимов контроля;
    - работу с журналом регистрации системных событий и действий пользователей.
- возможность резервного копирования на отчуждаемый носитель и восстановления базы данных пользователей и списка контролируемых объектов;
- регистрацию и учет системных событий и действий пользователей в системном журнале, размещенном в энергонезависимой памяти аппаратной части комплекса.

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.

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.

Поскольку контроллер «ИНАФ» реализован в форм-факторе USB-устройства, он не требует для своей установки наличия на ПЭВМ свободного PCI-слота и может применяться в случаях, когда используются blade-серверы, в которых отсутствуют PCI-слоты, но имеются свободные внутренние или

внешние USB-разъемы (подробнее о возможных способах установки контроллера в СВТ см. 3.1).

Комплекс «ИНАФ» может использоваться как в качестве самостоятельного продукта, так и в качестве составного компонента различных программно-аппаратных комплексов средств защиты от НСД, разработанных ОКБ САПР.

1.2. Состав комплекса

Комплекс «ИНАФ» выпускается в программно-аппаратном исполнении.

Состав комплекса «ИНАФ»:

- специализированный контроллер (далее по тексту – контроллер) в форм-факторе, обеспечивающем подключение к шине USB с предустановленной на этапе изготовления резидентной операционной средой (специализированное программное обеспечение, СПО), который не реализует функциональные требования безопасности комплекса и представляет собой среду функционирования для функционального программного обеспечения;
- функциональное программное обеспечение (далее по тексту – ФПО), которое является ядром защиты комплекса, реализует функциональные требования безопасности комплекса и исполняется в резидентной операционной среде, предустановленной на специализированный контроллер.

Резидентная операционная среда включает:

- резидентные драйверы специализированных контроллеров;
- резидентные драйверы персональных идентификаторов.

В состав ФПО комплекса входят следующие функциональные модули:

- средства идентификации пользователей;
- средства аутентификации пользователей;
- средства контроля целостности технических средств ПЭВМ (PC);
- средства контроля целостности системных областей жесткого диска;
- средства контроля целостности программных средств;
- средства контроля целостности отдельных ветвей реестра (для ОС семейства Windows);
- средства аудита (работа с журналом регистрации событий);
- средства администрирования комплекса (среда администрирования).

Нерезидентная часть ПО - модуль BIOS - устанавливается на СВТ пользователя с помощью инструментов, получаемых по запросу в техническую поддержку ОКБ САПР.

Доступ к средствам администрирования и аудита комплекса предоставляется только администратору ПАК «ИНАФ».

Среда администрирования является частью комплекса «ИНАФ» и не требует установки какого-либо дополнительного ПО. С помощью нее администратор ПАК «ИНАФ» может добавлять и удалять пользователей, назначать пользователям идентификаторы и пароли, контролировать

аппаратную часть ПЭВМ, прикладные и системные файлы, получать доступ к системному журналу контроллера.

1.3. Условия применения комплекса

1.3.1. Технические условия, необходимые для применения комплекса

Для установки комплекса «ИНАФ» требуется следующий минимальный состав технических и программных средств:

- ПЭВМ типа IBM PC, сервер или рабочая станция, основанная на процессоре с архитектурой x86 (IA-32) или x86-64 (AMD64), функционирующая под управлением операционной системы, поддерживающей любую из файловых систем, приведенных в подразделе 1.1 настоящего руководства;
- наличие свободного USB-разъема на корпусе СВТ или штырькового USB-разъема на материнской плате СВТ, соответствующего варианту исполнения специализированного контроллера «ИНАФ».

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.

2. Функции и интерфейсы администрирования

2.1. Функции администрирования

К функциям администрирования комплекса «ИНАФ», в зависимости от версии ФПО контроллера, относятся (подробнее см. соответствующие подразделы раздела 3):

- установка параметров учетной записи «Гл.Администратор» (настройка данных аутентификации, назначение персонального идентификатора и пароля);
- работа с учетными записями пользователей/ администраторов (создание/ удаление, настройка параметров);
- работа с группами пользователей/ администраторов (создание/ удаление, настройка параметров групп);
- настройки контроля целостности (аппаратуры, служебных областей жестких дисков, файлов);
- просмотр/очистка системного журнала «ИНАФ»;
- общие настройки комплекса (данные конфигурации, режим запуска ACRUN, сторожевой таймер);
- экспорт/импорт баз данных;
- форматирование баз данных контроллера.

2.2. Интерфейсы администрирования

Администрирование комплекса «ИНАФ» выполняется с помощью графического интерфейса пользователя.

3. Управление СДЗ безопасным способом

ВНИМАНИЕ! Всем пользователям комплекса «ИНАФ» (пользователю «Гл.Администратор», пользователям, входящим в группы «Администраторы», «Обычные» и др.) запрещается передавать третьим лицам сведения о паролях от своих учетных записей, а также зарегистрированные для них персональные идентификаторы.

3.1. Сценарии применения

3.1.1. Общие сведения

Комплекс может использоваться в рамках реализации двух типов сценариев:

- стационарная установка в СВТ. В зависимости от конструктивных возможностей СВТ возможна как установка внутри корпуса в качестве штатного устройства с USB-разъемом типа «А», так и подключение к штырьковому разъему непосредственно на материнской плате;
- использование в качестве мобильного устройства с подключением контроллера «ИНАФ» во внешние USB-разъемы СВТ (PC).

3.1.2. Стационарная установка в СВТ

Данный тип сценария используется в том случае, когда необходима непрерывная реализация функционала «ИНАФ». В этом случае контроллер соответствующим образом настроен и подключен к USB-порту СВТ постоянно. Каждый раз перед загрузкой ОС пользователем СВТ контроллер «ИНАФ» выполняет процедуру контроля целостности определенных заранее объектов. В случае нарушения целостности загрузка ОС блокируется и требуется вмешательство администратора «ИНАФ» (пользователь из группы «Администраторы», обладающий соответствующими правами на администрирование комплекса).

Для корректной работы по данному типу сценария **необходимо**:

- установить в BIOS вариант загрузки с «ИНАФ» как с жесткого диска;
- установить пароль на вход в BIOS;
- принять административные меры, исключающие несанкционированное отключение устройства от USB-порта:
  - ограничить физический доступ к СВТ и/или
  - зафиксировать устройство с помощью специальных креплений и/или голографической наклейки или установить контроллер внутрь корпуса СВТ.

3.1.3. Использование в качестве мобильного устройства

Данный тип сценария используется в том случае, когда нет необходимости выполнять процедуры контроля целостности объектов постоянно и запрещать

для пользователей СВТ загрузку ОС в случае нарушения целостности, а нужно только выявить сам факт нарушения целостности установленных на контроль объектов.

В этом случае сначала выполняются все необходимые настройки подключенного к СВТ контроллера «ИНАФ», затем контроллер извлекается из СВТ и хранится в надежном месте (например, в сейфе). Пользователи СВТ работают в обычном режиме, а обладающий соответствующими правами пользователь «ИНАФ» периодически подключает к СВТ свой контроллер «ИНАФ» с целью убедиться в неизменности состава СВТ и установленных ранее на контроль объектов.

Возможен также вариант работы с «ИНАФ», когда контроллер подключается к СВТ каждый раз перед началом сеанса работы и извлекается из СВТ после ее выключения.

Для корректного осуществления работы по данному типу сценария обязательно должны быть предусмотрены специальные регламенты действий пользователей ПЭВМ, в чьи обязанности входит запуск ПЭВМ, так как наличие «ИНАФ» в USB-порту должны контролировать именно они.

Следует помнить о том, что поскольку для работы с «ИНАФ» требуется настраивать порядок загрузки ОС в BIOS компьютера, **необходимо** накладывать определенные ограничения (особенно в случае стационарной установки «ИНАФ» в СВТ) на доступ пользователей СВТ к BIOS (путем установки пароля на BIOS), а также контролировать целостность BIOS средствами «ИНАФ».

3.2. Порядок установки и настройки комплекса

ВНИМАНИЕ! Перед началом установки ПАК СЗИ НСД «ИНАФ» рекомендуется подробно ознакомиться с эксплуатационной документацией, прежде всего с «Описанием применения» (11443195.4012-046 31) и настоящим руководством.

ВНИМАНИЕ! Перед началом установки и настройки ПАК СЗИ НСД «ИНАФ» **необходимо** подробно ознакомиться с содержанием подразделов 1.3, 3.1.

Перед установкой и эксплуатацией комплекса СЗИ НСД «ИНАФ» 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 ПАК СЗИ НСД «ИНАФ» осуществляется администратором безопасности информации в следующей последовательности:

1) установка контроллера в свободный USB-разъем СВТ (подробнее см. подраздел 3.3);

2) установка в BIOS приоритета загрузки с USB-устройства «ИНАФ»;

3) принятие организационных мер, необходимых для работы с ПАК СЗИ НСД «ИНАФ», в том числе установка пароля на вход в BIOS (подробнее см. подразделы 1.3, 3.1 настоящего руководства);

4) установка параметров учетной записи «Гл.администратор», настройка комплекса в соответствии с конфигурацией технических средств ПЭВМ (подробнее см. подразделы 3.5 и 3.15 настоящего руководства);

5) регистрация пользователей, назначение пользователям персональных идентификаторов, паролей и времени доступа (подробнее см. соответствующие подразделы раздела 3 настоящего руководства);

6) назначение списка дисков, файлов, разделов реестра, контролируемых на целостность (подробнее см. соответствующие подразделы раздела 3 настоящего руководства).

3.3. Установка контроллера

ВНИМАНИЕ! Установка контроллера должна производиться только при выключенном питании СВТ!

Для установки контроллера комплекса необходимо:

1) отключить питание СВТ;

2) установить контроллер в свободный USB-порт СВТ.

3.4. Начало работы

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

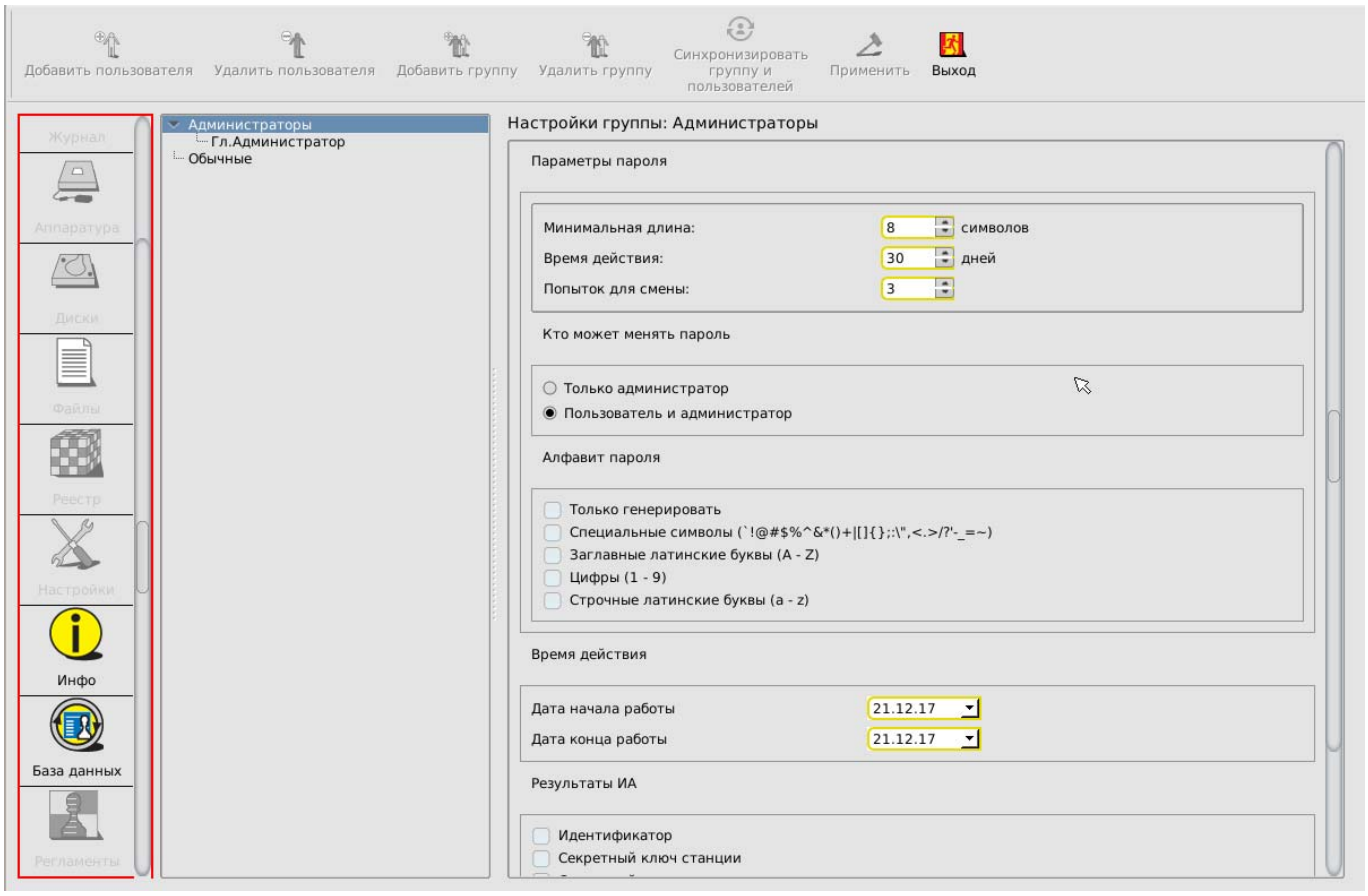

Рисунок 1 - Главное окно среды администрирования

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;
- <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 2), без выполнения которой не доступны никакие функции «ИНАФ».

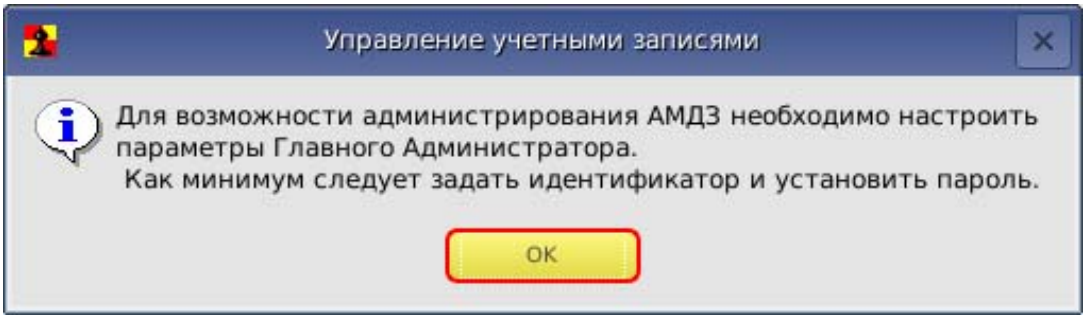

Рисунок 2 - Сообщение с требованием настроить параметры учетной записи «Гл.Администратор»

После выполнения процедуры установки параметров учетной записи «Гл.Администратор», описанной в подразделе 3.5 настоящего руководства, функционал «ИНАФ» 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).

3.5. Установка параметров учетной записи «Гл. Администратор» (администратора безопасности информации)

При инициализации контроллера в базе данных создается учетная запись «Гл.Администратор»[1] – пользователя, имеющего особый статус и абсолютные полномочия в среде администрирования «ИНАФ».

При этом для этого пользователя не установлены параметры учетной записи.

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

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

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

- параметры пароля (см. подраздел 3.6.2.1);
- результаты ИА (см. подраздел 3.6.2.2).

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

Далее следует перейти к настройке обязательных для учетной записи параметров:

- персональный идентификатор (см. подраздел 3.5.1);
- пароль (см. подраздел 3.5.2).

3.5.1. Назначение персонального идентификатора

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

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

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

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

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

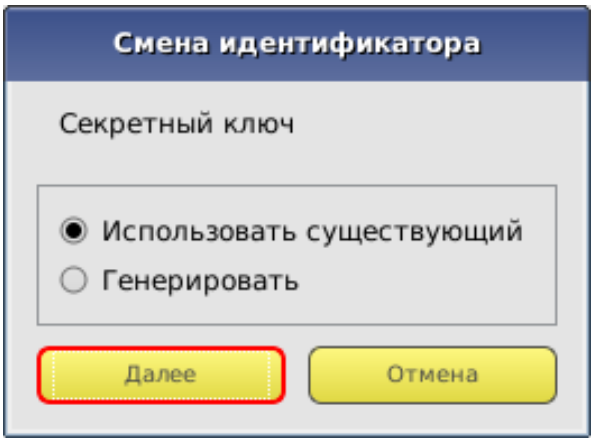

Рисунок 3 – Окно выбора секретного ключа

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

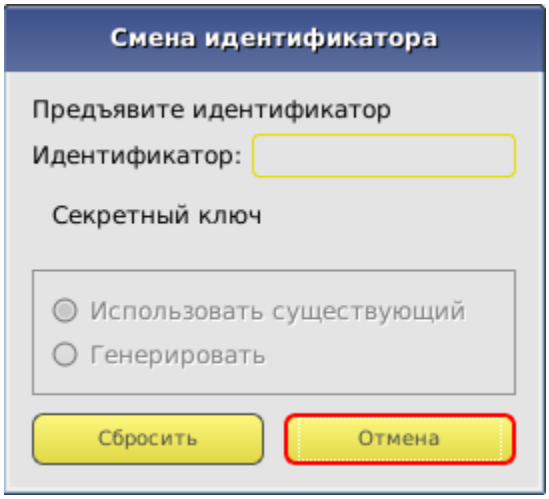

Рисунок 4 – Окно с запросом идентификатора для смены

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

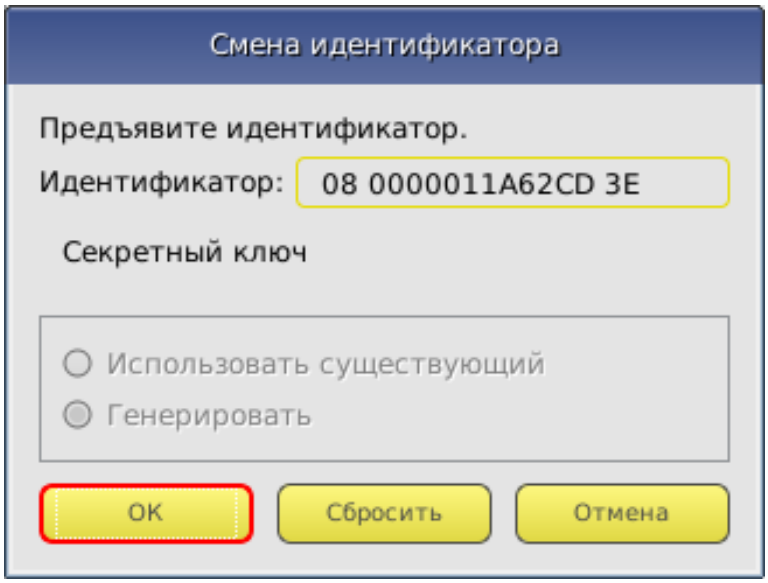

Рисунок 5 – Окно смены идентификатора

Необходимо подтвердить завершение операции нажатием кнопки <OK>.

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

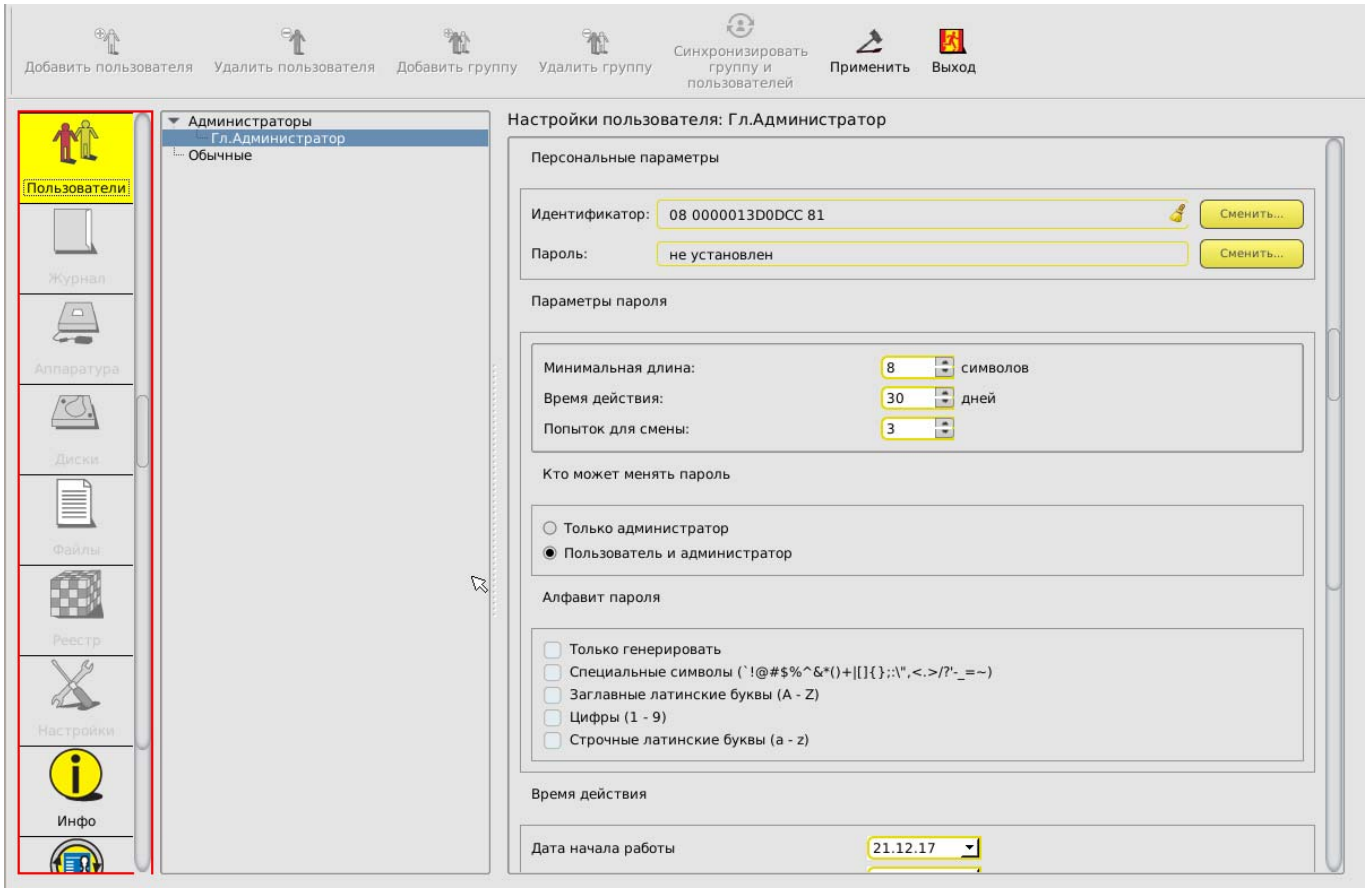

Рисунок 6 - Идентификатор для учетной записи «Гл.Администратор» установлен

Далее необходимо перейти к процедуре назначения пароля (см. 3.5.2).

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

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

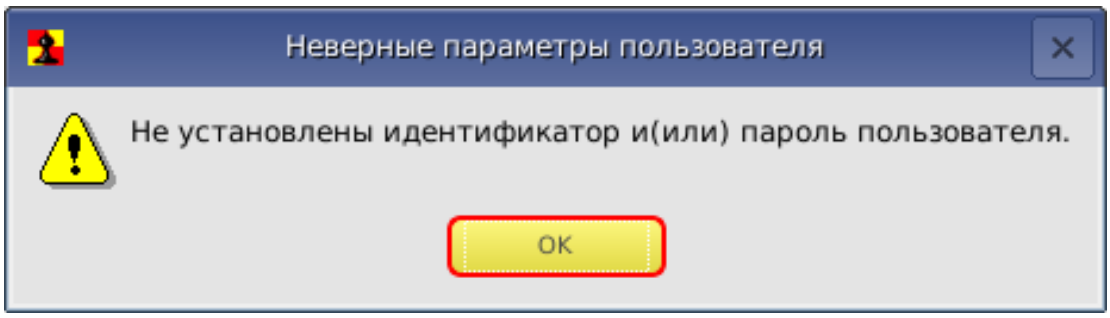

Рисунок 7 - Сообщение о том, что идентификатор или пароль пользователя не установлены

3.5.2. Назначение пароля

Перед выполнением процедуры назначения пароля на правой панели главного окна среды администрирования (рисунок 1) нужно установить необходимые параметры пароля (подробнее см. 3.6.2.1).

Выполнение процедуры назначения пароля начинается посредством нажатия кнопки <Сменить> в строке «Пароль» главного окна среды администрирования (рисунок 6).

На экран выводится окно ввода пароля (рисунок 8). При первоначальной регистрации параметров пользователя строка «Старый пароль» недоступна. Необходимо ввести новый пароль и подтвердить ввод пароля во второй строке.

Пароль может состоять из букв, цифр и специальных символов (в зависимости от установленных администратором параметров пароля – см. 3.6.2.1). 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.

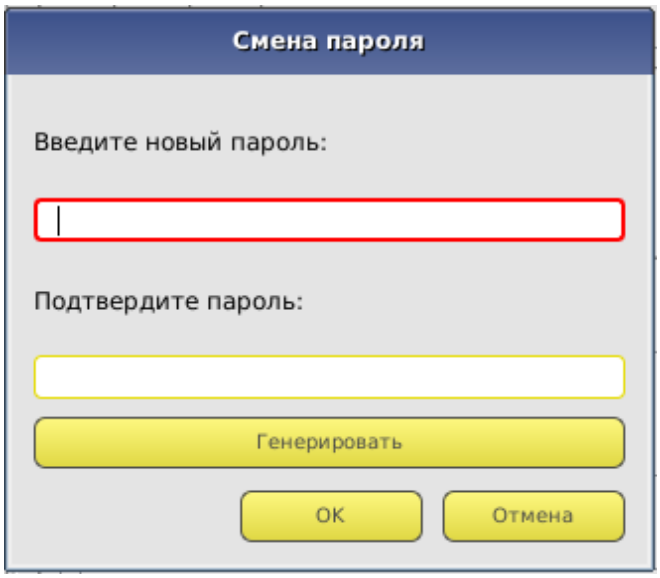

Рисунок 8 – Окно ввода пароля

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

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

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

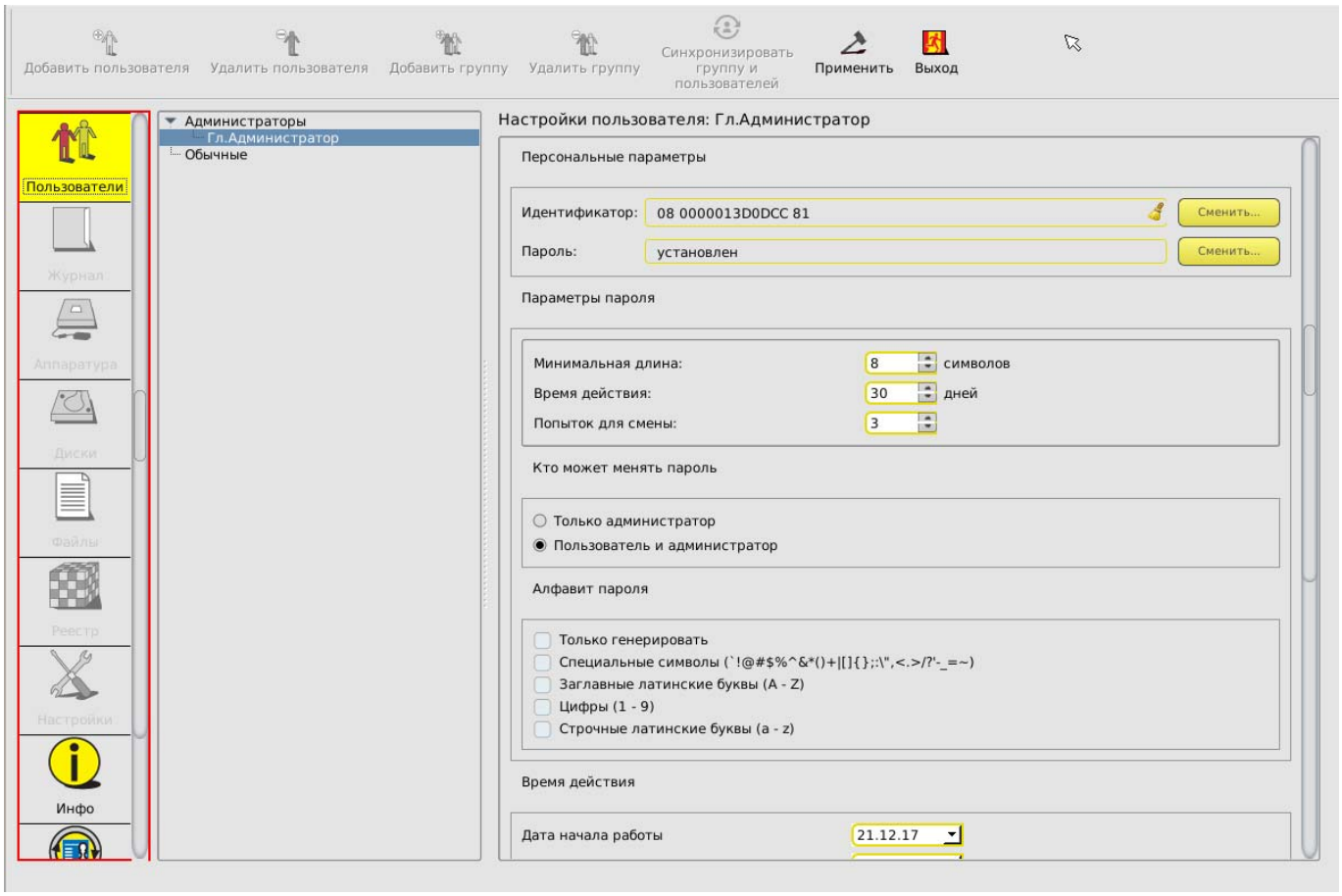

Рисунок 9 - Пароль для учетной записи «Гл.Администратор» установлен

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

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

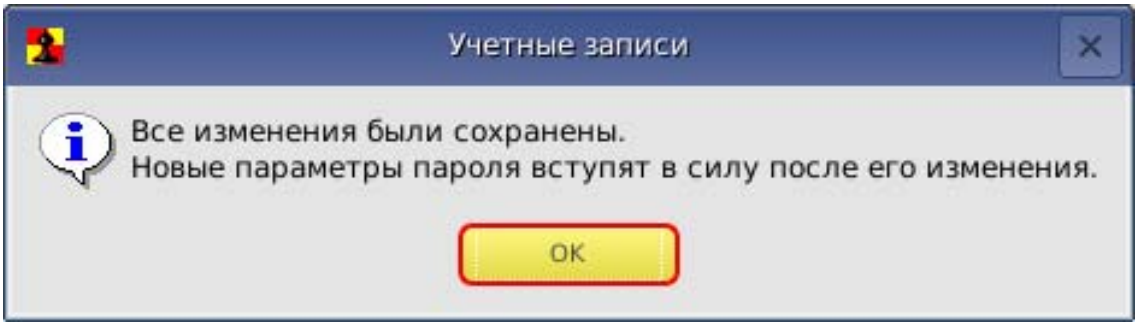

Рисунок 10 - Сообщение о сохранении внесенных изменений

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

3.6. Настройка параметров групп и учетных записей пользователей

3.6.1. Список пользователей

При инициализации контроллера создаются две зарезервированные группы пользователей – «ADMINS» (далее – «Администраторы») и «EVERYONE» (далее – «Обычные»)[1]. Эти две группы нельзя ни переименовать, ни удалить.

Для каждой из групп можно задать общие параметры, которые будут устанавливаться по умолчанию при создании пользователя в группе.

Для каждого зарегистрированного пользователя можно изменить данные параметры при индивидуальной настройке. Такие же правила будут выполняться и для любой группы, созданной администратором.

Для редактирования общих параметров группы пользователей необходимо в главном окне среды администрирования выбрать из списка нужную группу пользователей, мышью установив курсор на строке заголовка группы (рисунок 1).

3.6.2. Общие параметры группы «Администраторы»

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

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

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

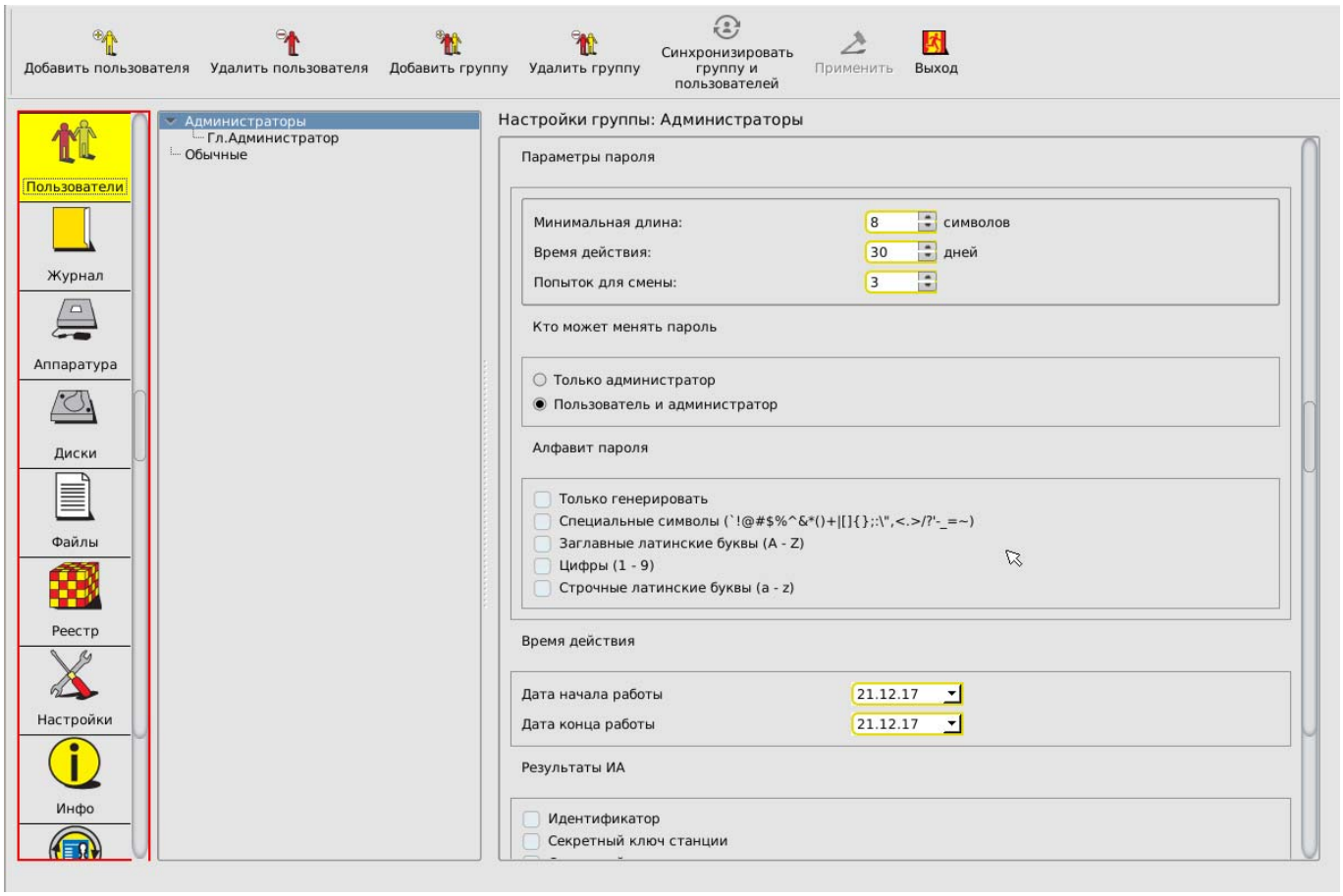

Рисунок 11 - Общие параметры группы «Администраторы»

3.6.2.1. Параметры пароля

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

- «Минимальная длина» - параметр определяет количество символов, контролируемое при создании и смене пароля. Нельзя ввести пароль меньшей длины. Если для авторизации пользователя предполагается использовать только идентификатор, этот параметр нужно установить равным 0 (пароль задавать не обязательно). По умолчанию длина пароля установлена равной 8 символам, максимальное допустимое значение - 12 символов.
- «Время действия» - время действия пароля до смены в календарных днях: от 0 (смены пароля не требуется) до 366 дней.
- «Попыток для смены» - количество попыток смены пароля: от 0 (не ограничено) до 5. Этот параметр определяет допустимое число попыток смены пароля, если пользователю разрешено самому выполнять такую операцию. Если за отведенное число попыток пароль не сменен корректно, выполняется перезагрузка компьютера.
- «Кто может менять пароль» - установка этого параметра позволяет задать политику в отношении смены пароля: пользователь может самостоятельно менять пароль (после истечения времени действия или в произвольный момент времени по своей инициативе) или смену пароля осуществляет только администратор.

– «Алфавит пароля» - определяет набор символов, которые обязательно должны использоваться при вводе пароля. Например, если в алфавите заданы цифры и буквы, то нельзя ввести пароль, состоящий из одних цифр. При установке флага «Только генерировать» пароль будет генерироваться случайным образом из символов заданного алфавита при смене пароля пользователя.

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

3.6.2.2. Результаты ИА

В разделе «Результаты ИА» устанавливается, какая информация о пользователе, полученная в результате процесса идентификации/аутентификации, будет передаваться из контроллера в программную подсистему разграничения доступа (если таковая установлена на компьютере) 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 «ИНАФ» 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 «ИНАФ» 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 «ИНАФ» (без подсистемы разграничения доступа).

3.6.3. Общие параметры группы «Обычные» (пользователи)

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

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

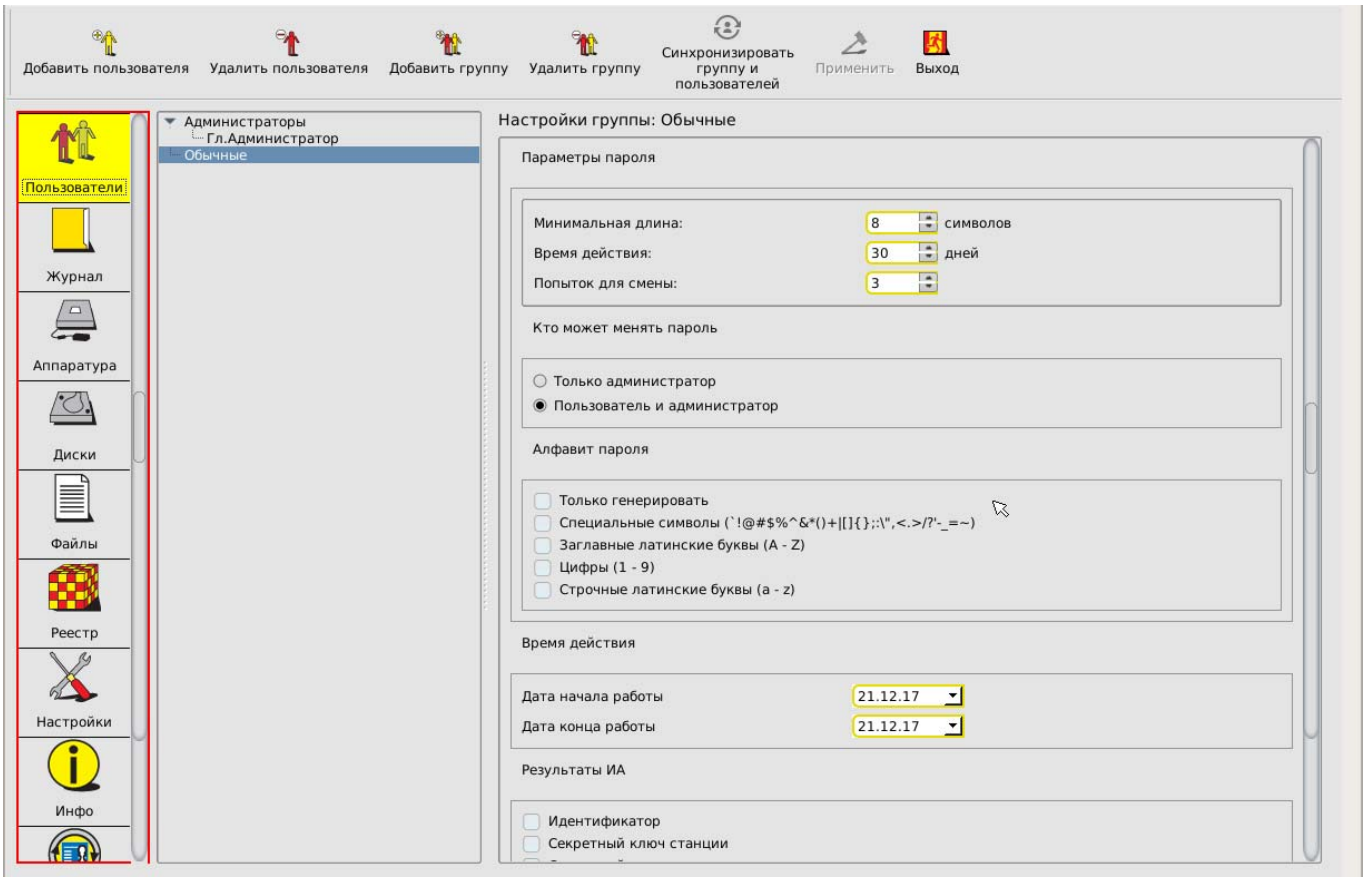

Рисунок 12 – Общие параметры группы «Обычные»

Настройки параметров пароля и результатов ИА аналогичны настройкам соответствующих общих параметров для группы «Администраторы».

3.6.4. Параметры пользователей в группе «Администраторы»

3.6.4.1. Общие сведения

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

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

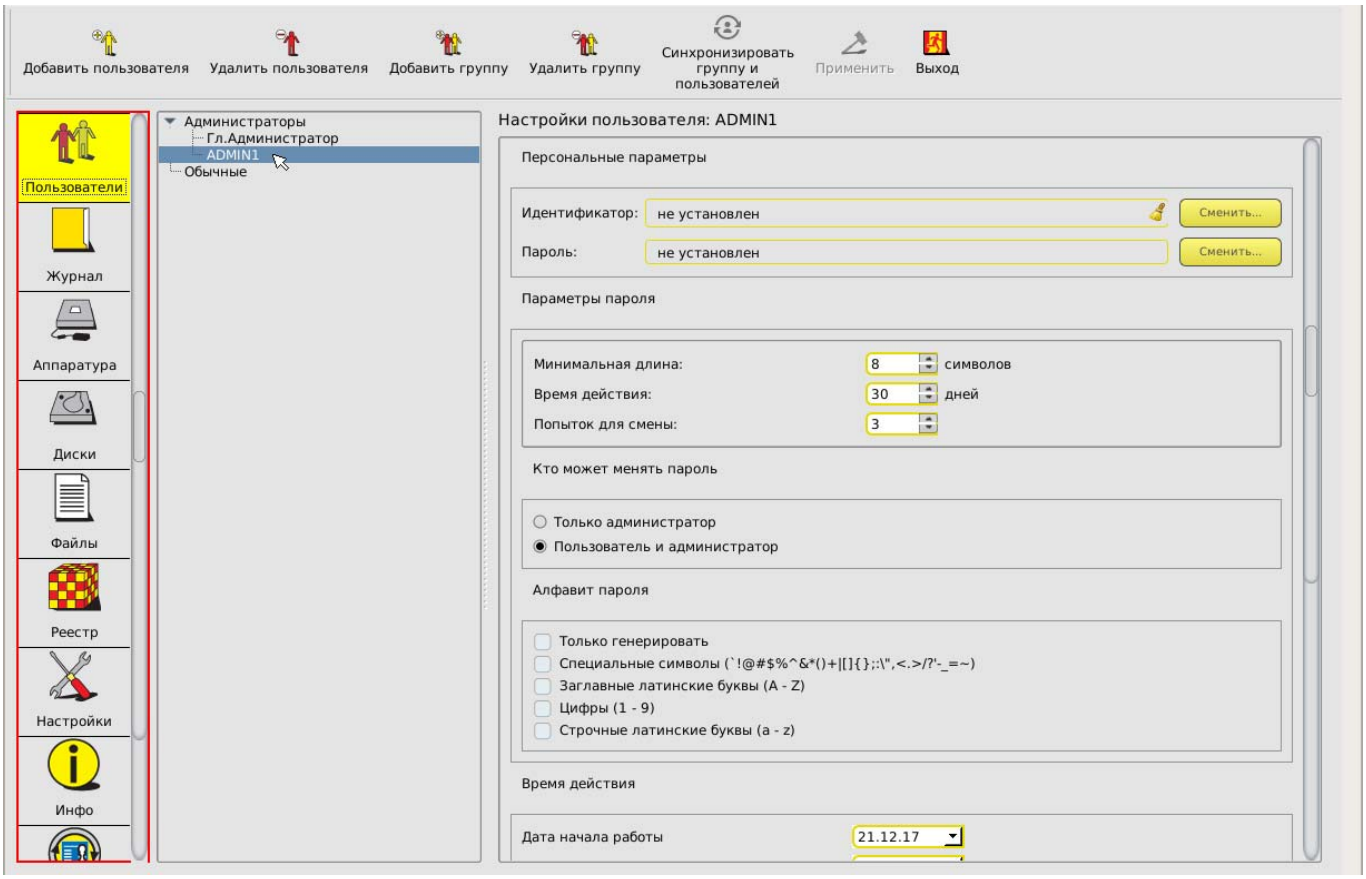

Рисунок 13 – Параметры пользователей в группе «Администраторы»

3.6.4.2. 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 13).

В поле «Идентификатор» отображается восьмизначный 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 3.5.1.

Поле «Пароль» содержит информацию о наличии установленного пароля пользователя и может иметь только одно из двух значений: «установлен» или «не установлен». Пароль пользователя может быть установлен или сменен посредством выполнения операций, описанных в подразделе 3.5.2.

3.6.4.3. Параметры пароля

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

3.6.4.4. Атрибуты доступа

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

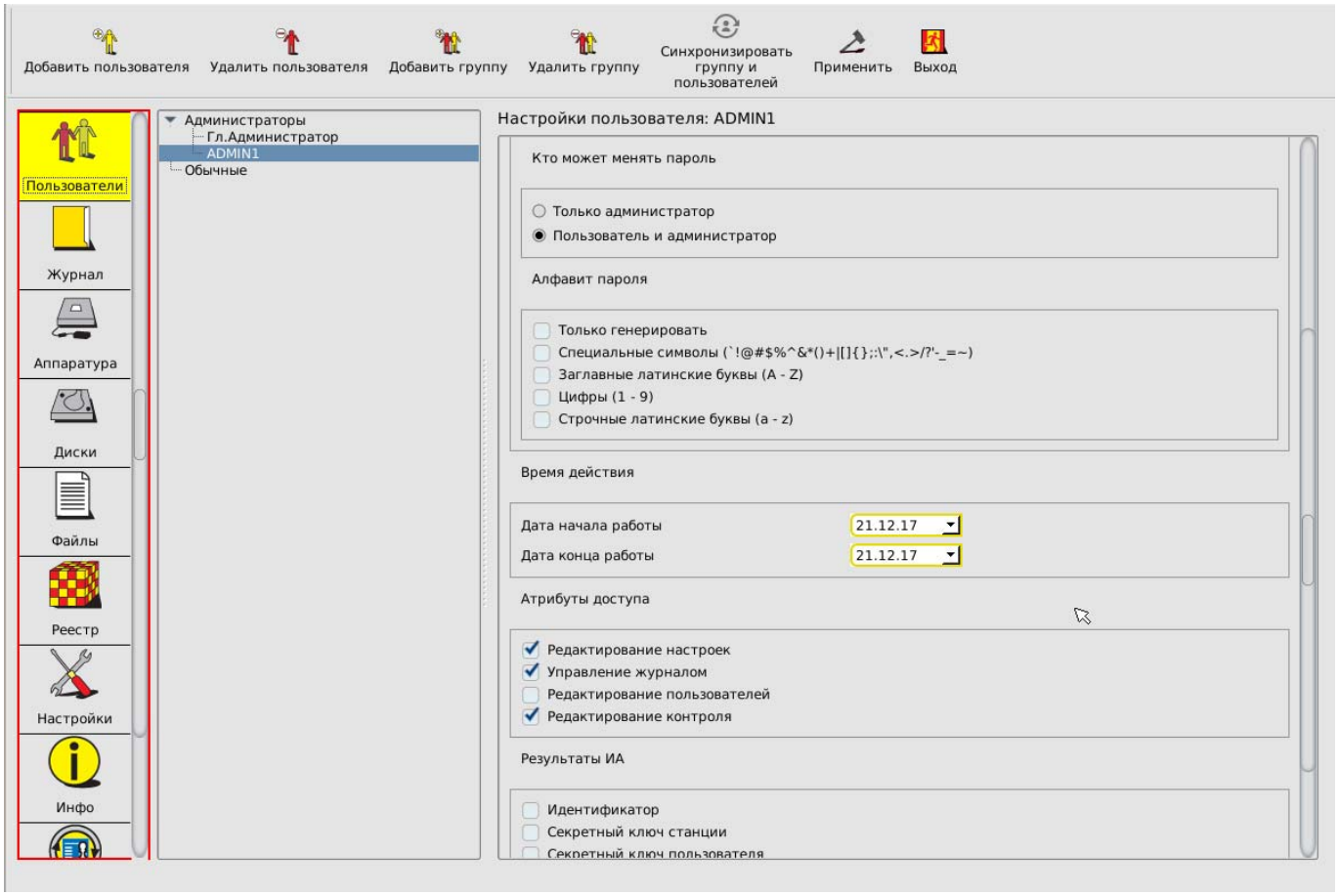

Рисунок 14 – Атрибуты доступа для пользователей из группы «Администраторы»

В данном разделе для выбранного пользователя из группы «Администраторы» 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. 3.15). При снятии данного флага для выбранного пользователя функции изменения настроек недоступны, кнопка <Настройки> в меню выбора объектов администрирования отсутствует.

- Управление журналом. При установке данного флага выбранный пользователь может просматривать и очищать системный журнал (подробнее см. 3.14). При снятии данного флага для выбранного пользователя функции редактирования журнала недоступны, кнопка <Журнал> в меню выбора объектов администрирования отсутствует.
- Редактирование пользователей. При установке данного флага выбранный пользователь может выполнять редактирование списков пользователей (подробнее см. подразделы 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.8, 3.9, 3.10, 3.11). При снятии данного флага для выбранного пользователя функции редактирования списков пользователей недоступны, кнопка <Пользователи> в меню выбора объектов администрирования отсутствует.
- Редактирование контроля. При установке данного флага выбранный пользователь может выполнять редактирование списков контроля целостности аппаратуры и реестра, служебных областей жестких дисков, файлов (подробнее см. 3.13). При снятии данного флага для выбранного пользователя функции редактирования списков контроля целостности недоступны, кнопки <Аппаратура>, <Диски>, <Файлы> в меню выбора объектов администрирования отсутствуют.

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

3.6.4.5. Результаты ИА

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

3.6.5. Параметры пользователей в группе «Обычные»

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

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

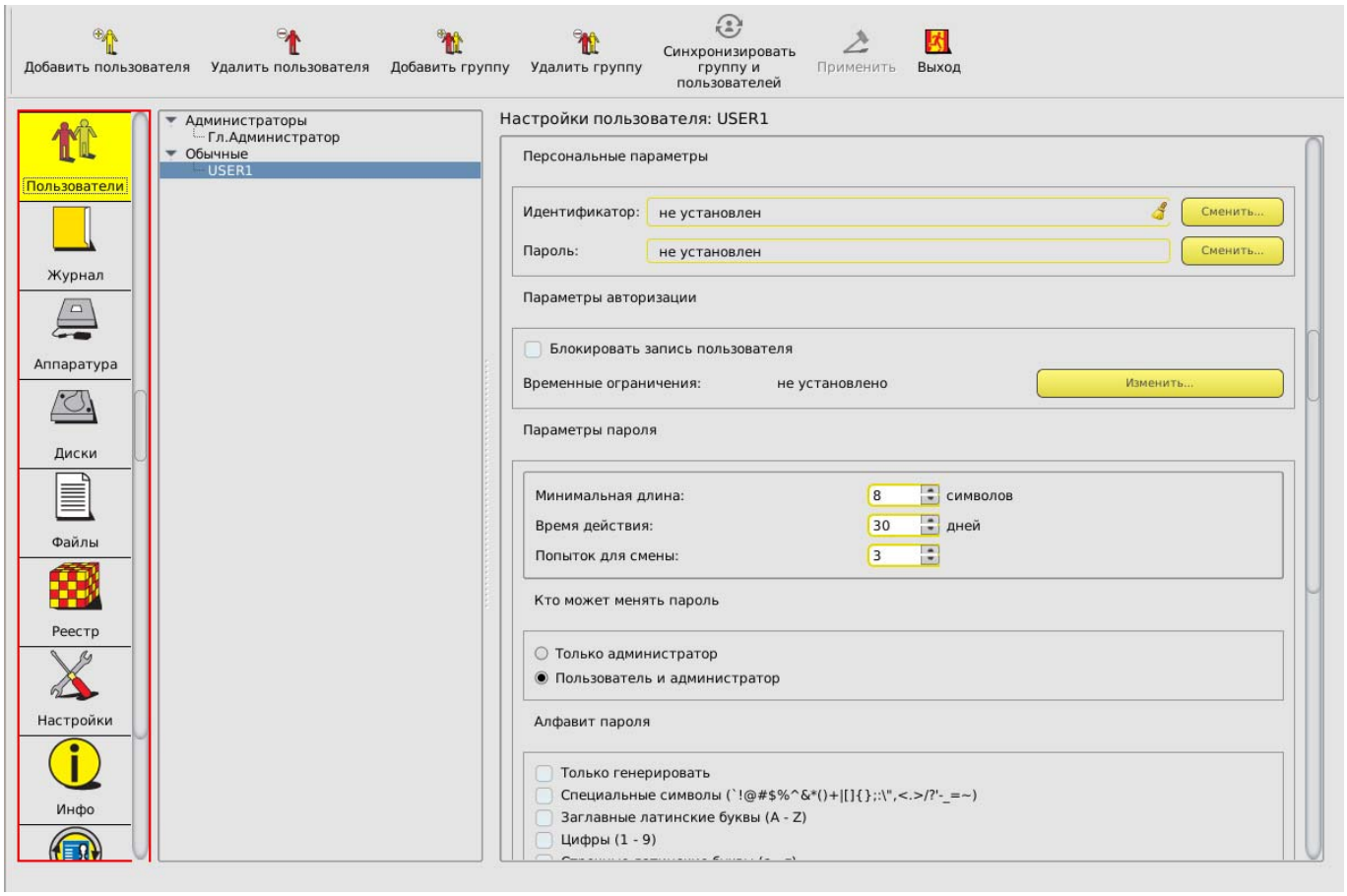

Рисунок 15 – Параметры пользователей в группе «Обычные»

3.6.5.1. Персональные параметры

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

3.6.5.2. Параметры авторизации

Для пользователей группы «Обычные» установлены следующие параметры авторизации:

- режим блокировки;
- временные ограничения.

3.6.5.2.1. Режим блокировки

При установке флага «Блокирован» в состояние «Да» все параметры пользователя сохраняются в базе данных, но вход в систему и работа данного пользователя будут запрещены. Данный флаг можно использовать для временной блокировки пользователя. После того, как администратор снимет блокировку, работа пользователя восстановится со всеми установленными настройками. Изменить состояние данного флага можно щелчком мыши.

3.6.5.2.2. Временные ограничения

Администратор может устанавливать для пользователя ограничения на вход в систему с точностью до 30 минут в любой день недели. Для этого нужно

нажать кнопку <Изменить> в строке «Временные ограничения». На экран выводится окно редактирования параметров «Временные ограничения» (рисунок 16).

Рисунок 16 - Временные ограничения на загрузку компьютера

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

3.6.5.3. Параметры пароля

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

3.6.5.4. Результаты ИА

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

3.7. Регистрация нового администратора

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

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

Далее необходимо зарегистрировать идентификатор и задать пароль пользователя. Данная процедура аналогична соответствующим процедурам, выполняемым при настройке параметров учетной записи «Гл. Администратор» (подробнее см. в 3.5.1 и 3.5.2).

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

3.8. 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» (подробнее см. в 3.5.1 и 3.5.2).

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

3.9. 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.

3.10. 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 подразделе 3.6.3.

3.11. 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.

3.12. 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.

3.13. 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>.

3.13.1. Контроль аппаратуры

ПАК «ИНАФ» 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 17).

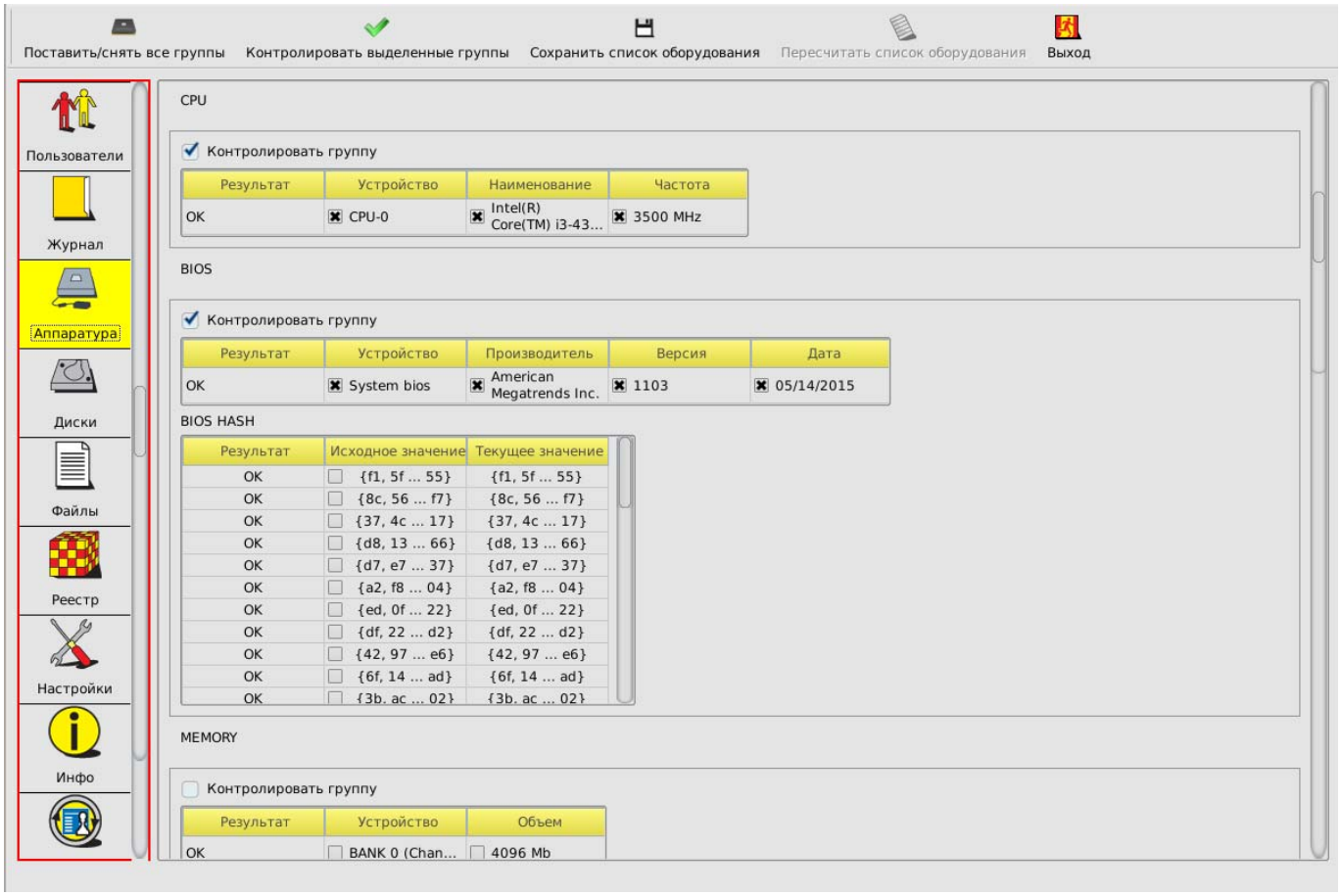

Рисунок 17 - Окно контроля аппаратной части компьютера

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 ПАК «ИНАФ» хотя бы одного пользователя контроль аппаратуры производится при каждой загрузке компьютера после идентификации/аутентификации пользователя. Если обнаруживается несовпадение параметров конфигурации, записанных в памяти контроллера и текущих параметров системы, то выдается сообщение «Контроль не пройден» и загрузка компьютера блокируется – для обычного пользователя или выводится запрос на администрирование, если идентифицирован администратор.

Может встречаться ситуация, когда после перезагрузки ПАК «ИНАФ» 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>.

3.13.2. 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 18). В рамках контроля поддерживаются файловые системы, список которых приведен в подразделе 1.1 настоящего руководства.

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

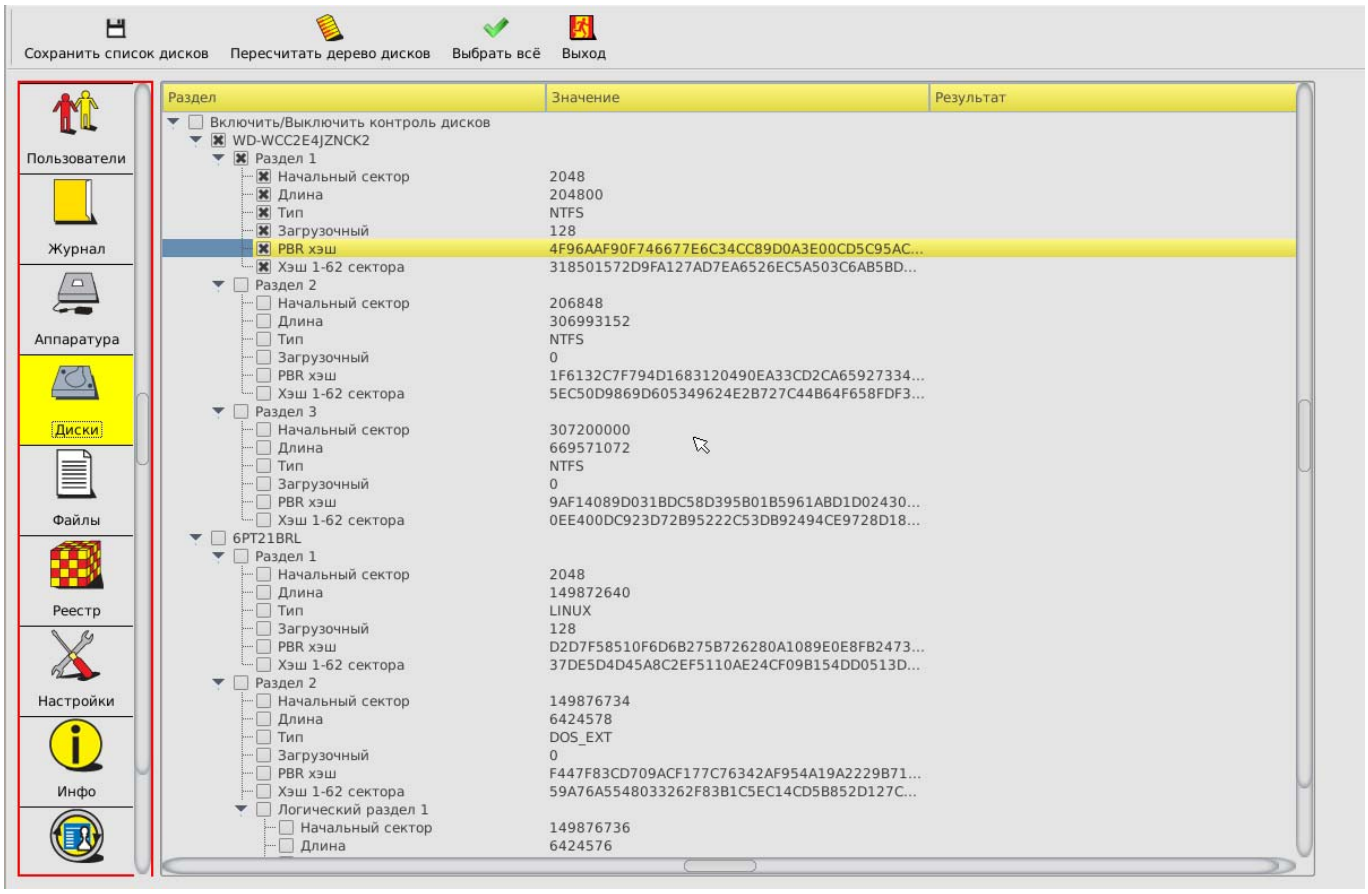

Рисунок 18 - Окно контроля служебных областей диска

3.13.3. Контроль целостности файлов

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

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

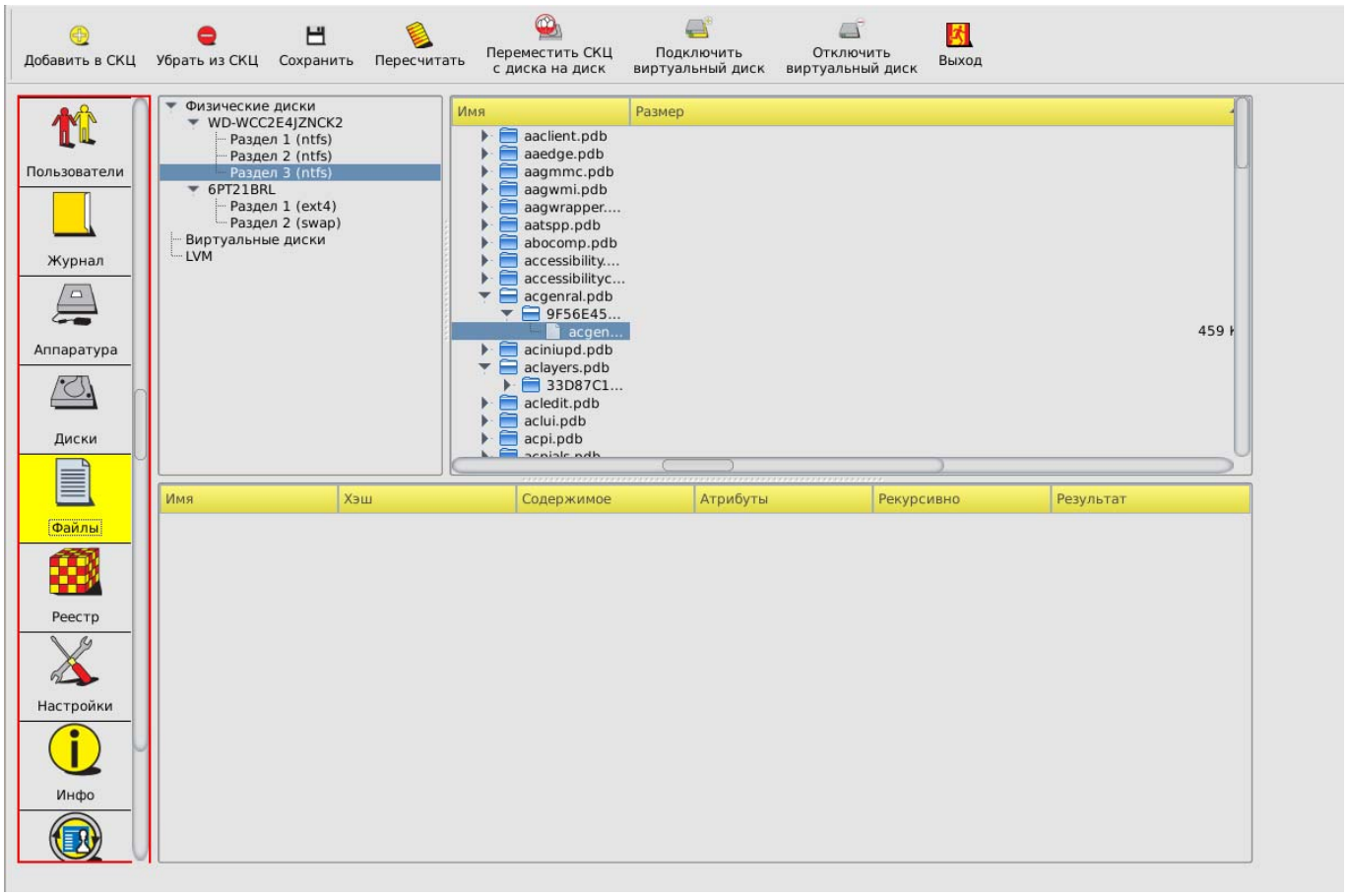

Рисунок 19 - Окно контроля целостности файлов

В правой части экрана можно выбрать конкретные файлы или каталоги.

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

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

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

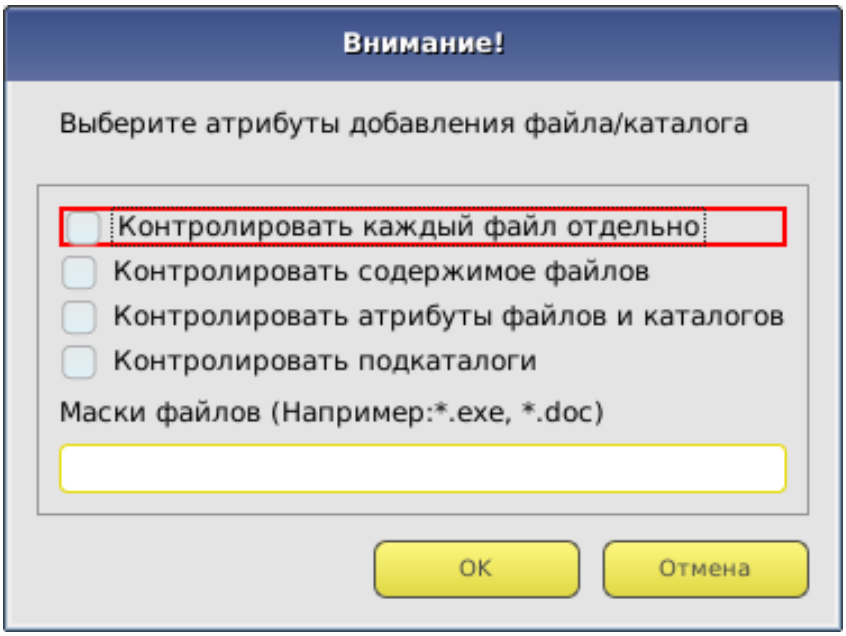

Рисунок 20 – Окно выбора атрибутов добавления каталога

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

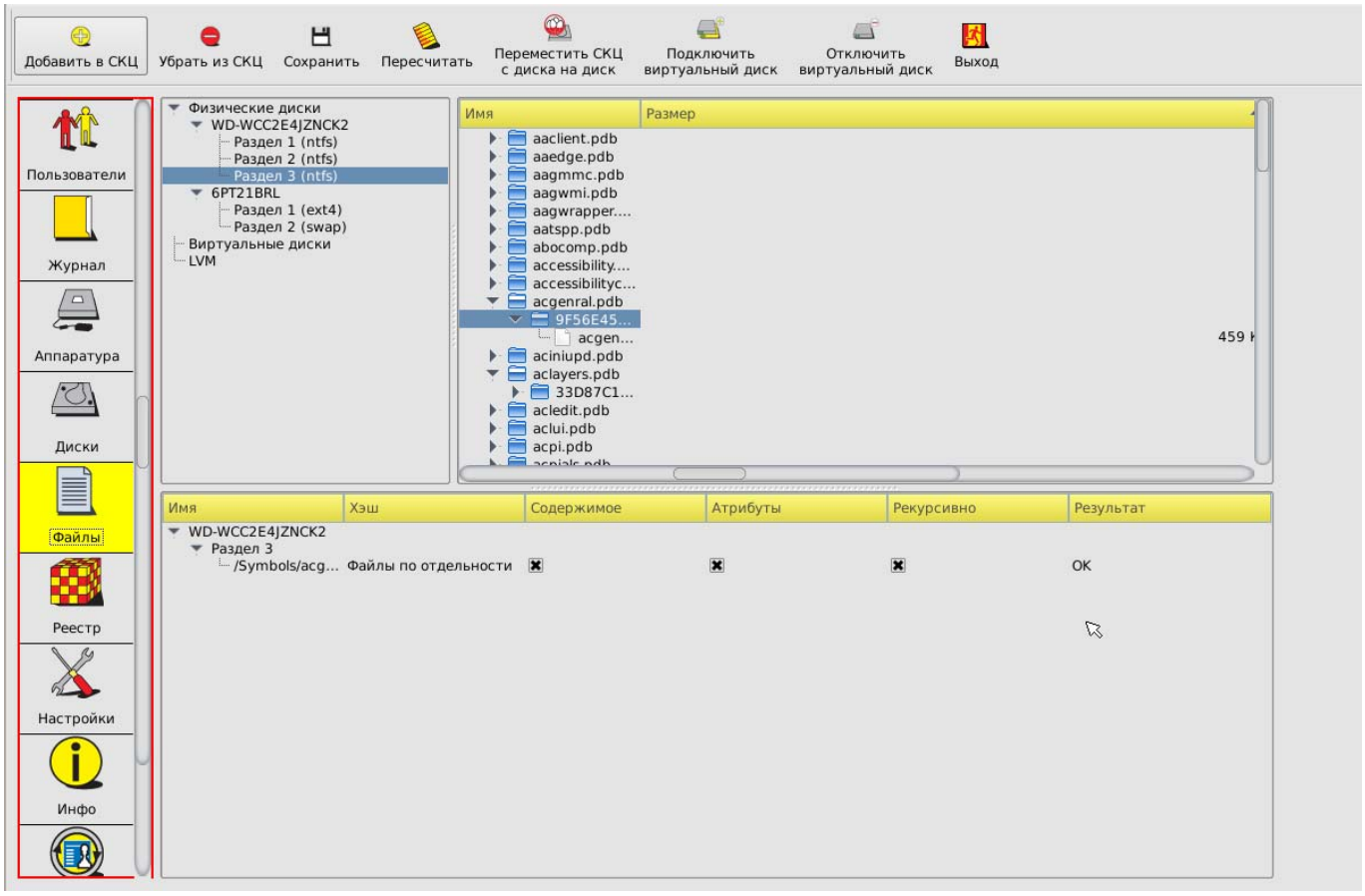

Рисунок 21 – Список контроля целостности с добавленным в него каталогом

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

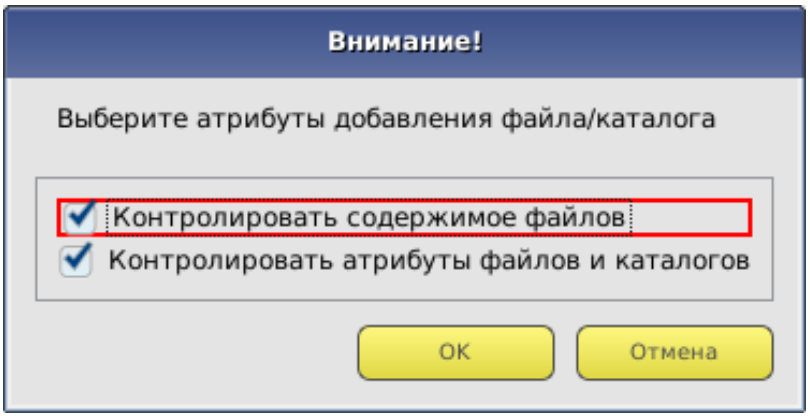

Рисунок 22 – Окно выбора атрибутов добавления файла

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

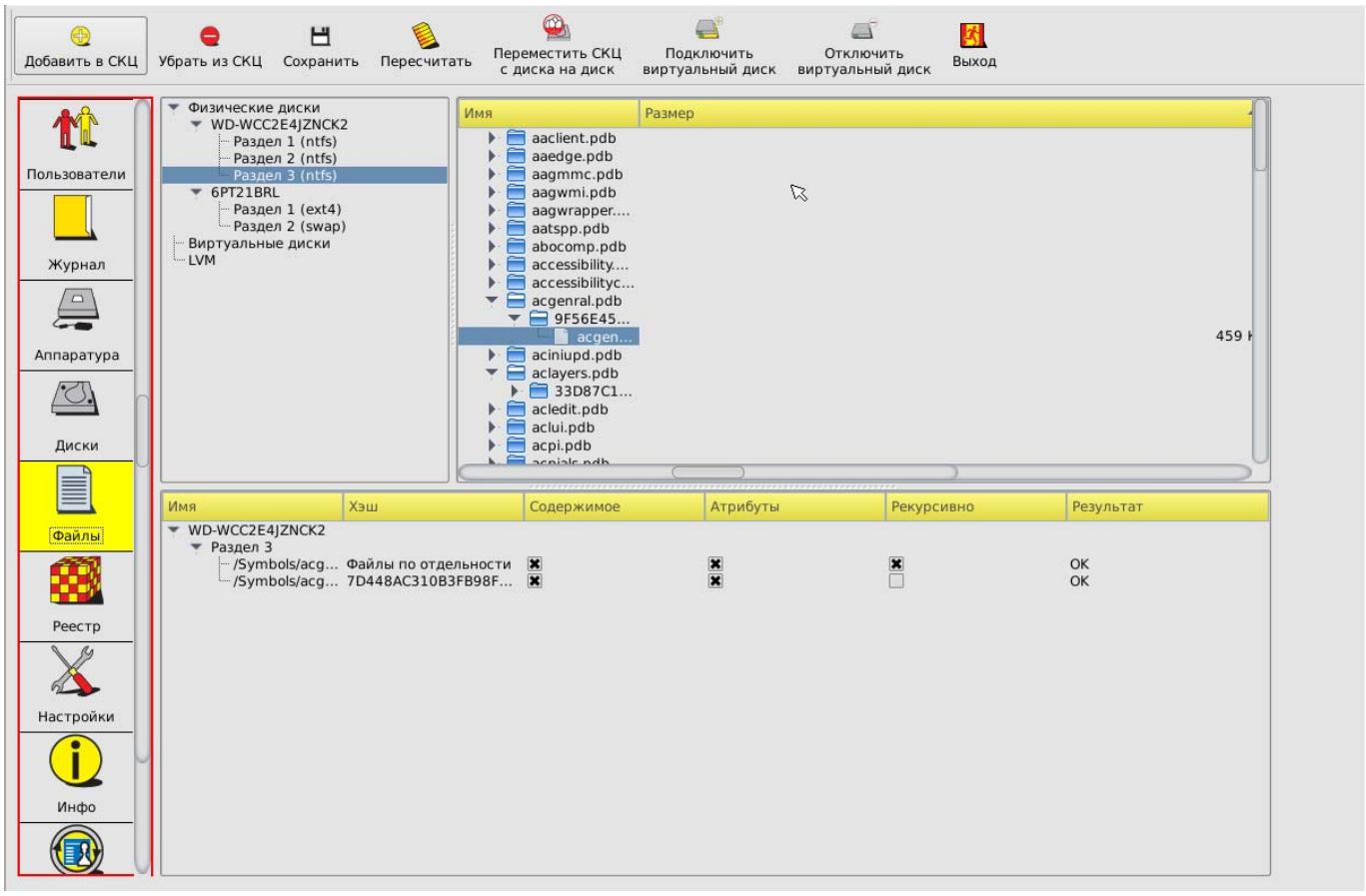

Рисунок 23 – Список контроля целостности с добавленным в него файлом

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

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

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

Хэш-функция контролируемых файлов пересчитывается при каждой загрузке компьютера с установленным контроллером «ИНАФ» 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 СКЦ>), затем выполнить необходимые изменения и нажать кнопку <Сохранить СКЦ>.

Примечание: *Количество файлов, которые можно установить на контроль, зависит от операционной системы и от длины пути к каталогу, где находятся файлы. Среднее количество составляет 1200-1500 файлов. Список файлов ОС Windows 7 (x32, x64), рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «ИНАФ»), приведен в Приложении 3.*

3.13.3.1. 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 24).

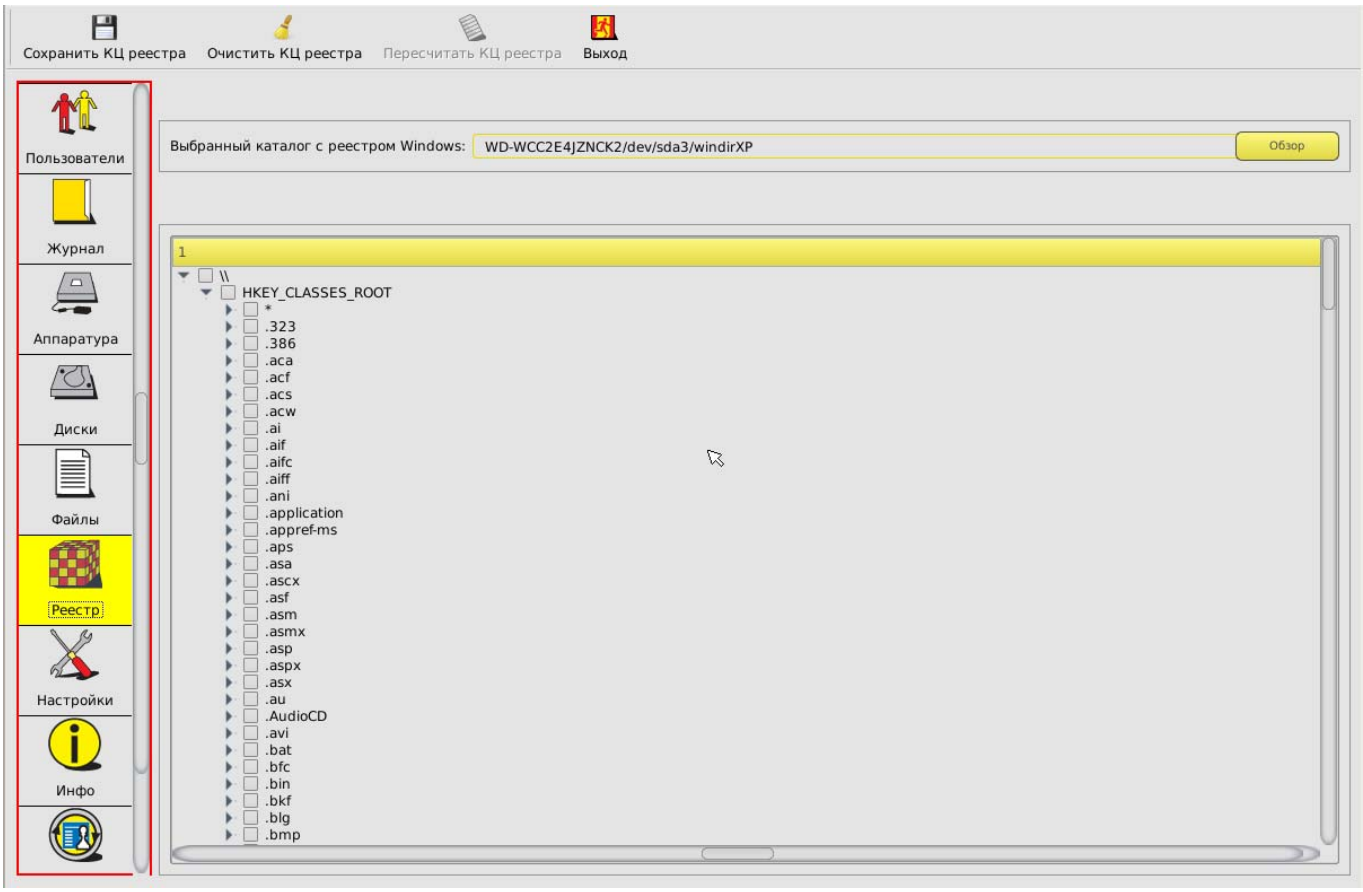

Рисунок 24 – Информация о состоянии реестра

Для добавления ветки реестра добавлена в список контролируемых комплексом объектов следует выбрать ее из списка, установить напротив нее галочку и нажать кнопку <Сохранить КЦ реестра> (рисунок 25).

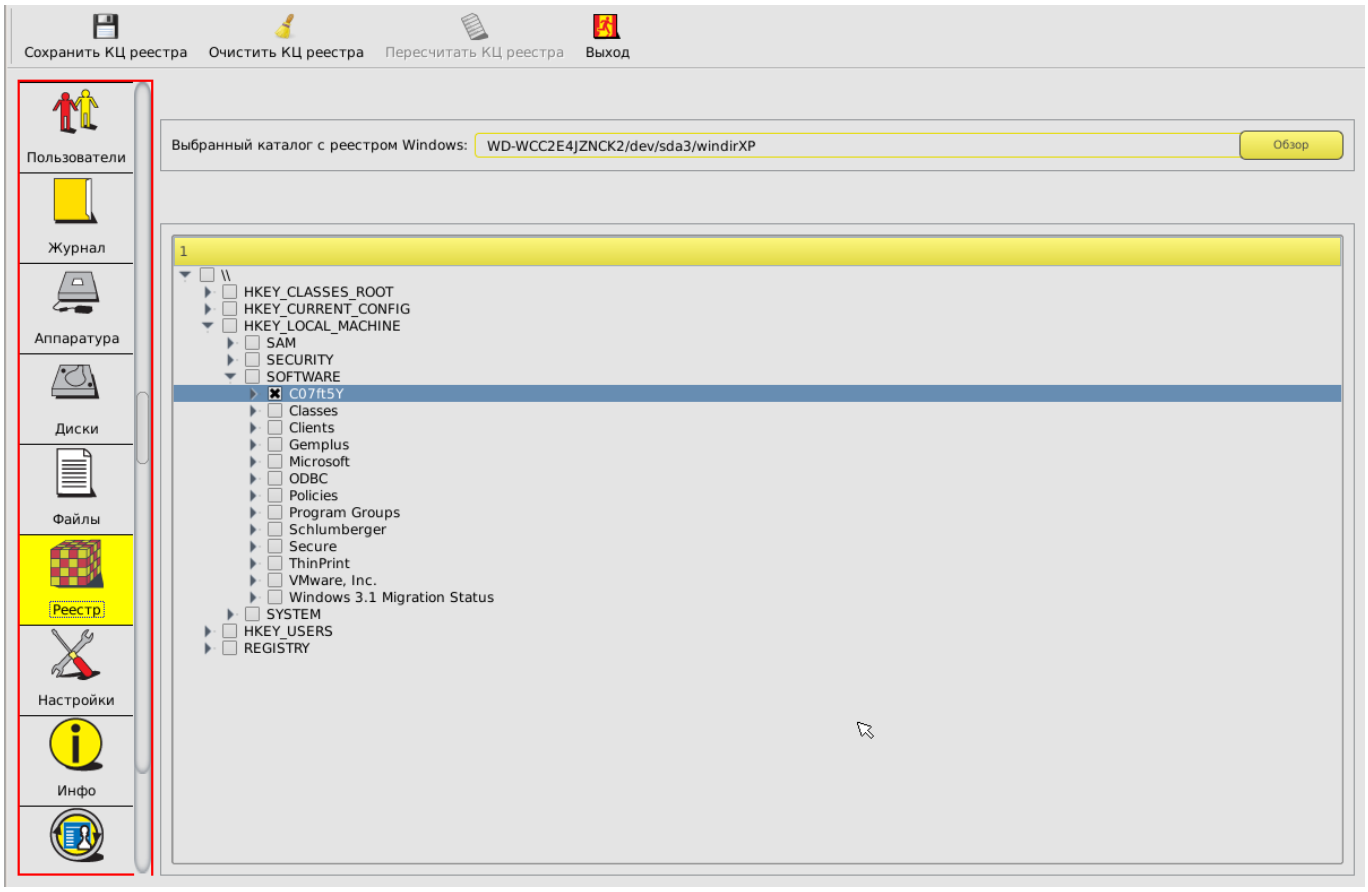

Рисунок 25 - Постановка ветви реестра на контроль целостности

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>.

3.14. Системный журнал

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

Для просмотра журнала следует в главном окне среды администрирования выбрать объект администрирования <Журнал>. На экран выводится окно системного журнала (рисунок 26). Подробнее об основных параметрах, фиксируемых в журнале, и их обозначениях см. Приложение 1.

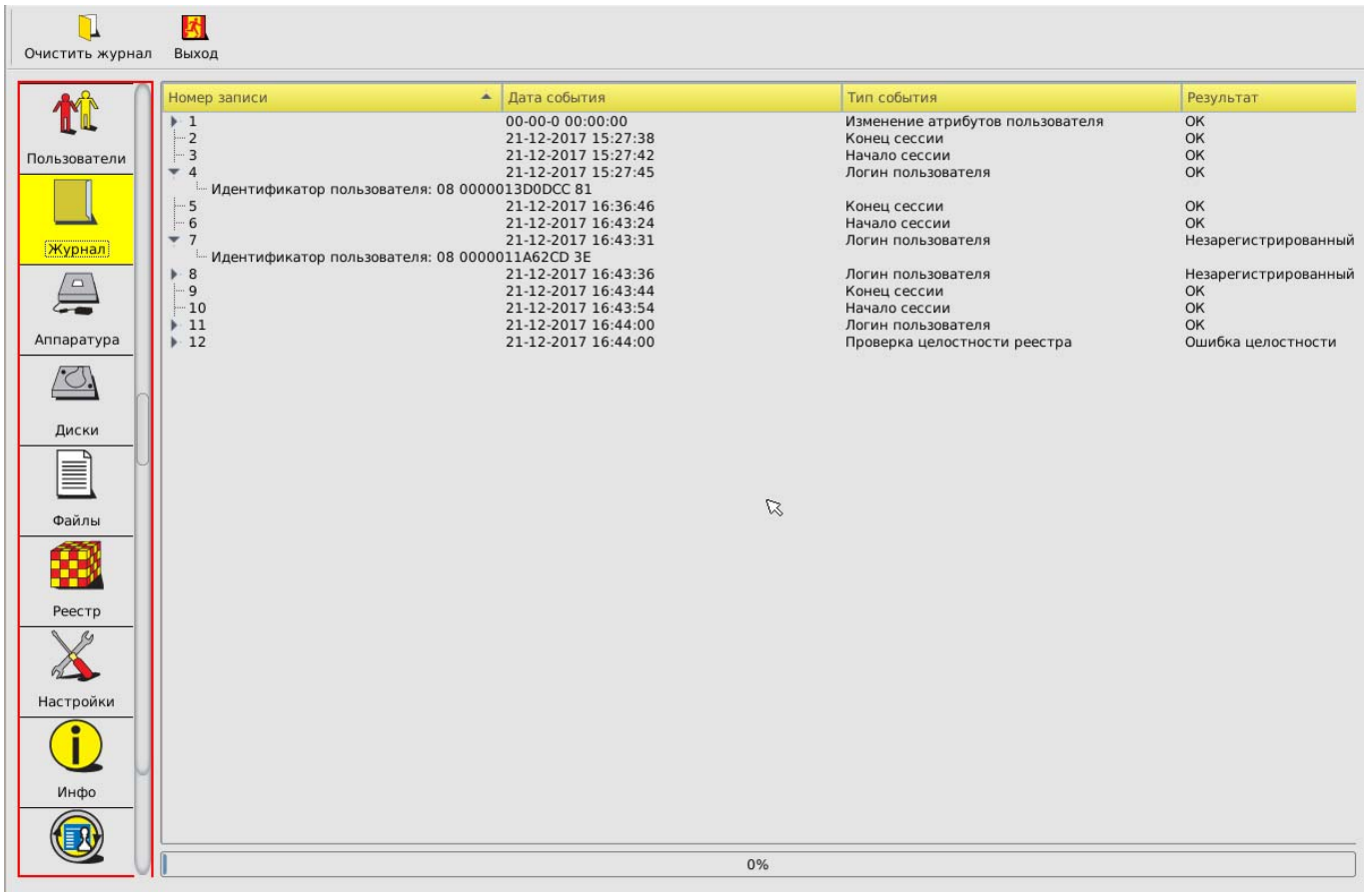

Рисунок 26 - Системный журнал контроллера

Если процент заполнения журнала превышает 85%, при загрузке компьютера выдается предупреждение, но загрузка продолжается. Если процент заполнения журнала превышает 95%, то загрузка для пользователя блокируется и требуется вмешательство администратора. Для очистки журнала служит кнопка <Очистить журнал> (рисунок 26).

3.15. Общие настройки комплекса

Редактирование общих настроек комплекса выполняется администратором комплекса, обладающим правами на изменение настроек комплекса «ИНАФ».

Для изменения общих настроек комплекса необходимо нажать кнопку <Настройки> в меню выбора объектов администрирования. На экран выводится окно с настройками комплекса (рисунок 27).

В настройках комплекса представлены данные конфигурации.

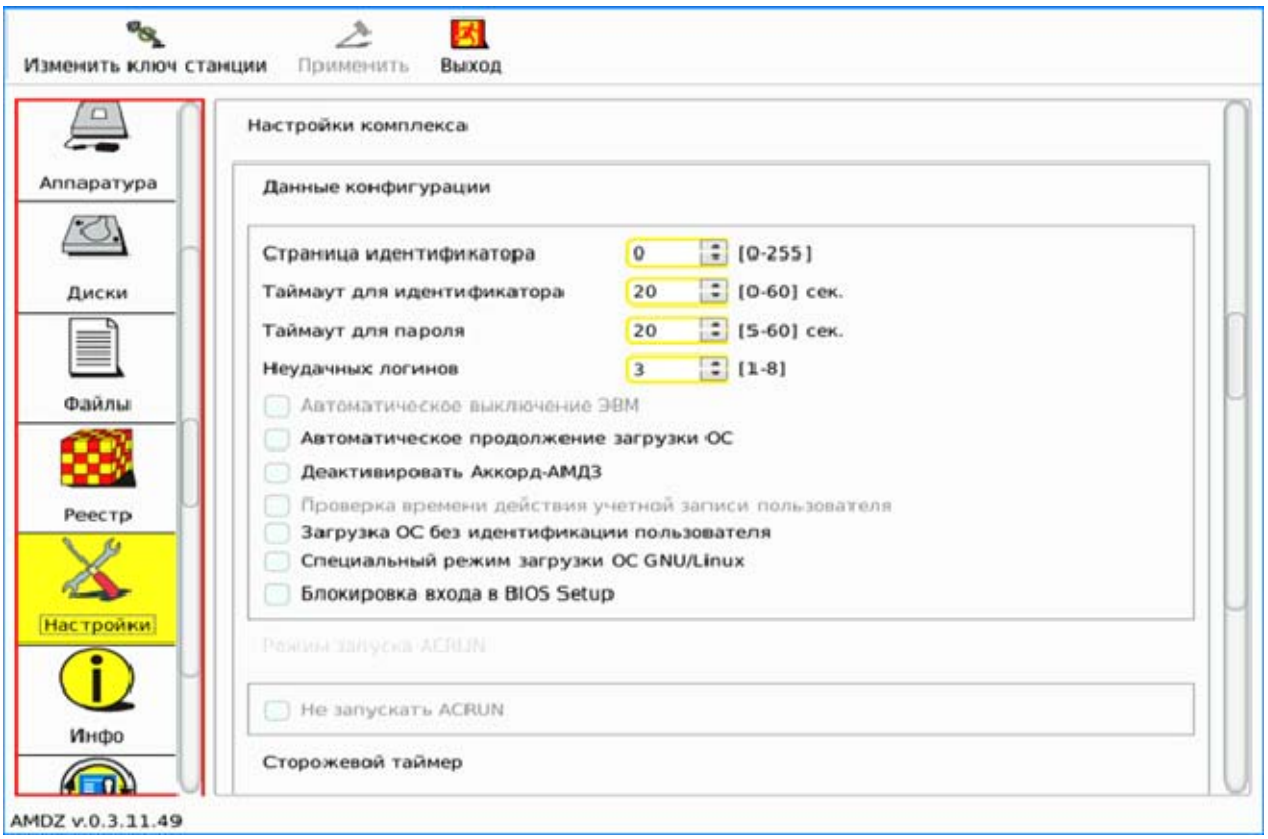

Рисунок 27 – Общие настройки комплекса

3.15.1. Данные конфигурации

Для настроек данных конфигурации установлены следующие параметры:

- страница идентификатора;
- таймаут для идентификатора;
- таймаут для пароля;
- количество неудачных логинов
- автоматическое продолжение загрузки ОС;
- загрузка ОС без идентификации пользователя;
- специальный режим загрузки ОС GNU/Linux;
- блокировка входа в BIOS Setup.

«Страница идентификатора» – определяет, с какой страницы внутренней памяти персонального идентификатора располагается служебная информация ПАК «ИНАФ». Данный параметр изменять не рекомендуется. Изменение допускается, если используется ПО других производителей, которое осуществляет запись/чтение в идентификатор именно в 0-1 страницу памяти. Номер страницы должен быть четным.

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

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

Параметр «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.

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.

Если в настройках конфигурации установлен параметр «Загрузка ОС без идентификации пользователя», то в процессе загрузки компьютера с установленным ПАК «ИНАФ» выполнение процедур идентификации и аутентификации пользователя не требуется, но загрузка ОС осуществляется только после успешного завершения всех контрольных процедур (установленных в рамках подраздела 3.13).

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

При установке параметра «Блокировка входа в BIOS Setup» любые попытки войти в BIOS с целью изменения ее настроек будут блокированы.

3.15.2. Установка специального режима загрузки ОС GNU/Linux»

В ПАК «ИНАФ» 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 «ИНАФ» передает управление выбранному ядру ОС, минуя передачу управления дисками.

Для активации данного режима следует:

1. в разделе с ядром ОС и загрузчиком создать файл конфигурации с именем ACBOOT, прописав в нем следующие параметры:
   - в первой строке – имя ядра linux (полный путь в разделе);
   - во второй строке – имя initrd (полный путь в разделе);
   - в третьей строке – параметры ядра, передающиеся при загрузке;
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.

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

Пример настройки:

```
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
```

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
```

3.15.3. Информация о комплексе

На вкладке «Инфо» главного окна среды администрирования отображается следующая информация о комплексе:

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

3.16. Экспорт/импорт баз данных

3.16.1. Общие сведения

Базу данных «ИНАФ» 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. в 3.16.2).

3.16.2. 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. 3.16.3).

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

3.16.3. Экспорт/импорт баз данных

Для того чтобы начать процедуру экспорта/импорта базы данных «ИНАФ», 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 28).

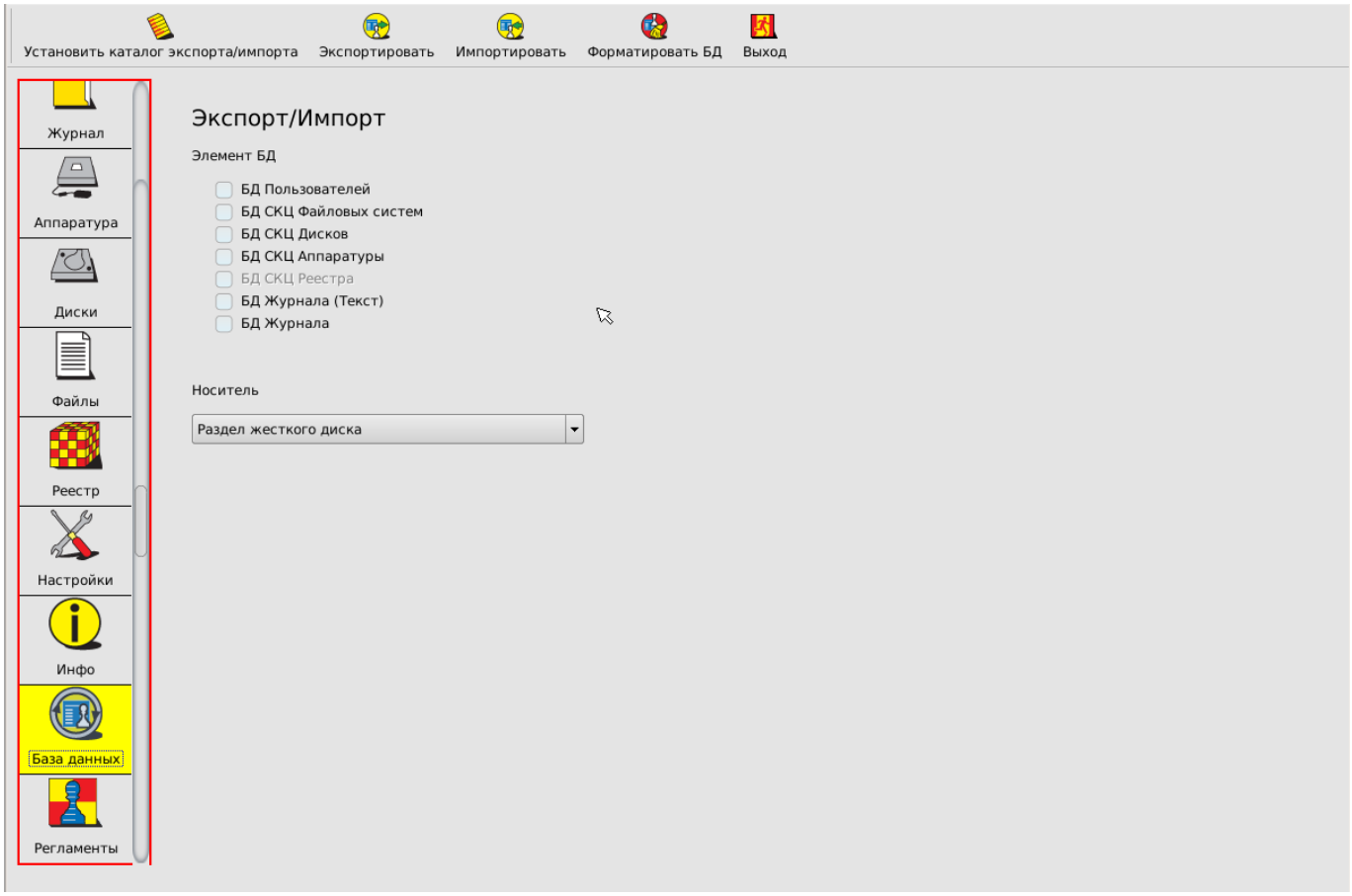

Рисунок 28 - Выбор носителя для экспорта базы пользователей

Далее, в случае 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 29).

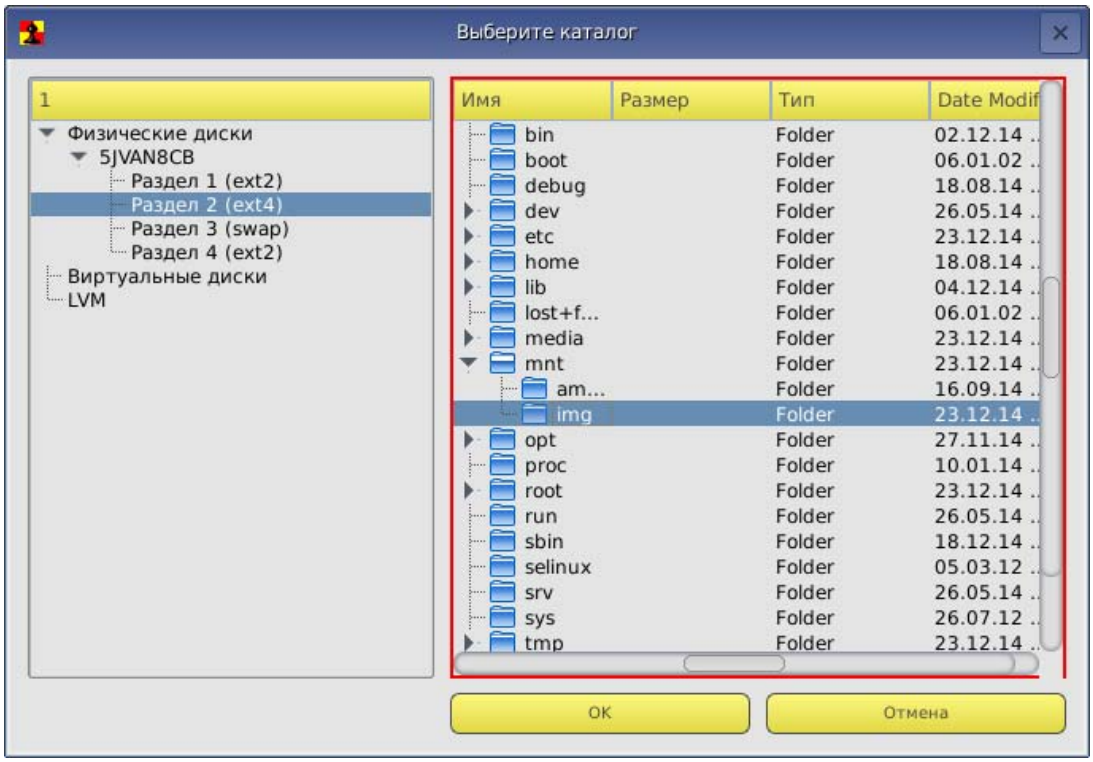

Рисунок 29 - Установка директории экспорта/импорта БД

После установки директории экспорта/импорта следует выбрать нужные элементы БД, указав их галочками, и нажать кнопку <Экспортировать>/<Импортировать> (рисунок 28).

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

3.17. 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 предустановленным ПАК «ИНАФ», или при централизованной установке комплекса с последующей отправкой компьютера в филиалы в разных регионах. После установки контроллера «ИНАФ» 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 28).

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.

3.18. Регламентные проверки

В работе ПАК «ИНАФ» предусмотрена возможность выполнения процедур самотестирования.

На вкладке «Регламенты» (рисунок 30) главного окна среды администрирования можно выполнить следующие регламентные проверки в рамках самотестирования комплекса «ИНАФ»:

- проверка целостности ПО;
- проверка целостности данных.

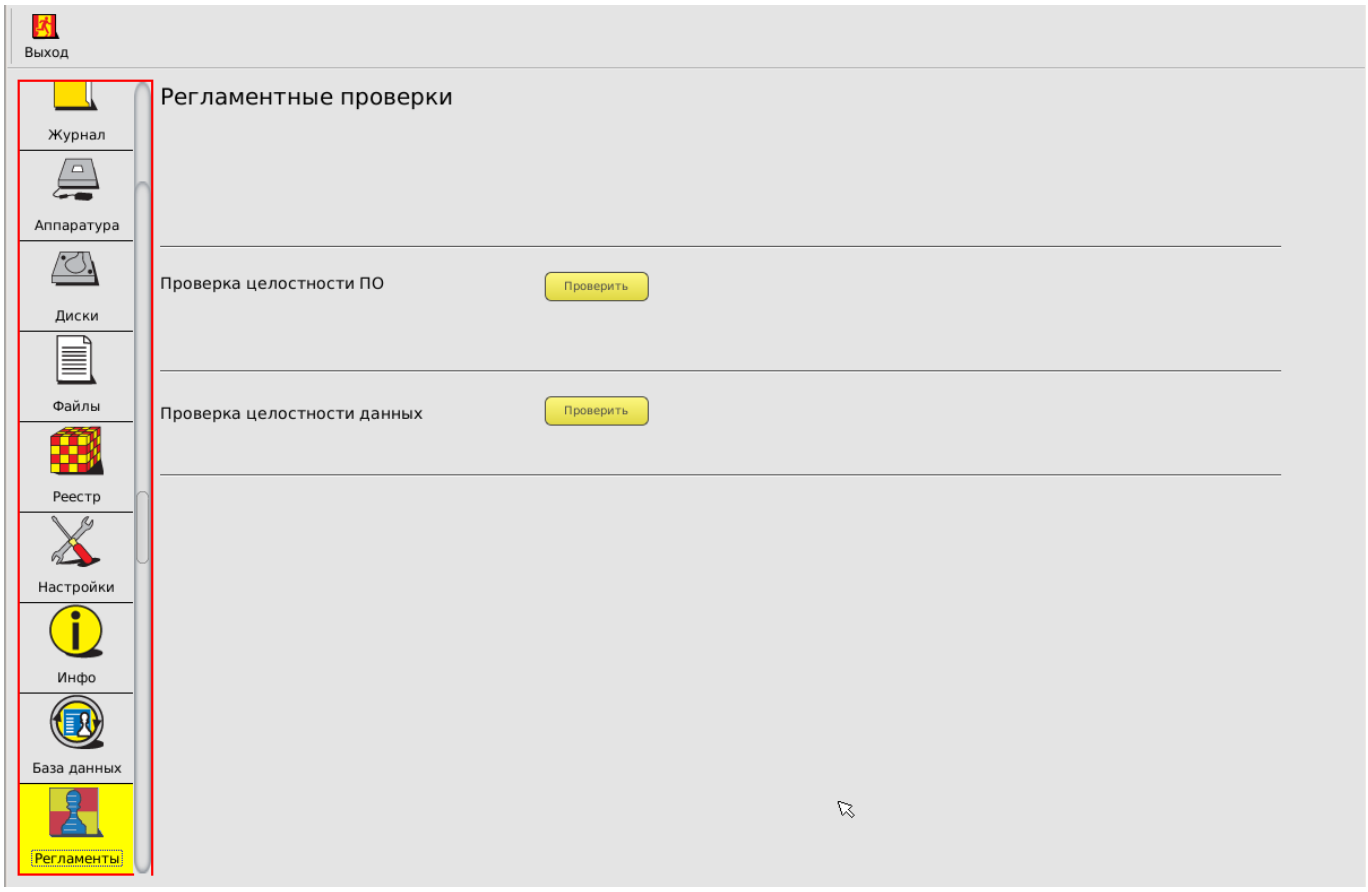

Рисунок 30 - Регламентные проверки

3.19. Выход из среды администрирования

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

4. Снятие средств защиты ПАК «ИНАФ»

ВНИМАНИЕ! Снятие защиты разрешено только администратору БИ (супервизору).

Для снятия защиты необходимо выполнить следующие действия:

1) отключить питание СВТ (РС);
2) извлечь контроллер «ИНАФ» из USB-порта СВТ (РС).

5. Параметры безопасности

Для всех пользователей «ИНАФ» должны быть установлены следующие параметры безопасности:

- парольный и аппаратный механизм аутентификации (установленный пароль и назначенный персональный идентификатор);
- количество неуспешных попыток аутентификации – 3;
- длина пароля до 12 знаков (по умолчанию 8);
- алфавит пароля: специальные символы, заглавные латинские буквы, цифры, строчные латинские буквы.

6. Требования безопасности к среде ИТ и указания по их выполнению

6.1. Требования безопасности к среде ИТ

Представленные в данном подразделе требования реализуются совместно «ИНАФ» и средой информационных технологий (ИТ).

6.1.1. FAU Аудит безопасности

FAU_SAA.1 Анализ потенциального нарушения

FAU_SAA.1.1. Функции безопасности (ФБ) среды функционирования должны быть способны применить набор правил мониторинга событий, подвергающихся аудиту, и указать на возможное нарушение ПБО, основываясь на этих правилах.

FAU_SAA.1.2. ФБ среды функционирования при мониторинге событий, подвергающихся аудиту, должны реализовывать накопление или объединение следующих событий, указывающих на возможное нарушение безопасности:

- начало сеанса пользователя;
- прохождение процедуры аутентификации пользователем;
- осуществление контроля целостности аппаратуры ПЭВМ;
- осуществление контроля целостности отдельных файлов и программ;
- осуществление контроля целостности системных областей жестких дисков (секторов);
- осуществление контроля целостности системного реестра (для ОС семейства Microsoft Windows);
- создание журнала системных событий и действий пользователей;
- изменение полномочий пользователей.

6.1.2. FIA Идентификация и аутентификация

FIA_UAU.1 Выбор момента аутентификации

FIA_UAU.1.1. ФБ среды функционирования не должны допускать выполнение никаких действий от имени пользователя прежде, чем пользователь аутентифицирован.

FIA_UAU.1.2. ФБ среды функционирования должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения любого другого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

FIA_UID.1 Выбор момента идентификации

FIA_UID.1.1. ФБ среды функционирования не должны допускать выполнение каких-либо действий от имени пользователя прежде, чем он идентифицирован.

FIA_UID.1.2. ФБ среды функционирования должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения любого

другого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

6.1.3. FPT Защита ФБО

FPT_AMT.1 Тестирование абстрактной машины

FPT_AMT.1.1. ФБ среды функционирования должны выполнять пакет тестовых программ при первоначальном запуске для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая положена в основу комплекса.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1. Комплекс должен быть способен предоставлять надежные метки времени для собственного использования.

6.2. Указания по выполнению требований безопасности к среде ИТ

Выполнение требований FAU_SAA.1.1 и FAU_SAA.1.2

В энергонезависимой памяти контроллера «ИНАФ» ведется системный журнал событий (подробнее см. 3.14).

В журнал заносится информация о сеансах работы пользователей с указанием номера идентификатора и все попытки несанкционированного доступа к компьютеру. Сведения о наименовании и результатах операций, фиксируемых в системном журнале «ИНАФ», см. в Приложении 1.

Перед каждым сеансом работы «ИНАФ» выполняет контроль целостности объектов по спискам контроля.

Если обнаруживается несовпадение параметров конфигурации, записанных в памяти контроллера, и текущих параметров системы, выдается сообщение «Контроль не пройден» и загрузка компьютера блокируется для обычного пользователя; или выводится запрос на администрирование, если идентифицирован администратор.

В этом случае администратору необходимо изучить содержимое системного журнала, принять соответствующие меры по выявлению нарушителя, затем выполнить пересчет контрольных сумм (подробнее см. 3.13).

Выполнение требований FIA_UAU.1 и FIA_UID.1

Среда функционирования ПАК «ИНАФ» должна запрещать любые действия от имени пользователя до завершения процедур идентификации и аутентификации пользователя, а также требовать выполнения данных процедур до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Выполнение требования FPT_AMT.1

Контроллер «ИНАФ» в процессе каждого старта компьютера выполняет ряд тестовых программ для демонстрации правильности выполнения предположений безопасности, обеспечиваемых абстрактной машиной, которая положена в основу комплекса.

Для выполнения данного требования нет необходимости в каких-либо действиях администратора «ИНАФ».

Выполнение требования FPT_STM.1

Во всех контроллерах «ИНАФ» установлена батарейка часов реального времени, предоставляющая надежные метки времени.

Для выполнения данного требования нет необходимости в каких-либо действиях администратора «ИНАФ».

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 «ИНАФ»

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	
Ctrl+D Alt+D	Удалить пользователя	
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 «ИНАФ» 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 7, рекомендуемых для контроля целостности на аппаратном уровне (с помощью встроенного ПО «ИНАФ»)

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

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

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

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

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

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